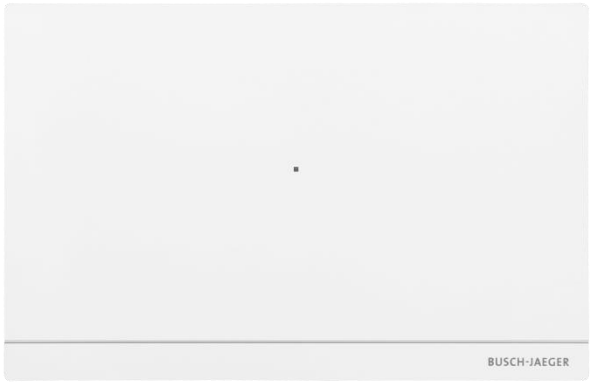
2TMD041800D0090 | 12.08.2025

Product manual

Busch-Welcome® IP

Busch-AccessControl

D04011-03 Smart Access Point Pro



BUSCH-JAEGER

1 Notes on the instruction manual

Please read through this manual carefully and observe the information it contains. This will assist you in preventing injuries and damage to property and ensure both reliable operation and a long service life for the device.

Please keep this manual in a safe place. If you pass the device on, also pass on this manual along with it. Busch-Jaeger accepts no liability for any failure to observe the instructions in this manual.

2 Safety

Warning

Electric voltage!

Dangerous currents flow through the body when coming into direct or indirect contact with live components.

This can result in electric shock, burns or even death.

– Disconnect the mains power supply prior to installation and/or disassembly!
– Permit work on the 100-240 V supply system to be performed only by specialist staff!

3 Intended use

As a part of the Busch-Welcome® IP system, this device can only be used with accessories from the system

IC statement

Product name:

Model:

IC:XXX-YYY

CAN ICES-3 (B)/NMB-3(B)

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. L'appareil ne doit pas produire de brouillage;

2. L’appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d’en compromettre le fonctionnement.

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

Cet ééquipement est conforme aux limites d exposition aux rayonnements de la IC éétablies pour un environnement non contrôéé. Cet ééquipement doit êêtre installé et fonctionner à au moins 20 cm de distance d un radiateur ou de votre corps.

4 Environment

Consider the protection of the environment!

Used electric and electronic devices must not be disposed of with household waste.

– The device contains valuable raw materials that can be recycled. Therefore, dispose of the device at the appropriate collecting facility.

4.1 Busch-Jaeger devices

All packaging materials and devices from Busch-Jaeger bear the markings and test seals for proper disposal. Always dispose of the packing materials and electric devices and their components via an authorized collection facility or disposal company.

Busch-Jaeger products meet the legal requirements, in particular the laws governing electronic and electrical devices and the REACH ordinance.

(EU-Directive 2012/19/EU WEEE and 2011/65/EU RoHS)

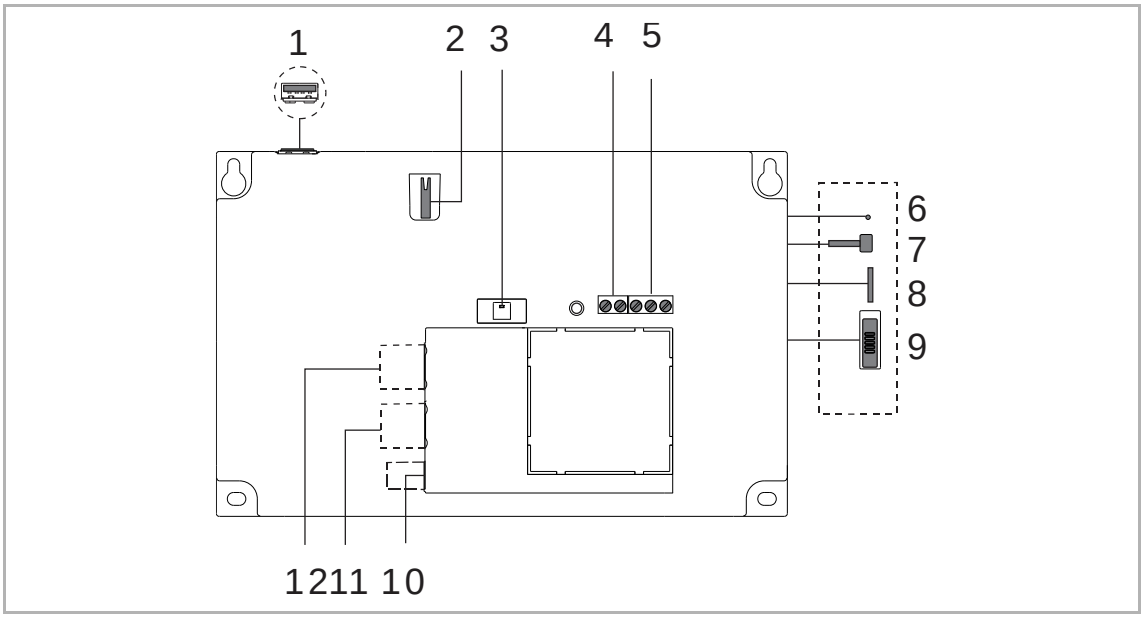
(EU-REACH ordinance and law for the implementation of the ordinance (EG) No.1907/2006)

5 Product description

5.1 Device type

Article number	Product ID	Product name	Color	Size (DxHxW) Unit: mm
D04011-03	2TMA400260W0008	Smart Access Point Pro	White	204 x 132 x 32

5.2 Terminal description



No.	Function
1	USB stick connector (reserved)
2	**Tamper switch** It is used to prevent intruders breaking into the Smart Access Point. Once the front shell of Smart Access Point is opened, a tamper alert will be sounded by the built-in speaker of Smart Access Point. The tamper alert can be also set as the precondition and/or event in the "Action" function. Then it can be triggered together with other actions (e.g. pushing notification).
3	(1) Status indicator LED
4	Binary input (used to interact with other systems)
5	Binary output (used to interact with other systems)
6	**Reset button** Press and hold this button for 10 s to enter the reset mode to reset the password of the first admin user.
7	**Switch on/off to activate/deactivate WiFi Access Point mode** When WiFi Access Point mode is activated, Status indicator LED flashes red.
8	Micro SD card connector (reserved)
9	**Security switch** ON = The devices are not allowed to be added or deleted OFF = The devices are allowed to be added or deleted (default)
10	Power input connector (DC-JACK input)
11	LAN (PoE)
12	LAN (2)

(1) Status indicator LED

Description	Blue	Red	Green	White	Priority
Reset to factory default				Flashing slowly	7 (Highest)
Alarm (e.g. tamper alarm)				Flashing quickly	6
Power on or Initial setup				on	5
WiFi Access Point is enabled		Flashing slowly			4
Security mode is disabled		on			3
Doorbell is muted	on				2
Normal operation			on		1

6 Technical data

Designation	Value
Rating voltage	24 V ⎓
Operating voltage range	20-27 V ⎓
Rating current	24 V ⎓, 375 mA
PoE standard	IEEE802.3 af
Wireless transmission band	**802.11b/g/n:** 2412...2462MHz (for United States) 2412...2472MHz (for European countries) **802.11a/n:** 5150…5250MHz 5250…5350MHz 5470…5725MHz (not used in Russia) 5725…5850MHz (for United States)
Wireless transmission power	Max. 20 dBm@12 Mbps OFDM 2.4 G Max. 20 dBm@12 Mbps OFDM 5.8 G
Wireless transmission standard	IEEE 802.11 a/b/g/n
Operating temperature	-10 °C…+45 °C
Storage temperature	-25 °C…+70 °C
IP level	IP 30
IK level	IK 05
Relay output	30 V ⎓, 1 A
Binary input	5 V ⎓, 1mA

Bluetooth data

Bluetooth standard	4.2
Frequency range	2.402…2.480 GHz
TX power	Maximum 8 dBm
RX sensitivity	Minimum -92 dBm

7 Mounting/Installation

Warning

Electric voltage!

Dangerous currents flow through the body when coming into direct or indirect contact with live components.

This can result in electric shock, burns or even death.

– Disconnect the mains power supply prior to installation and/or disassembly!
– Permit work on the 100-240 V supply system to be performed only by specialist staff!

7.1 Requirement for the electrician

Warning

Electric voltage!

Install the device only if you have the necessary electrical engineering knowledge and experience.

– Incorrect installation endangers your life and that of the user of the electrical system.
– Incorrect installation can cause serious damage to property, e.g. due to fire.

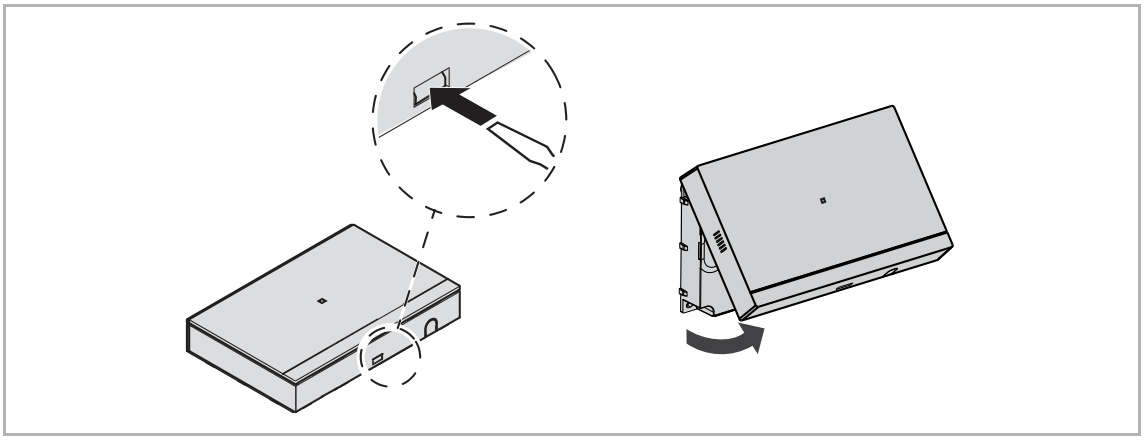
The minimum necessary expert knowledge and requirements for the installation are as follows:

– Apply the "five safety rules" (DIN VDE 0105, EN 50110):
  1. Disconnect
  2. Secure against being re-connected
  3. Ensure there is no voltage
  4. Connect to earth and short-circuit
  5. Cover or barricade adjacent live parts.
– Use suitable personal protective clothing.
– Use only suitable tools and measuring devices.
– Check the type of supply network (TN system, IT system, TT system) to secure the following power supply conditions (classic connection to ground, protective grounding, necessary additional measures, etc.).

7.2 Mounting

1. Dismantle

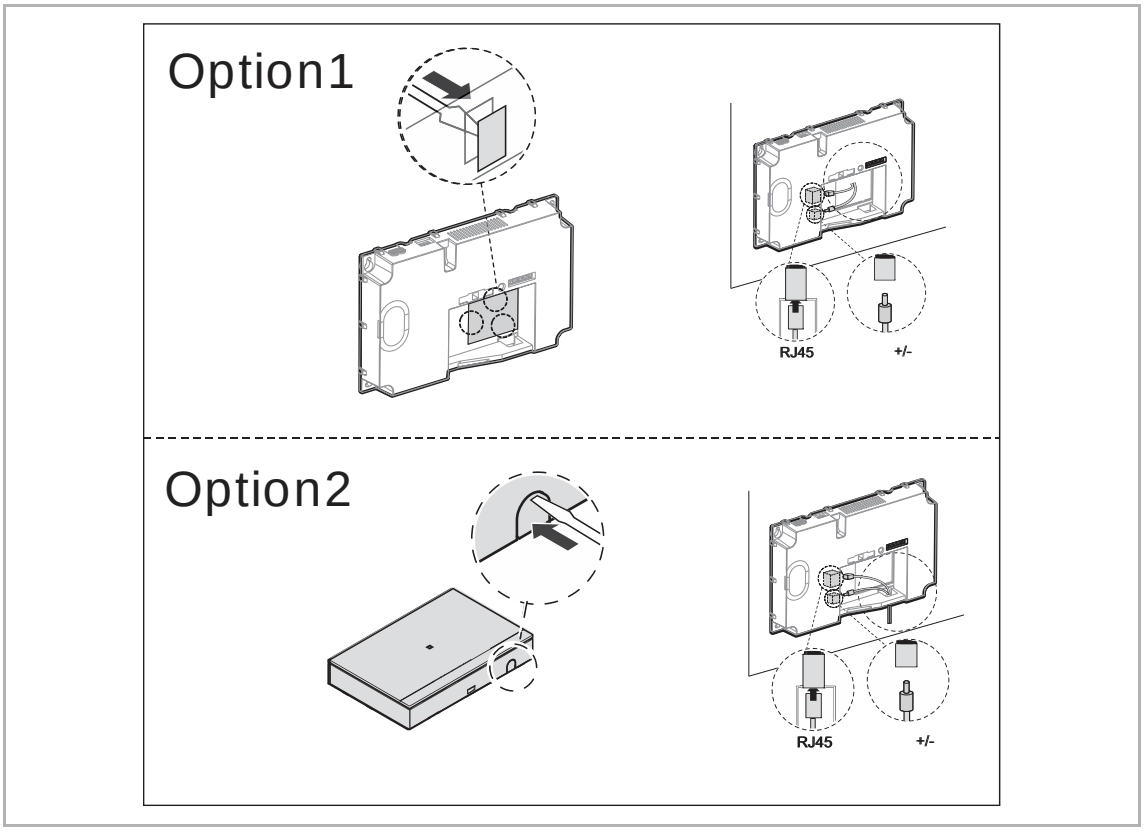
Pull the clamp on the bottom of the device and then open the front cover.



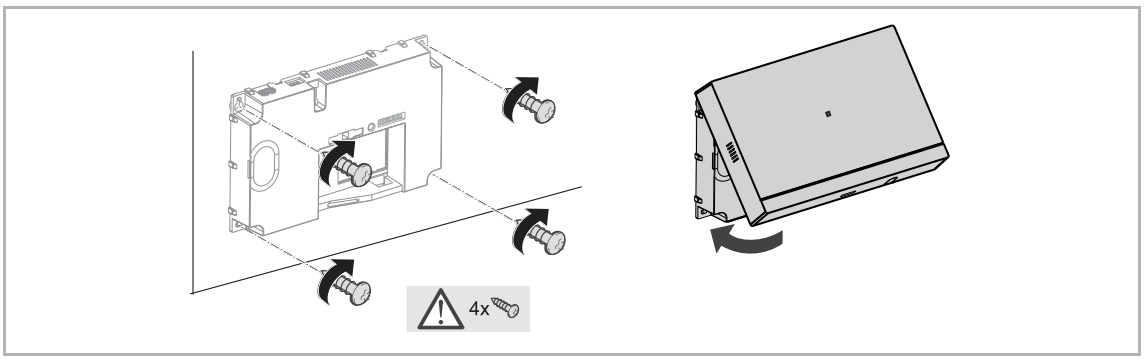
2. Wiring

Option 1: Wiring from the back

Option 2: Wiring from the bottom



3. Mounting



8 Commissioning

8.1 System requirements

User interface

Commissioning is always carried out via the web-based user interface of "Smart Access Point".

To open the web-based user interface, you require a computer with a LAN or WLAN network adaptor and an installed Internet browser.

The recommended browsers are:

- Firefox (from version 9)
- Google Chrome
- Safari

Welcome App

For the installation of the Welcome App you require a smartphone or tablet with an Android (from 4.0) or iOS (from iOS 7) operating system.

Home network

To be able to access the Welcome App and Internet services (e.g. e-mail) at the same time during standard operation, "Smart Access Point" must be integrated into the existing home network after commissioning. For this, a router with Ethernet or WLAN interface is required.

myBUSCH-JAEGER account

It is recommended to register a myBUSCH-JAEGER account before the initial setup.

1. Benefits for myBUSCH-JAEGER account

- It is necessary when you want to reset the password for the first admin user.
- It is necessary when you want to subscribe the "Remote-control" services.
- It is necessary when you want to receive the notification via the Welcome App
- It is necessary when you want to log in via the "Smart Access Point" web-based user interface.

Remote control service

There are 3 kinds of "Remote-control" services:

1. Remote Access and Notifications

Remote services for Welcome IP, AccessControl and VideoControl for Welcome App:

- Receive door calls.
- Video surveillance calls to outdoor stations and IP cameras.
- Remote release of digital door locks (support for maximum 8 "Electronic lock cylinders").
- Remote access to local smart access point web interface.
- Event history & push notifications service.
- Per subscription: Remote access for 10 mobile devices.

2. Remote Lock Release

Remote services for AccessControl for commercial use cases on Welcome App:

- Independent from user quantity (mobile devices).
- Four different packages for up to 600 locks available.
- Remote release of digital door locks.

3. How to register an account on the myBUSCH-JAEGER portal

see chapter 13.1 “Registering an account on the myBUSCH-JAEGER portal“ on page 296.

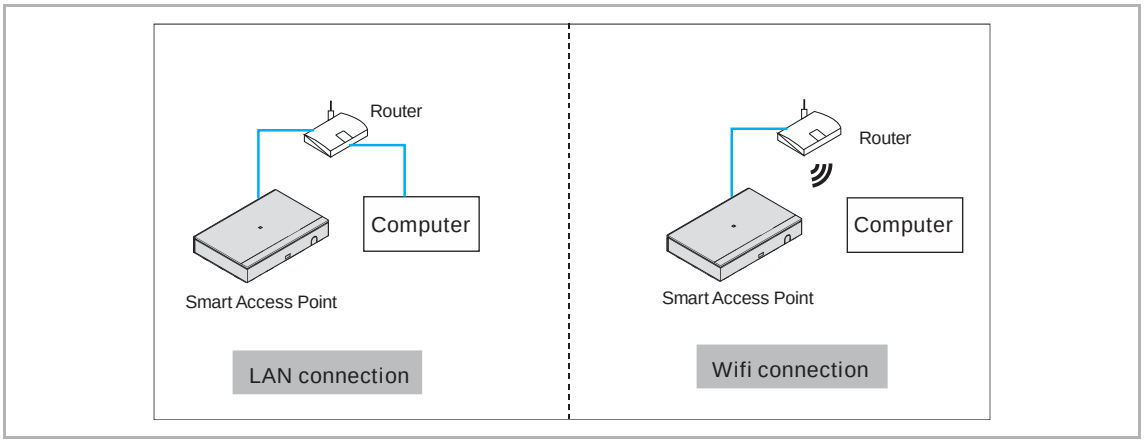
8.2 Accessing the web-based user interface of "Smart Access Point"

There are 3 options to access the web-based user interface of "Smart Access Point".

1. Through Windows UPnP service

Precondition

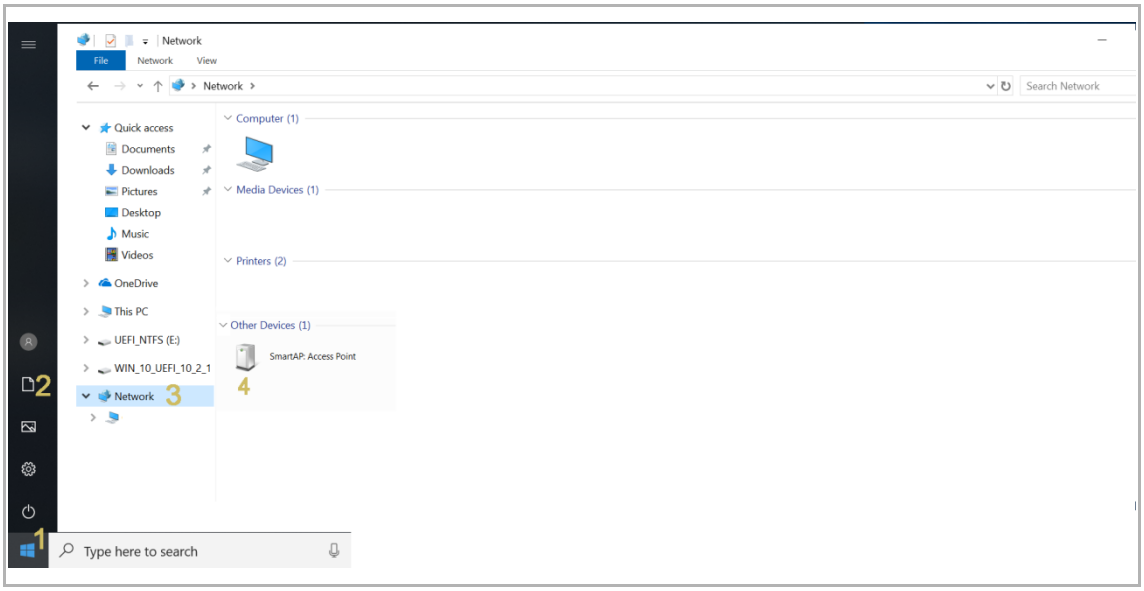
- There is a DHCP server on the network, e.g. integrated DHCP is used in the router.
- "Smart Access Point" is connected to the router by a LAN cable.
- The computer is connected to the router by LAN connection or WiFi connection.
- "Smart Access Point" is powered on and ready for operation.



Accessing "Smart Access Point" (Window 10 system as an example)

[1] Click "Start", followed by "Documents", "Network" to access "Network" screen.

[2] Double click "Smart Access Point" icon.

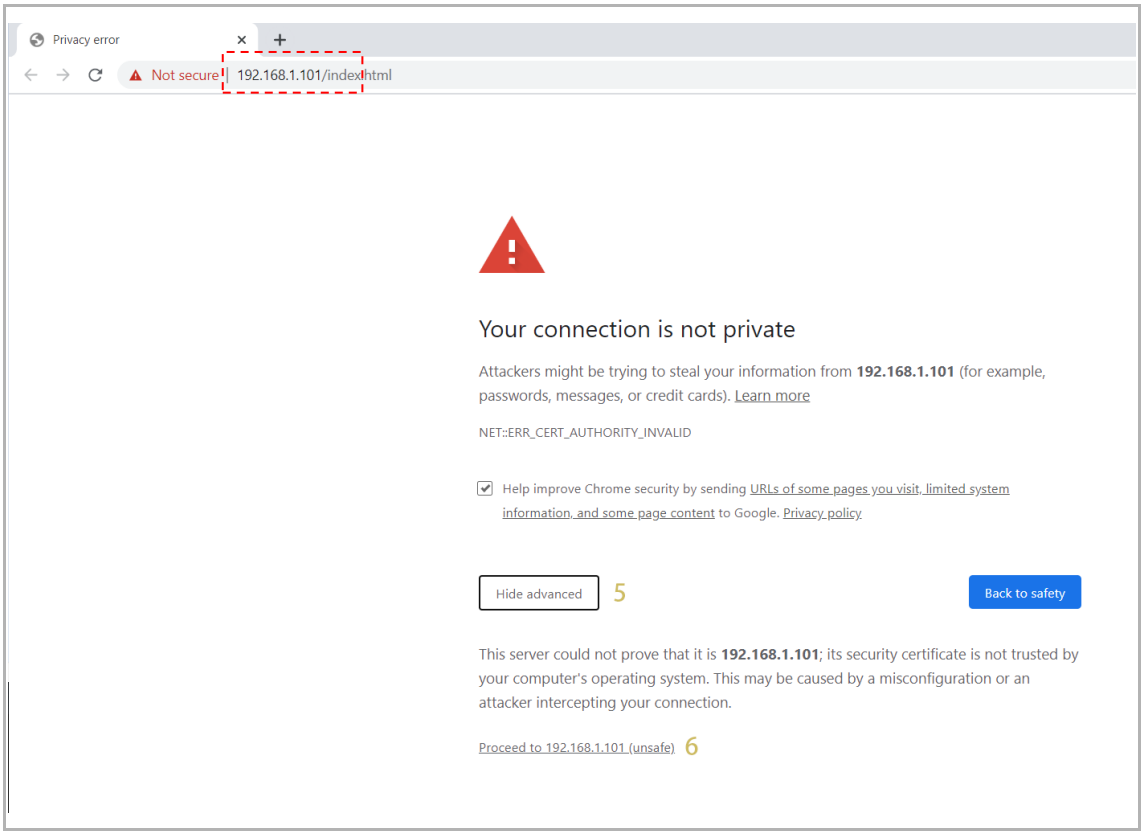


Note

If "Smart Access Point" icon is not displayed, please check the Windows firewall or ask help from your IT engineers.

[3] Switch to Security Login

- Http-connection is insecure. It is recommended to use an https-connection.
- Click "Advanced", followed by "Proceed to ...." to access the web-based user interface of "Smart Access Point". (Google chrome as an example)
- IP address of "Smart Access Point" can be viewed on the page.



2. Through entering the IP address

Precondition

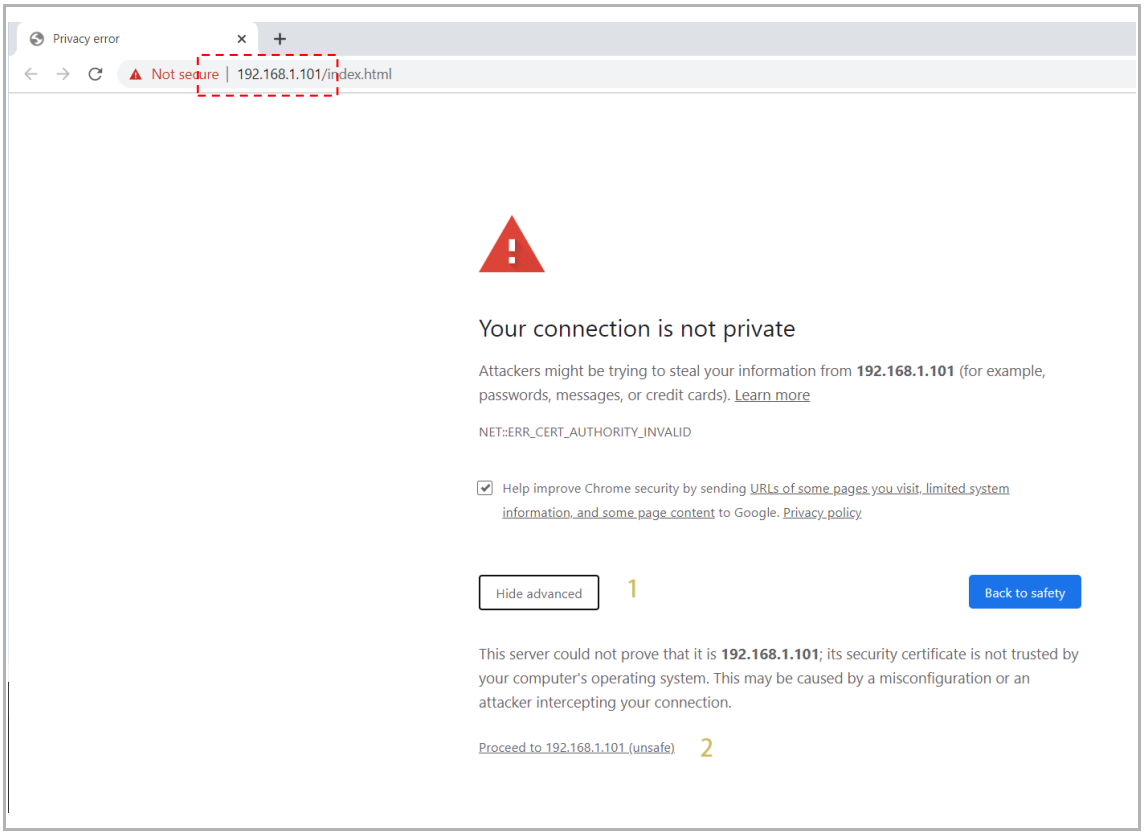
You can check the IP address of "Smart Access Point" on the router configuration website. Each router has usually an own management web interface where you can get the information. Please check your router's handbook.

Accessing "Smart Access Point" (Window 10 system as an example)

[1] Enter the IP address of "Smart Access Point" (e.g. "192.168.1.101") on the website.

[2] Switch to Security Login

- Http-connection is insecure. It is recommended to use an https-connection.
- Click "Advanced", followed by "Proceed to ...." to access the web-based user interface of "Smart Access Point". (Google chrome as an example)

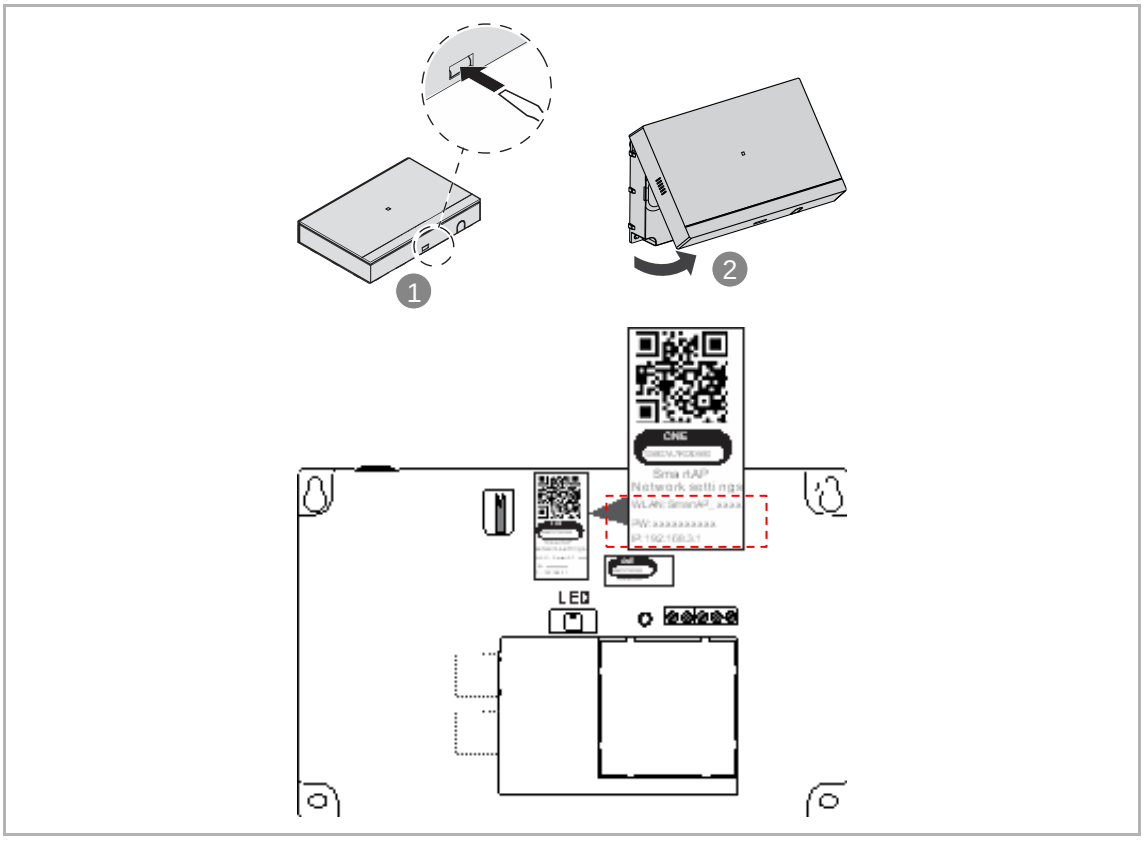


3. Through WiFi Access Point hotspot

Precondition

- Ensure network settings are obtained from the "Smart Access Point"
  - WLAN name (SSID)
  - Password
  - IP address

Please open the front shell of "Smart Access Point" and obtain the data above from the sticker.



- Ensure the alarm (e.g. tamper alarm) is not activated

Note

Status indicator LED light priority (in the sequence, high>>middle>>low):
Alarm (flash white quickly) >> Initial setup (light white on) >> WiFi Access Point mode is activated (flash red) >> Security mode is activated (light red on)

Temper alarm will be activated if the front cover of "Smart Access Point" is open. (Figure A) In this case, status indicator LED will flash white quickly and it is impossible to judge if WiFi Access Point mode is activated. Please close the front shell after you have obtained the SSID information. (Figure B)

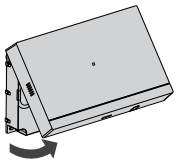


Figure A

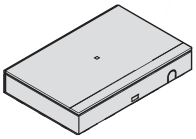
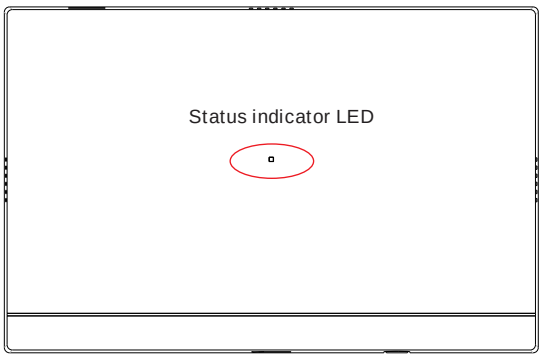


Figure B

- Ensure that the WiFi Access Point mode has been activated
  - During the initial setup: Status indicator LED lights white on.
  - After the initial setup: Status indicator LED flashes red.
- "Smart Access Point" is powered on and ready for operation.



Note

"Smart Access Point" works like a central WiFi router when it works in WiFi Access Point mode.

Accessing "Smart Access Point" (Window 10 system as an example)

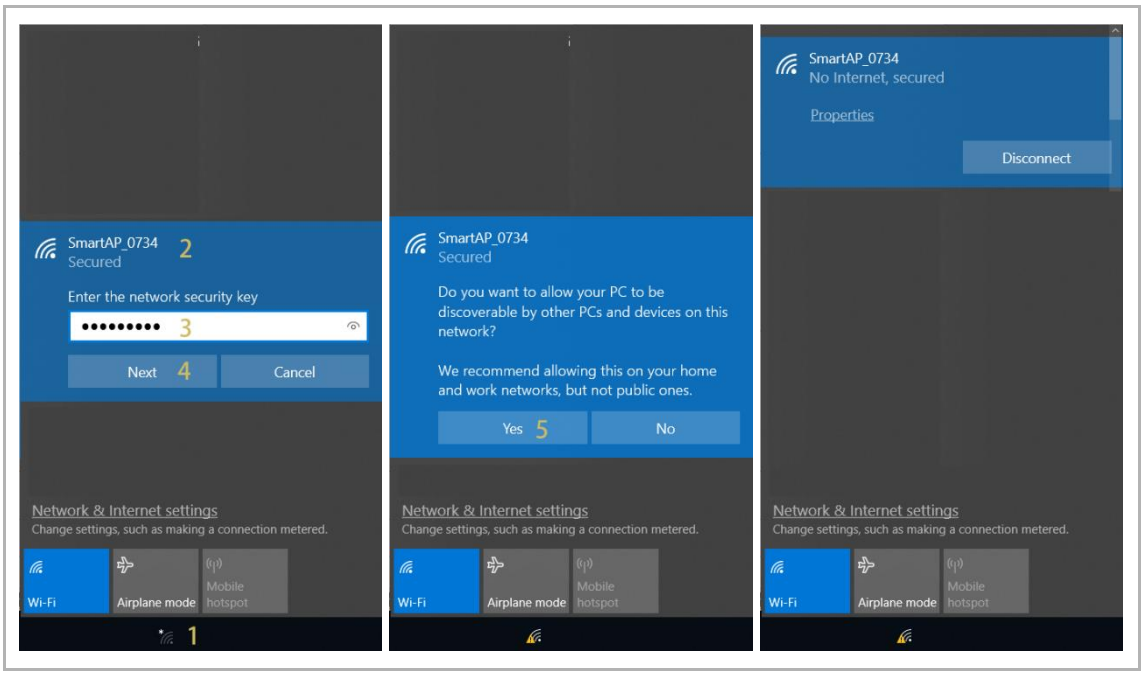
[1] Click "Internet access" icon.

[2] Click the WLAN name (SSID) of "Smart Access Point".

[3] Enter the password.

[4] Click "Next".

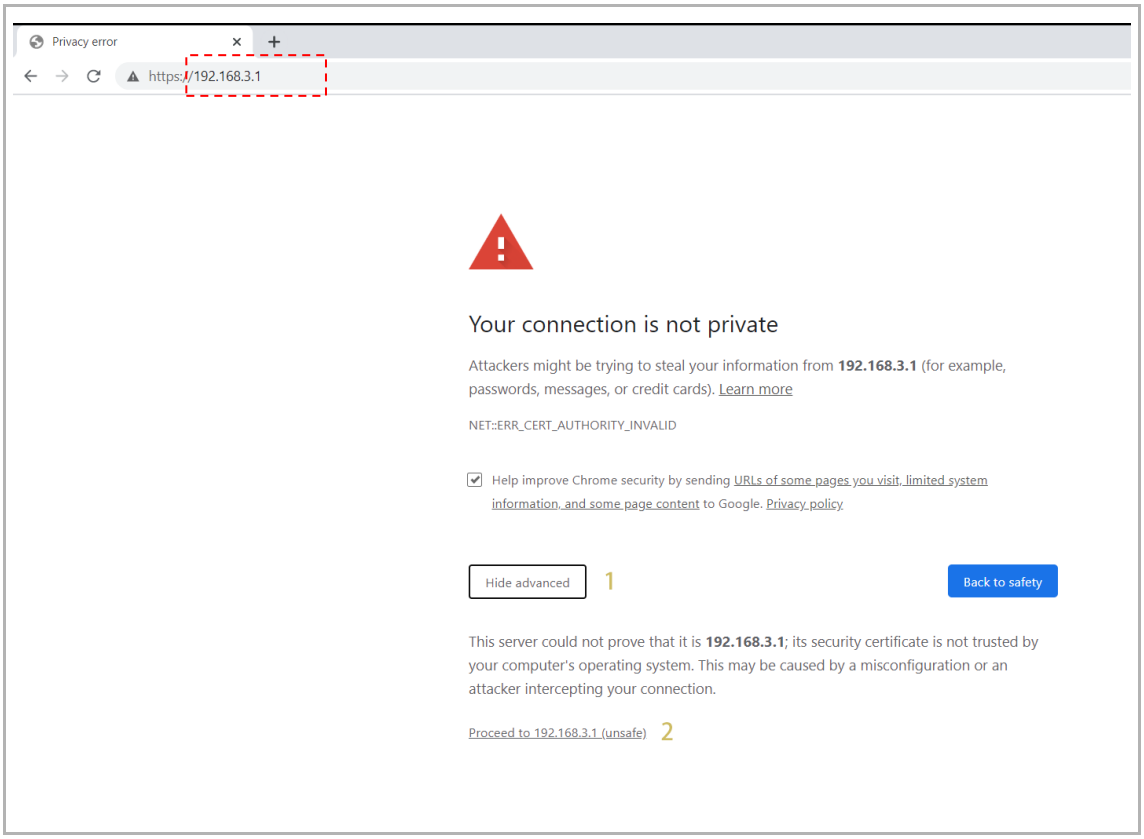
[5] Click "Yes" to connect your computer to the WiFi hotspot of "Smart Access Point".



[6] Enter "192.168.3.1" on the website to access "Smart Access Point".

[7] Switch to Security Login

- Http-connection is insecure. It is recommended to use an https-connection.
- Click "Advanced", followed by "Proceed to ...." to access the web-based user interface of "Smart Access Point". (Google chrome as an example)



8.3 Initial setup

You need to do the initial setup the first time "Smart Access Point" is powered on or "Smart Access Point" is reset to the factory defaults.

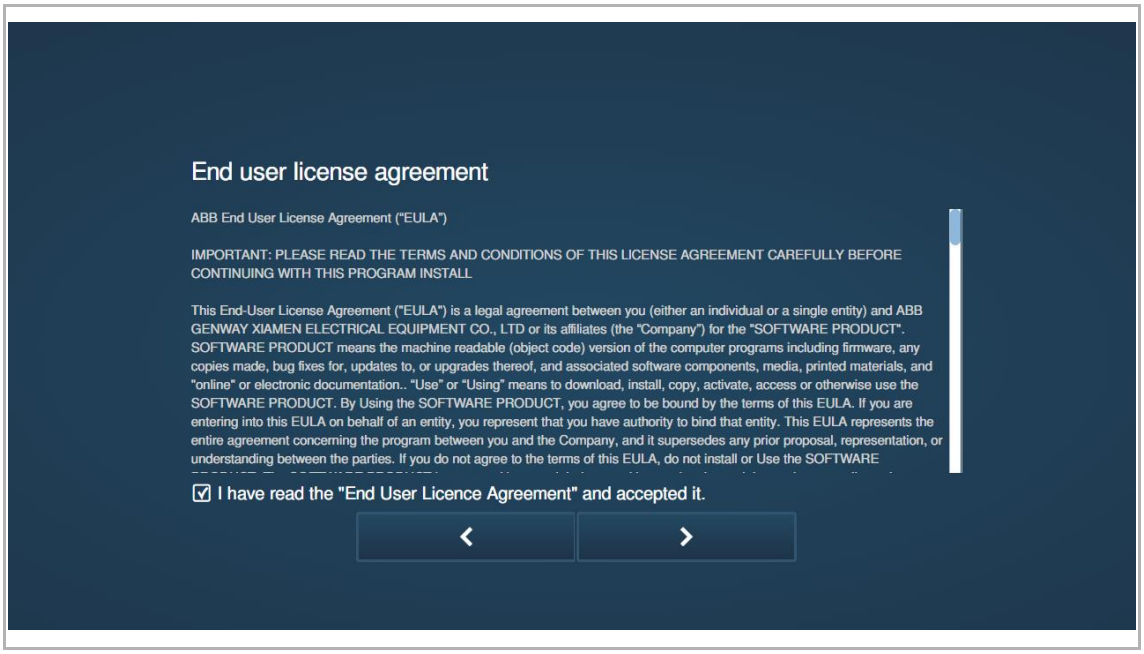
Follow the steps below on the web-based user interface of "Smart Access Point".

1. Select language

Selects a language for the display text of user interface, logs, messages, notifications and so on.

2. Accept end user license

You need to tick the checkbox to accept end user license. Then click ">" to continue.

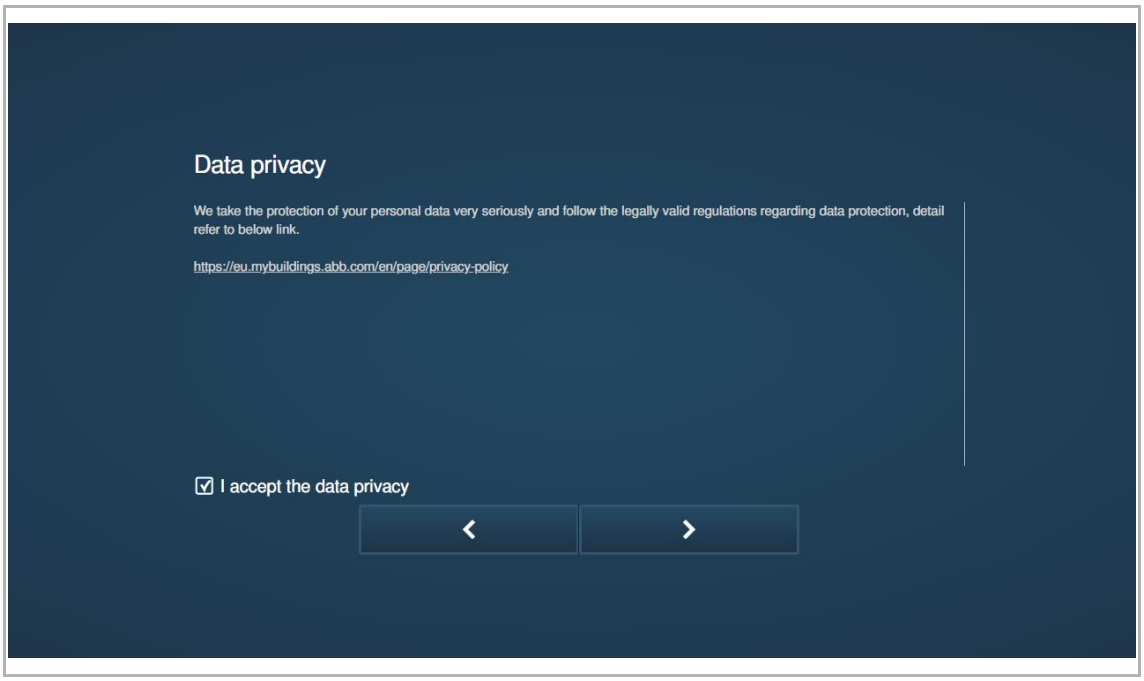


3. Accept Open Source Software license

You need to tick the checkbox to accept Open Source Software license. Then click ">" to continue.

4. Accept data privacy

You need to tick the checkbox to accept Data privacy. Then click ">" to continue.



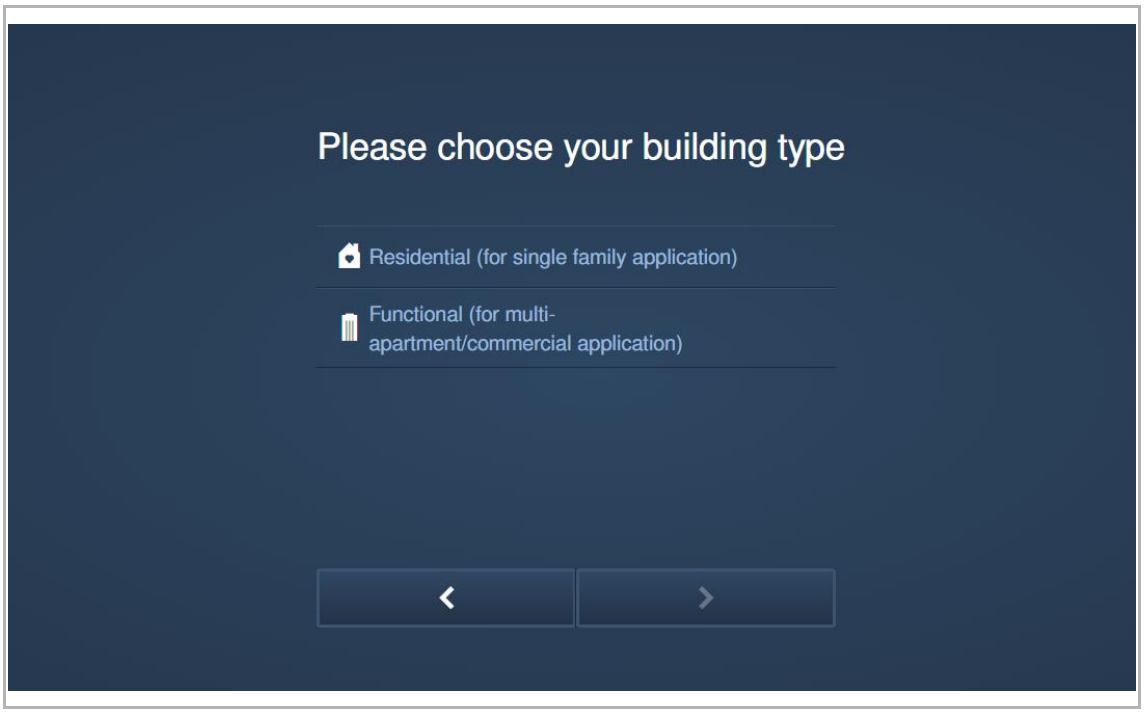
5. Choose building type

see chapter 8.1 “System requirements“ on page 17.

Attention!

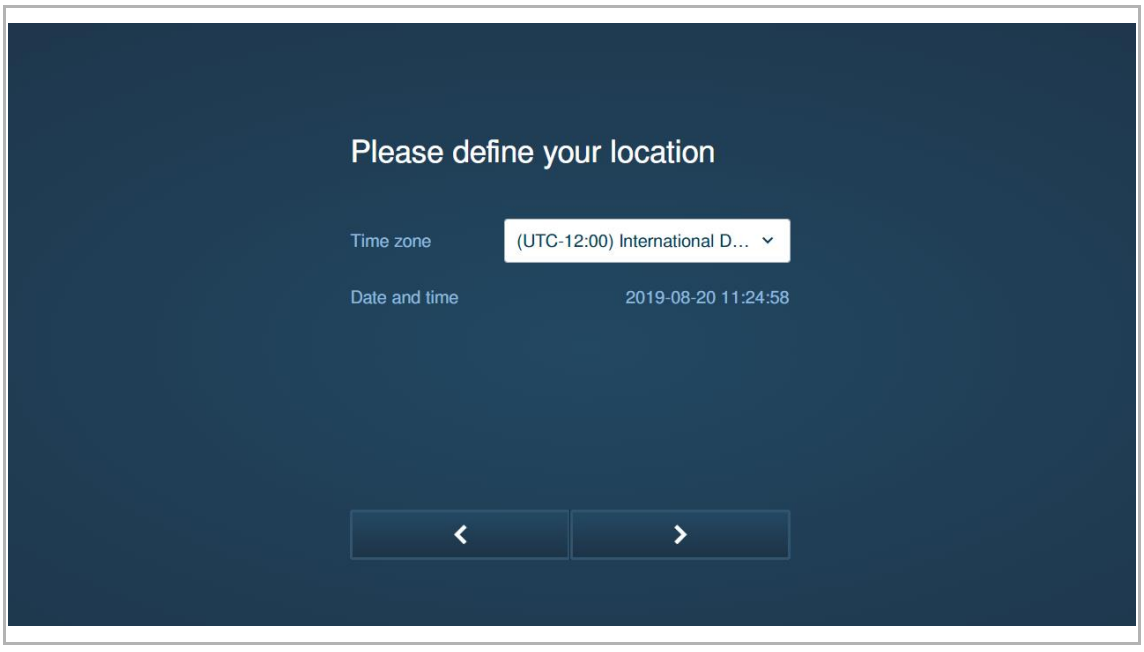
The building type can only be set in the initial setup and it cannot be changed after the initial setup.

If you want to change the building type, you need to reset "Smart Access Point" to the factory defaults.



6. Define your location

Select the time zone from the drop-down list.



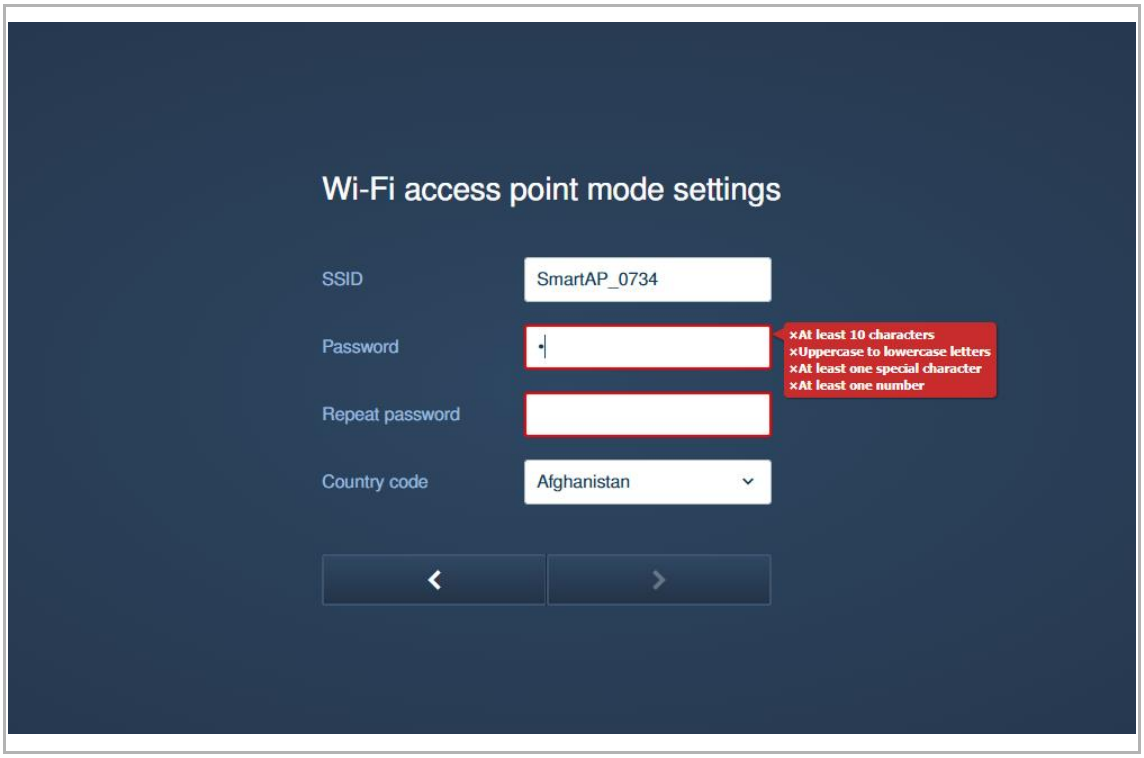
7. Change WiFi Access Point mode Wi-Fi setting and set country code

It is compulsory to change the password in the initial setup. The password rule is displayed on a pop-window when you enter the password.

Attention!

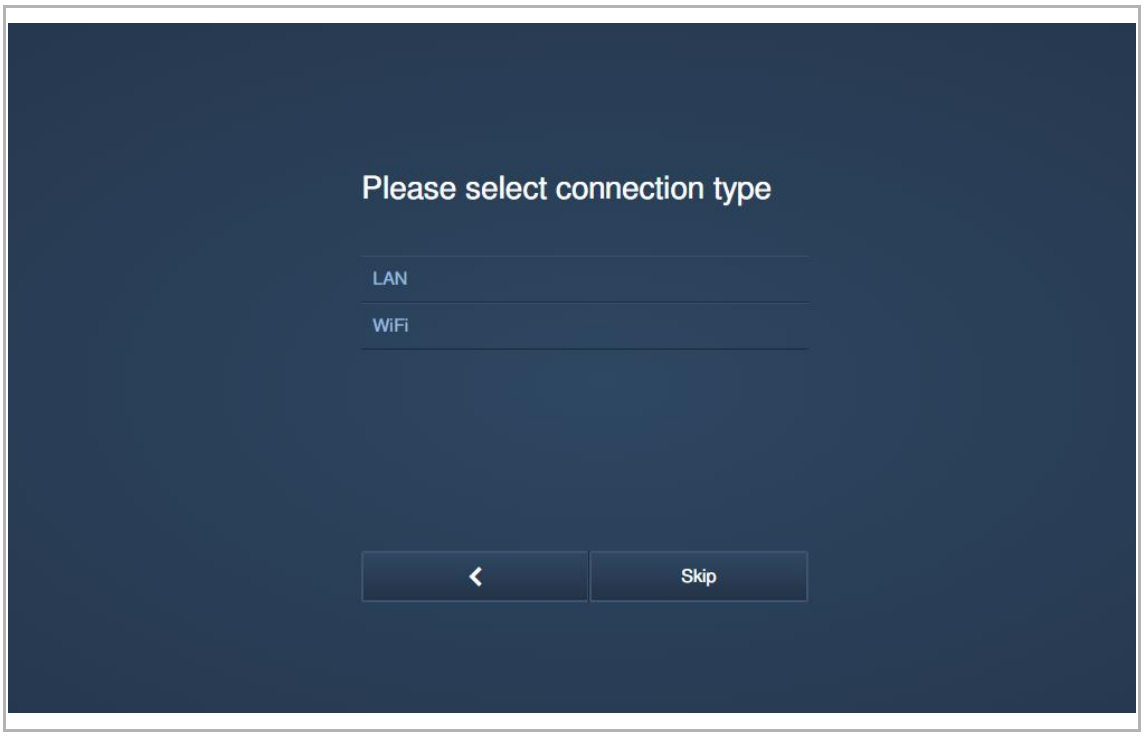
Please ensure that the country code is configured correctly according to the device location.

The "Country code" setting ensures that your router will only enable Wi-Fi radio settings that conform with the country's official regulatory laws.



8. Select a connection type

There are 3 options to connect to home network:



Option 1: LAN

- All communications to Door entry system devices, VideoControl devices and "RF/IP Gateway" run via LAN interface.
- All communications to RF devices run via RF connection.
- All Door Entry system devices keep their own IP address when they are used in the building network. "Smart Access Point" can reach them even if they use a DHCP client IP address.

Option 2: WiFi

- All communications to Door entry system devices, VideoControl devices and "RF/IP Gateway" run via WiFi interface.
- All communications to RF devices run via RF connection.
- All Door Entry system devices keep their own IP address when they are used in the building network. "Smart Access Point" can reach them even if they use a DHCP client IP address.

Option 3: Skip the selection

- No communications to Door entry system devices, VideoControl devices and "RF/IP Gateway" run through LAN or WiFi interface.
- Only RF devices can be communicated via RF connection.

Establish LAN connection

If LAN connection is selected, you need to set IP address to establish the LAN connection.

By activating the checkbox "Obtain IP address automatically", SmartAP will work as a DHCP client. The IP address needs to be assigned from DHCP server (such as router with DHCP enabled).

By deactivating the checkbox "Obtain IP address automatically", network parameters need to be configured including IP address, subnet mask and default gateway.

Connect to a WiFi Network

If WiFi connection is selected, you need to connect to a WiFi network.

All available nearby WiFi network will be displayed on the list. If you can’t find the designated nearby WiFi network, click the "Refresh" button to search again.

Click the designated WLAN name (SSID) in the list, enter the password, followed by "Connect" to connect the WiFi network.

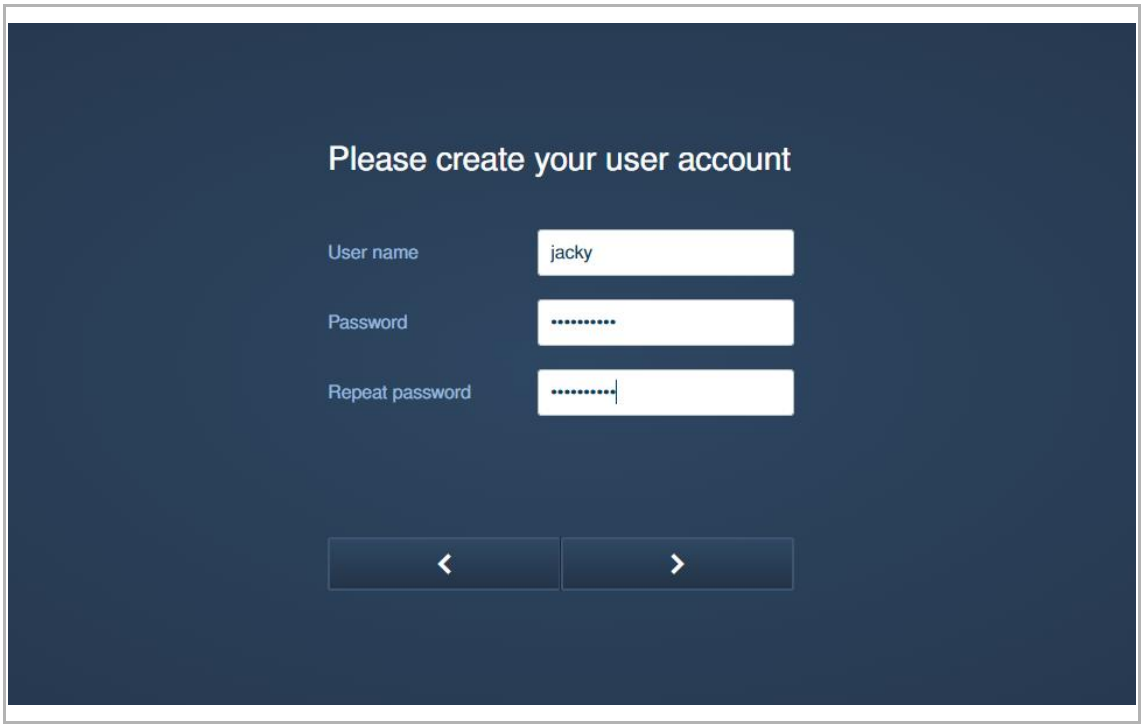
9. Create the first admin user

Enter the username and the password twice to create the first admin user.

Note

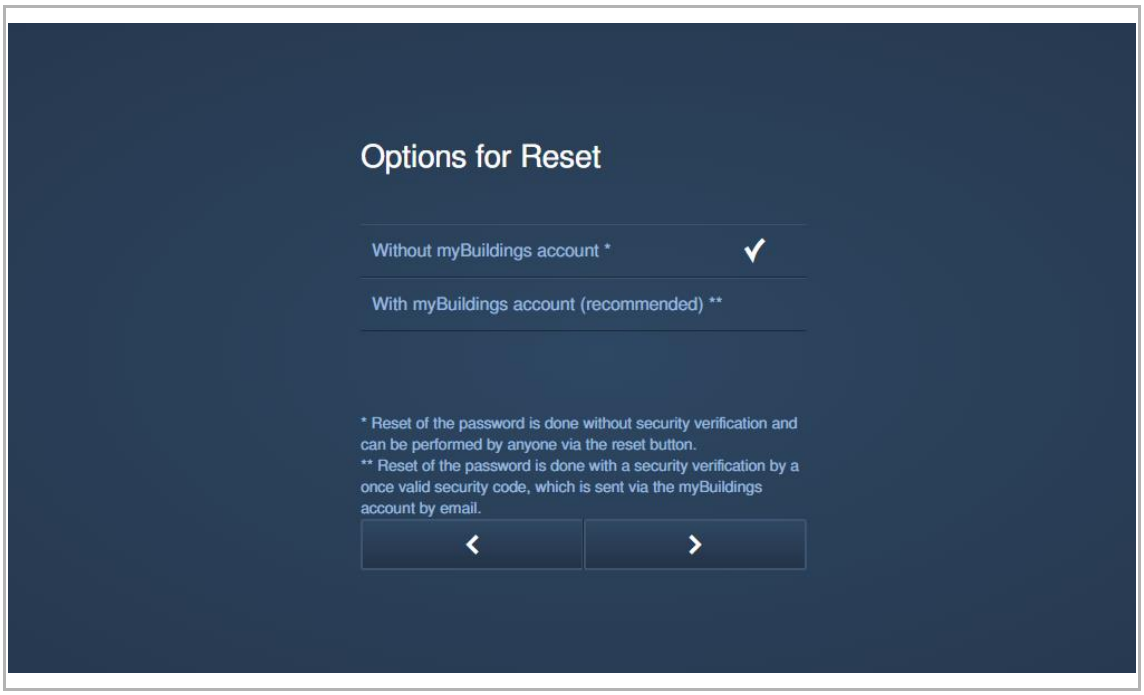
The first admin user cannot be deleted. It manages all other users.

If you want to reset the password for the first admin, see chapter 13.2 “Resetting the password for the primary admin“ on page 297.



10. Select reset option

You can select reset option according to the use scenario.



Reset option = Without MyBuildings account

- If this option is selected, anyone can reset the password for the first admin user by pressing the reset button.
- It is used for the scenario that "Smart Access Point" is installed in a private area and is not physically accessible to unauthorized users.

Reset option = With MyBuildings account

- If this option is selected, a one-time validity security code is needed when someone want to reset the password for the first admin user by pressing the reset button. And this security code will only be sent to the email set in the initial setup.
- It is used for the scenario that "Smart Access Point" is installed in a public area and is physically accessible to unauthorized users.

Attention!

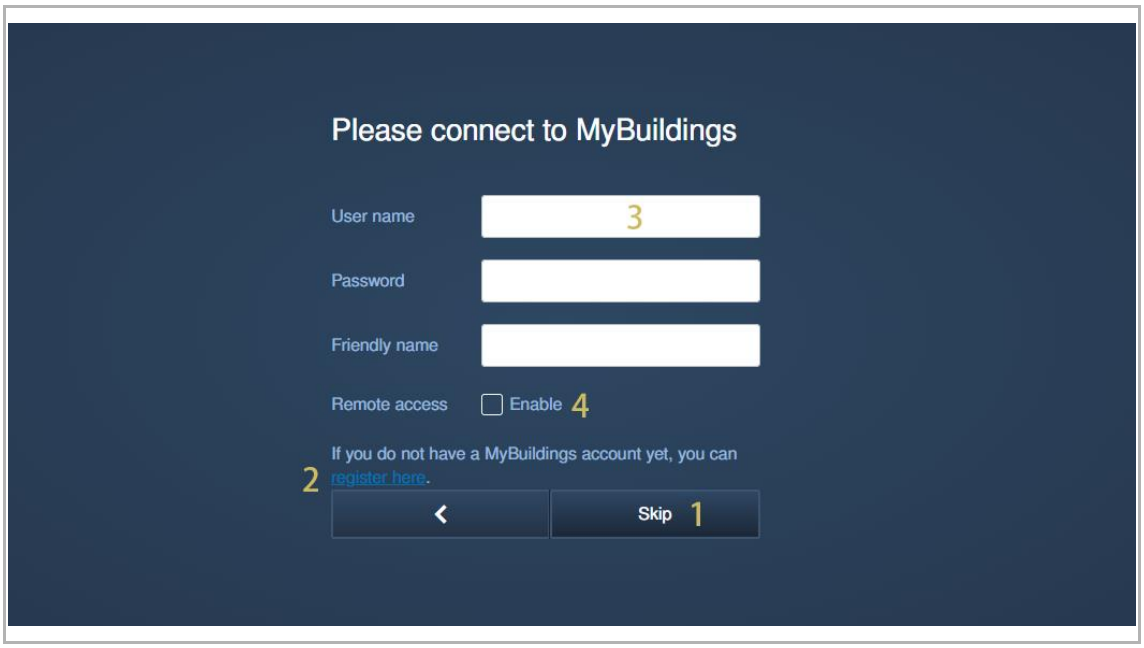
The reset option can only be set in the initial setup and cannot be changed after the initial setup.

The reset option can only be changed when you restore "Smart Access Point" to the factory defaults.

11. MyBuildings setting

Reset option = Without MyBuildings account

If the reset option is set to "Without MyBuildings account", you will access this screen.



[1] Click "Skip" to turn to next step if you don’t want to connect to MyBuildings currently.

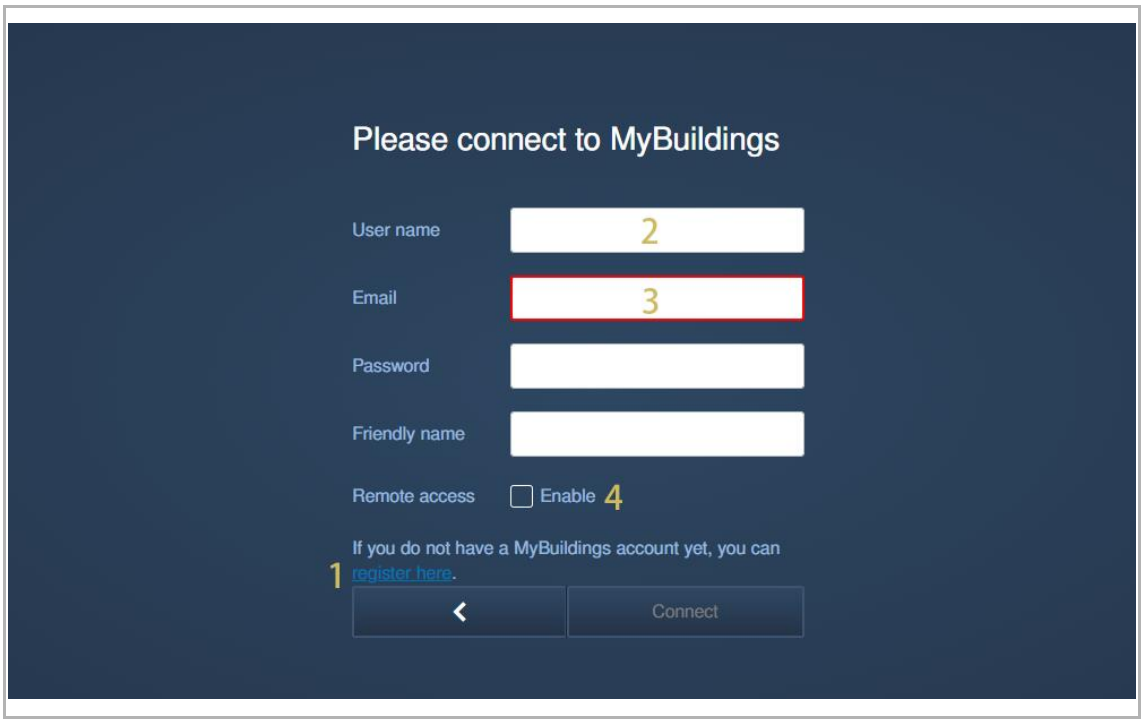
[2] Click "Register here" to access the MyBuildings portal to register an account. see chapter 13.1 “Registering an account on the myBUSCH-JAEGER portal“ on page 296.

[3] Enter the username, password and friendly name, followed by "Connect" to connect to MyBuildings portal.

[4] If you want to access "Smart Access Point" from the MyBuildings portal, you need to tick the "Enable" checkbox to enable the remote access function.

Reset option = With MyBuildings account

If the reset option is set to "With MyBuildings account", you will access this screen.



[1] Click "Register here" to access the MyBuildings portal to register an account. see chapter 13.1 “Registering an account on the myBUSCH-JAEGER portal“ on page 296.

[2] Enter the username, password and friendly name, followed by "Connect" to connect to MyBuildings portal.

[3] Enter the Email used to activate the MyBuildings account. This mail will receive a security code when you want to reset the first admin user. see chapter 13.2 “Resetting the password for the primary admin“ on page 297.

[4] If you want to access "Smart Access Point" from the MyBuildings portal, you need to tick the "Enable" checkbox to enable the remote access function.

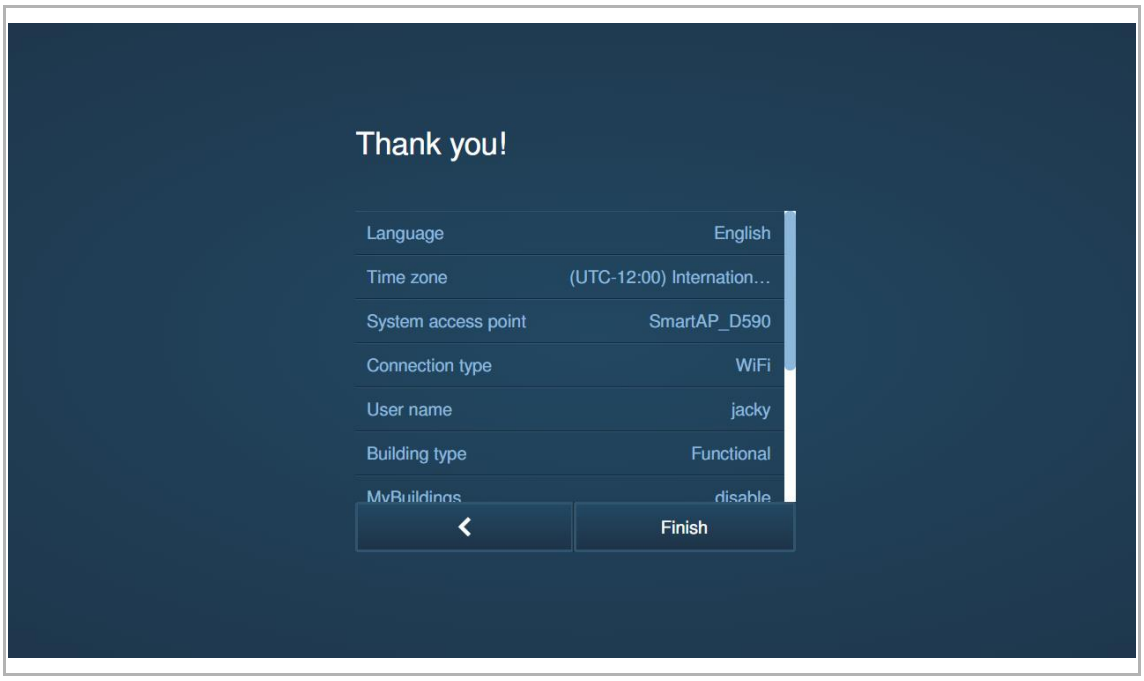
12. Set the device name

Enter the name for the device and this name will be displayed on the log in screen.

13. Confirm the settings

You can check all the settings again on the overview screen. You can click "<" to return to the previous screens to edit the settings.

Click "Finish" to complete the initial setup.

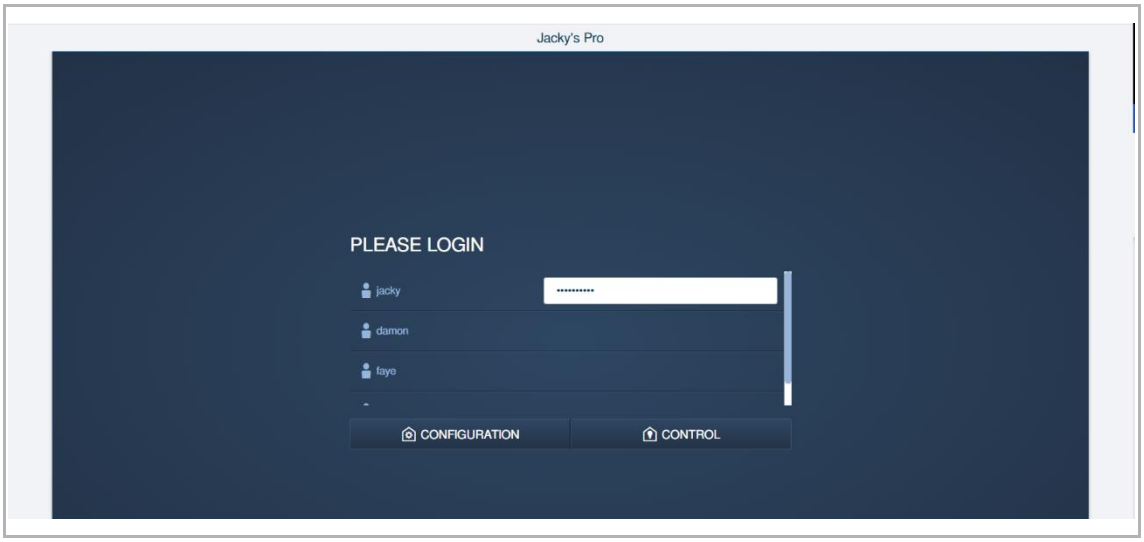


8.4 Login screen

After initial setup, you can access the login screen of "Smart Access Point" using the first admin user. The login screen will be different according to the number of users.

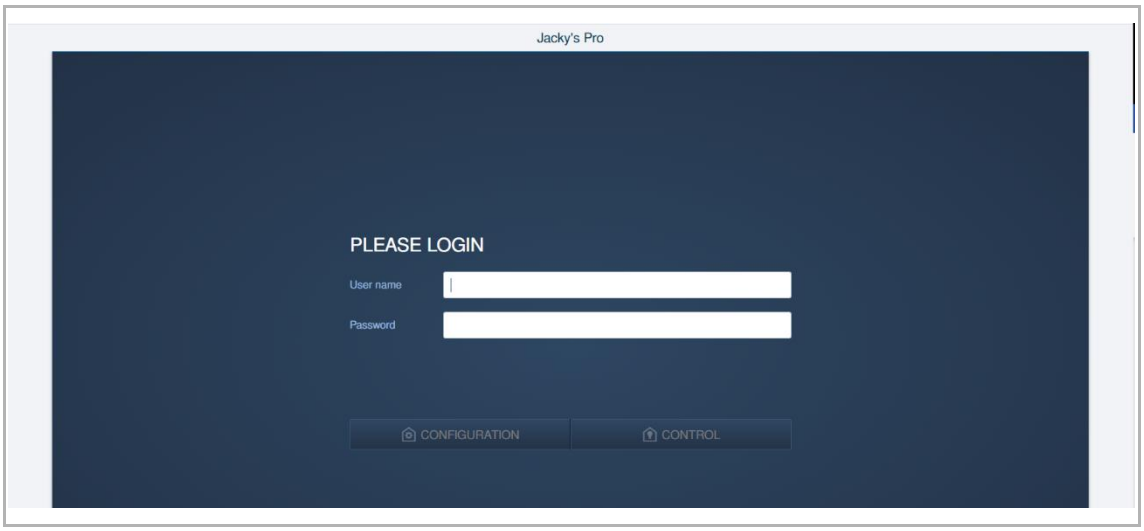
The number of users <6

If the number of users is <6, a name list is displayed on the screen. Enter the password on the right of the user name to continue.



The number of users ⩾6

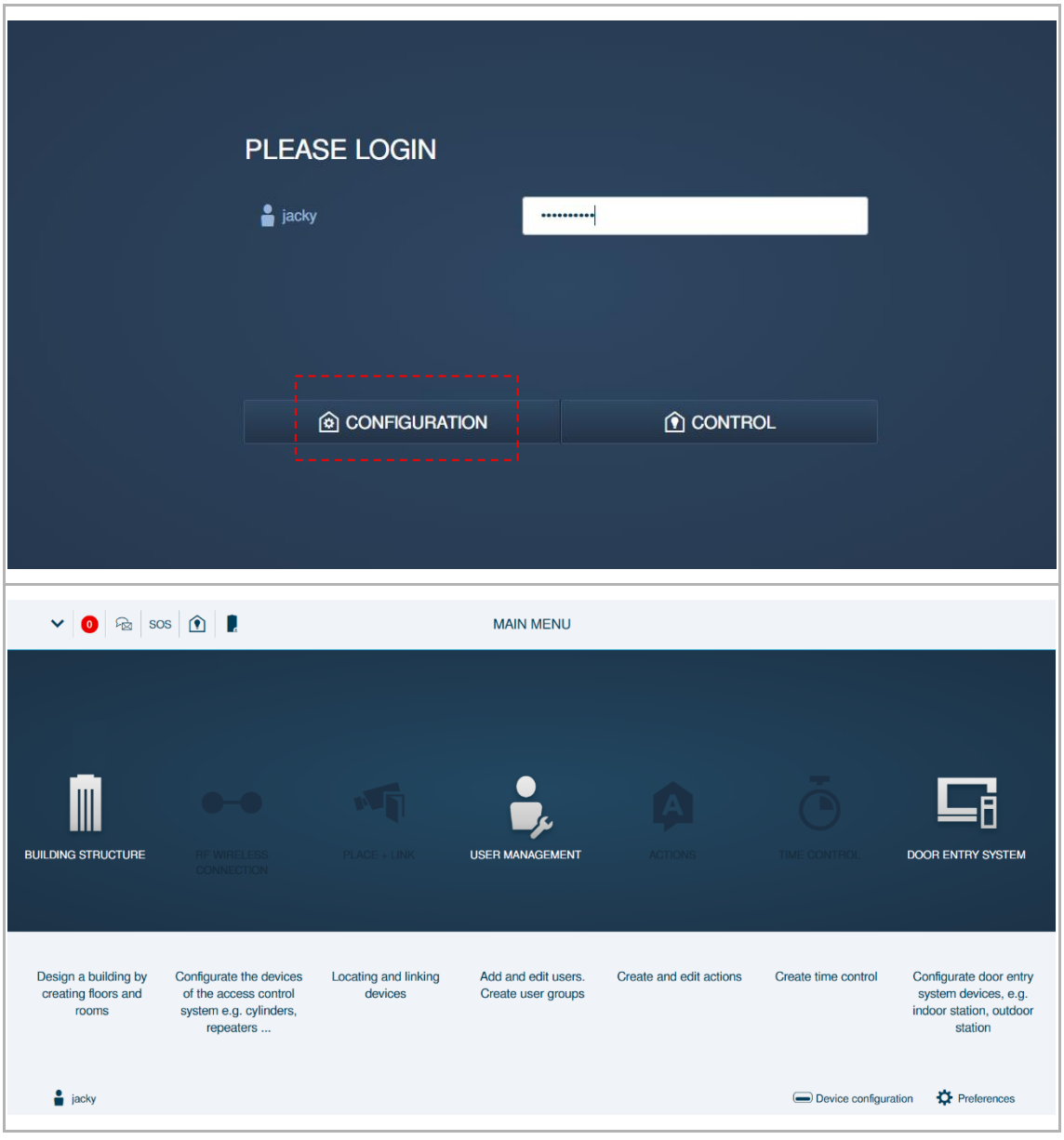
If the number of users is ⩾ 6, no name list is displayed on the screen. You need to enter the user name and the password to continue.



8.5 Configuration screen

The configuration screen is used to add and configure all devices and users.

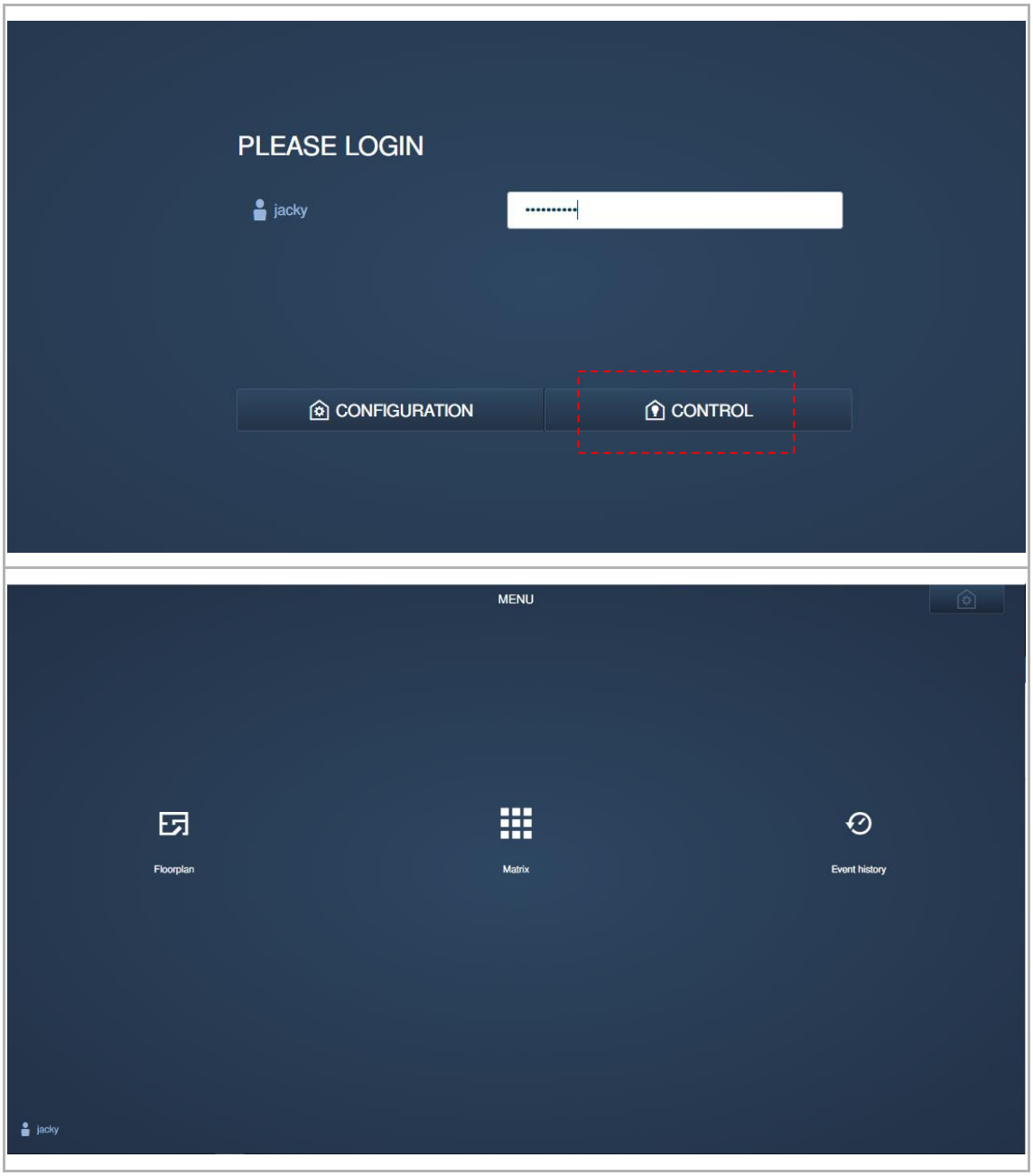
On the login screen, enter the password and click "Configuration" to access the configuration screen.



8.6 Control screen

The control screen is used to control the AccessControl devices.

On the login screen, enter the password and click "Control" to access the control screen.

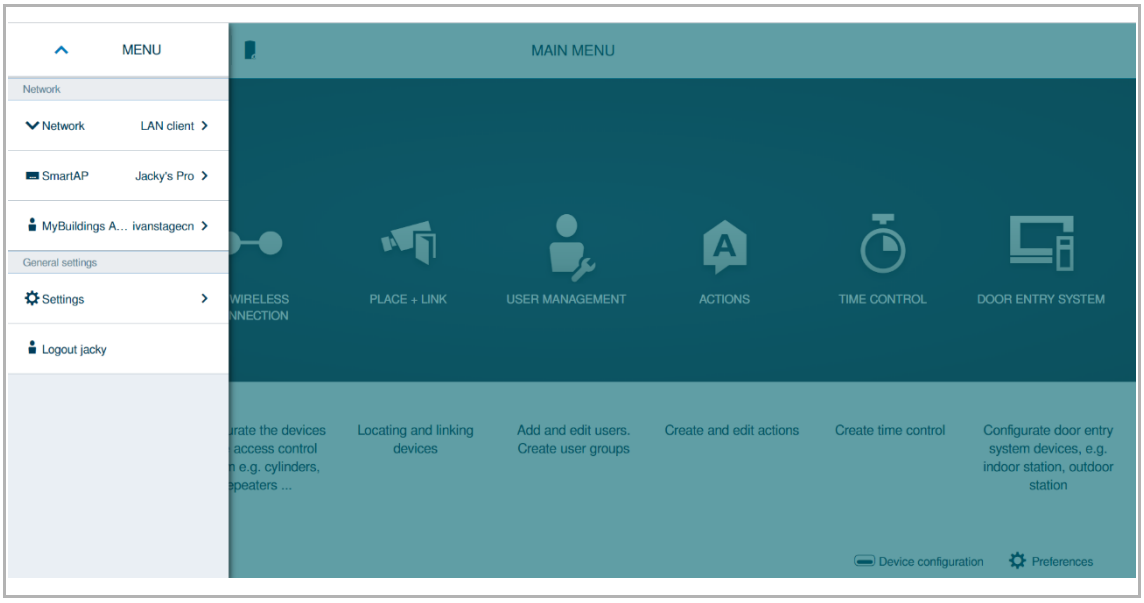


8.7 Settings

8.7.1 Accessing quick settings

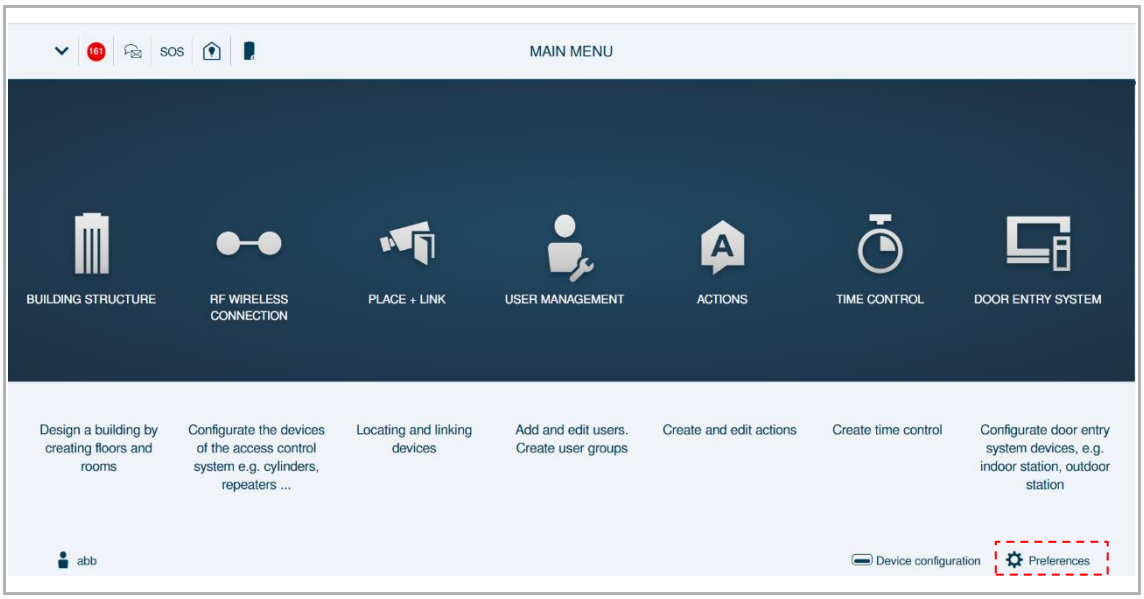
On the configuration screen, click "∨" to carry out some common operations:

- Setting the network (e.g. network mode and IP address)
- Check device status (e.g. device name, language, time zone and date/time)
- Setting the MyBuildings account (e.g. connect to MyBuildings portal, view the validity period of the license)
- General settings
- Logout from the account



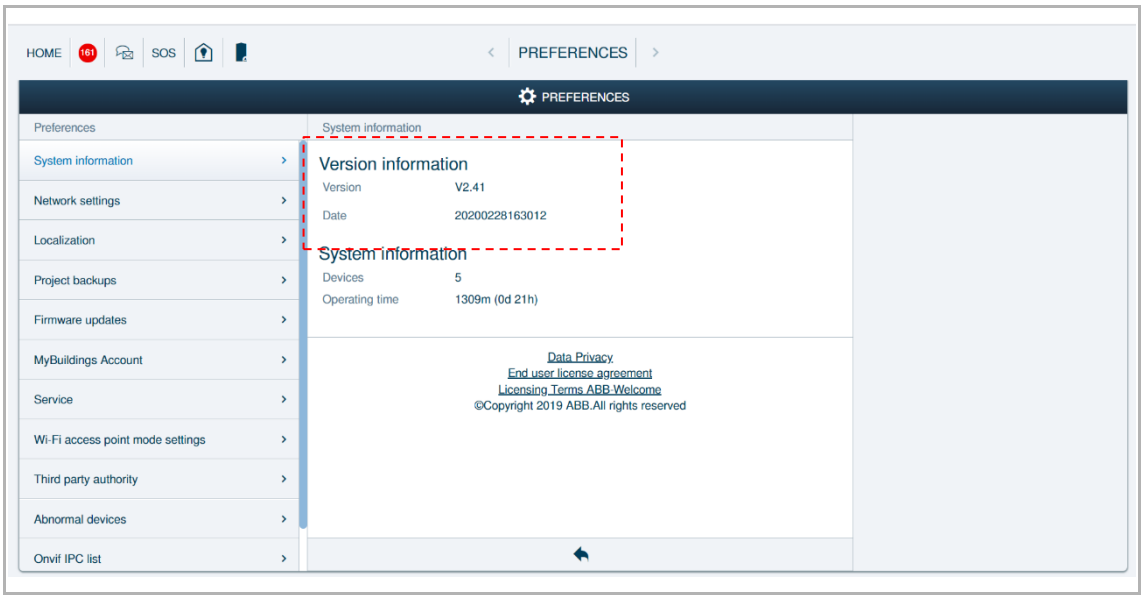
8.7.2 Accessing the "Preference" screen

On the configuration screen, click "Preferences" to access the corresponding screen.



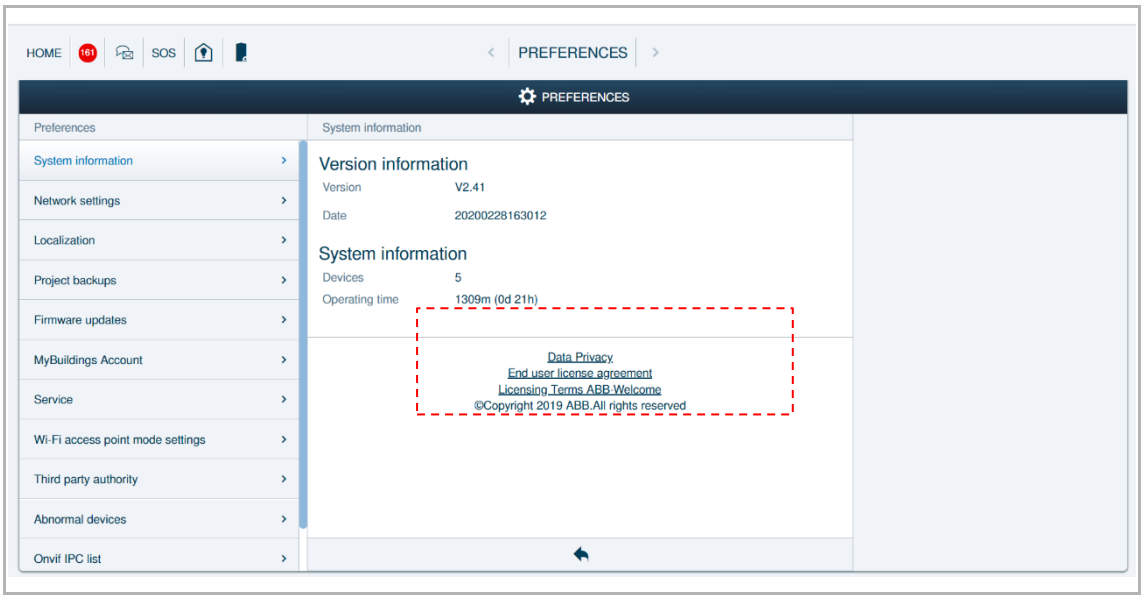
8.7.3 Viewing the version

On the "Preferences", "System information" screen, you can view the version information



8.7.4 Disclaimer information

On the "Preferences", "System information" screen, you can view the disclaimer information.

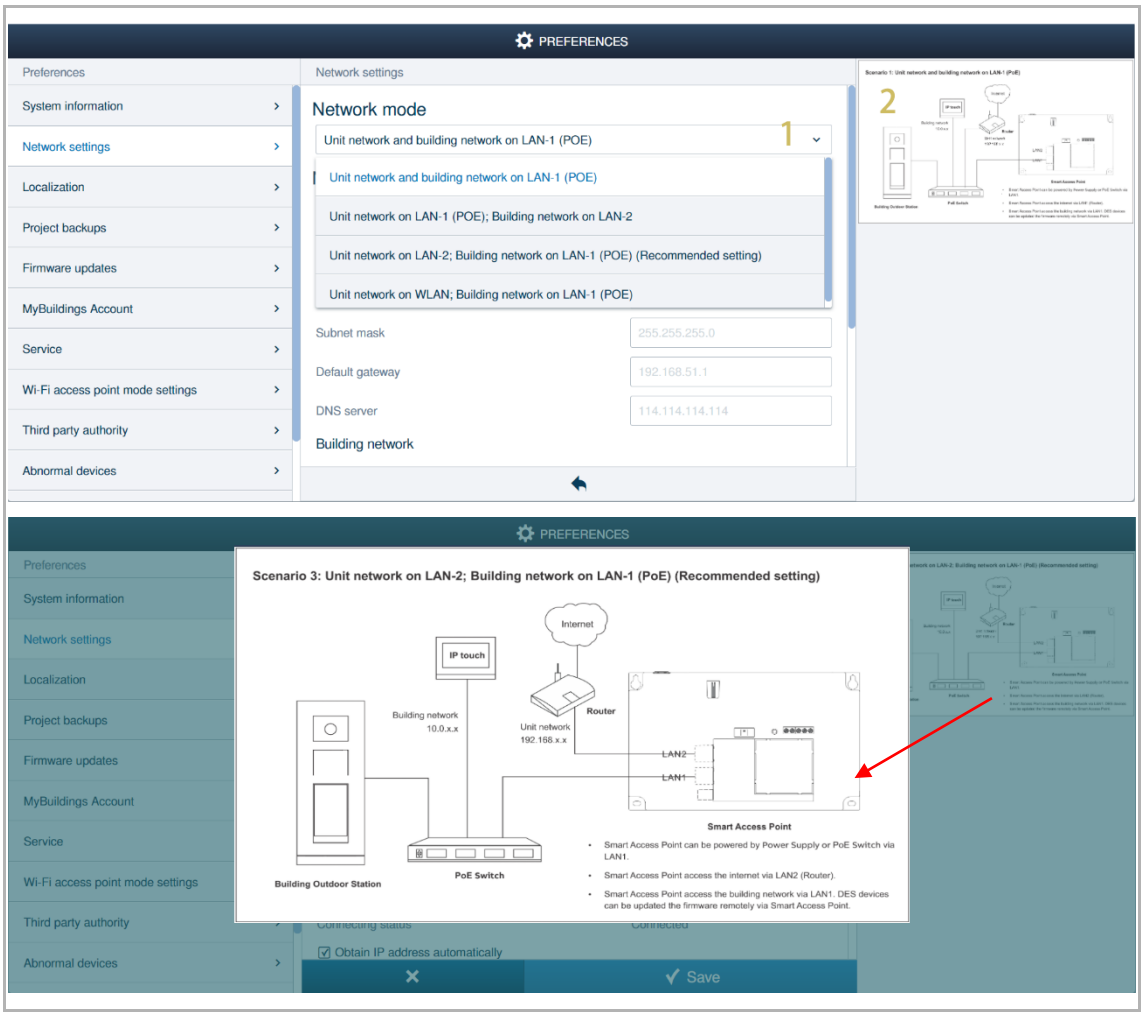


8.7.5 Network setting

On the "Preferences", "Network settings" screen, there are 4 options for selection.

[1] "Unit network and building network on LAN-1 (POE)" is used by default.

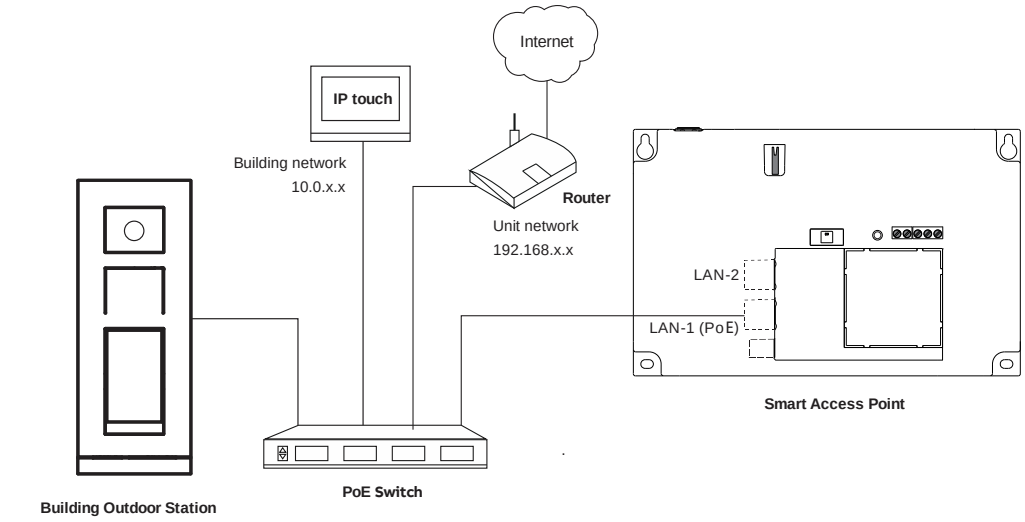
[2] Click the right diagram to view the zoom view.



1. Unit network and building network on LAN-1 (POE)

- Smart Access Point can be powered by Power Supply or PoE Switch via LAN-1 (PoE).
- Smart Access Point access the internet via LAN-1 (PoE).
- Smart Access Point access the building network via LAN-1 (PoE). DES devices can be updated the firmware remotely via Smart Access Point.

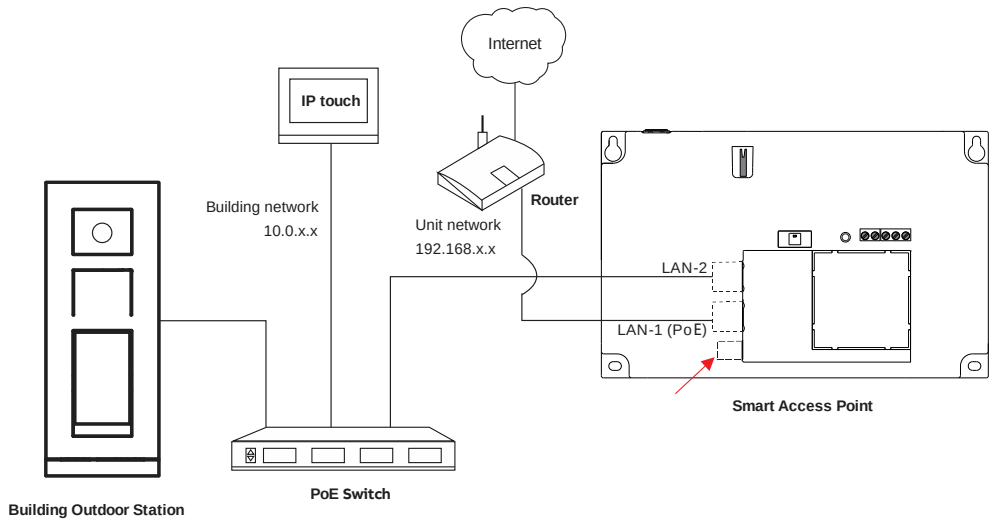
Scenario 1: Unit network and building network on LAN-1 (PoE)



2. Unit network on LAN-1 (POE); Building network on LAN-2

- Smart Access Point can be powered by Power Supply.
- Smart Access Point access the internet via LAN-1 (PoE).
- Smart Access Point access the building network via LAN-2. DES devices can be updated the firmware remotely via Smart Access Point.

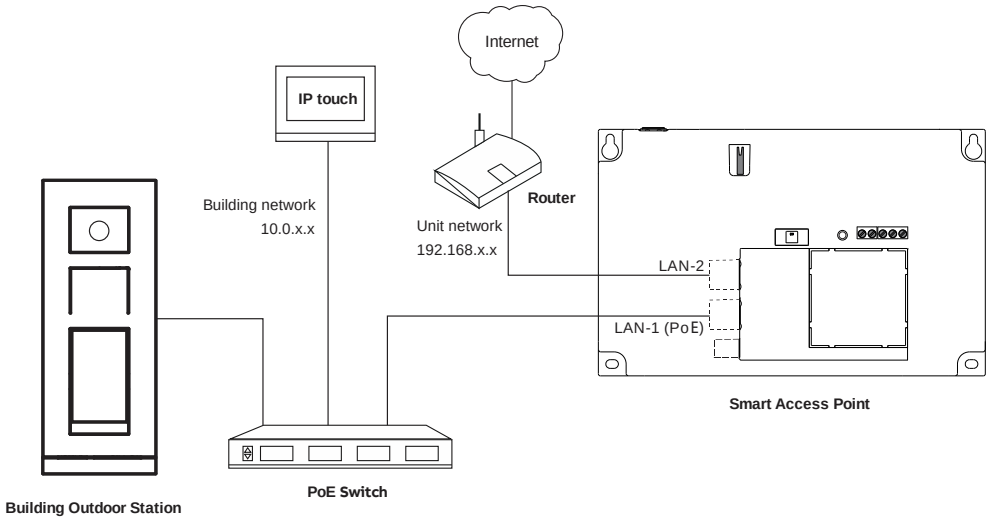
Scenario 2: Unit network on LAN-1 (PoE); Building network on LAN-2



3. Unit network on LAN-2; Building network on LAN-1 (POE) (Recommended setting)

- Smart Access Point can be powered by Power Supply or PoE Switch via LAN-1 (PoE).
- Smart Access Point access the internet via LAN-2.
- Smart Access Point access the building network via LAN-1 (PoE). DES devices can be updated the firmware remotely via Smart Access Point.

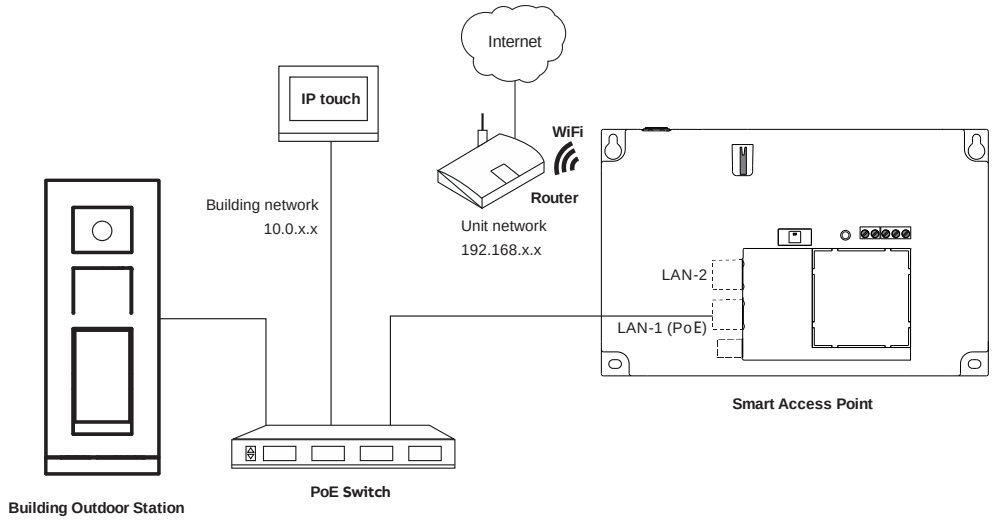
Scenario 3: Unit network on LAN-2; Building network on LAN-1 (PoE) (Recommended setting)



4. Unit network on WLAN; Building network on LAN-1 (POE)

- Smart Access Point can be powered by Power Supply or PoE Switch via LAN-1 (PoE).
- Smart Access Point access the internet via WiFi (Router).
- Smart Access Point access the building network via LAN-1 (PoE). DES devices can be updated the firmware remotely via Smart Access Point.

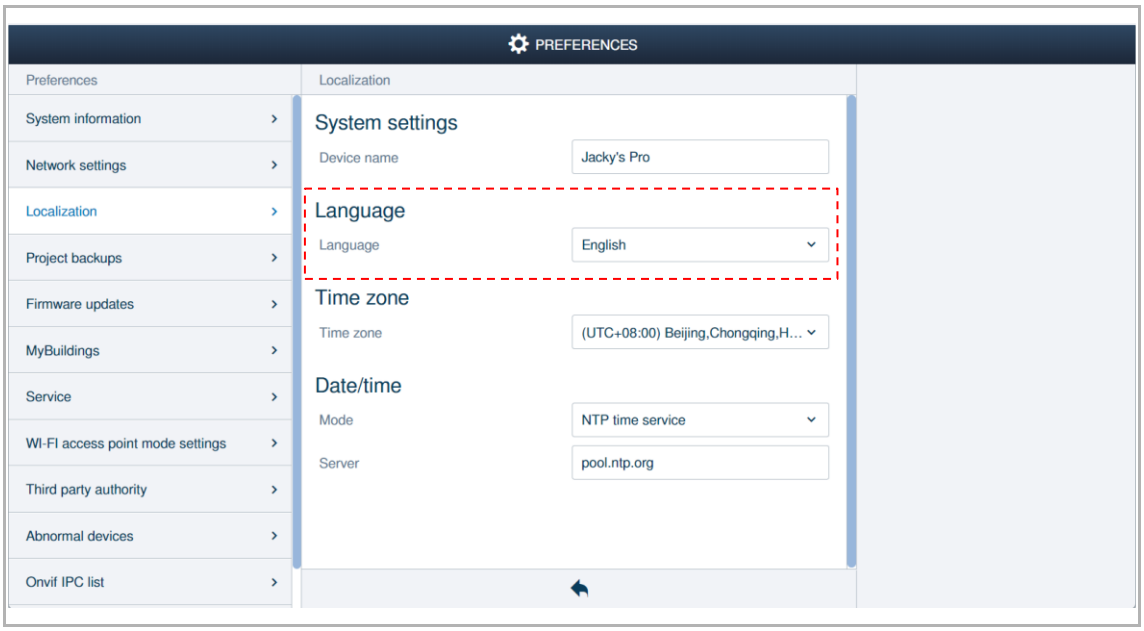
Scenario 4: Unit network on WLAN; Building network on LAN-1 (PoE)



see chapter 8.3 “Initial setup“ on page 26

8.7.6 Language setting

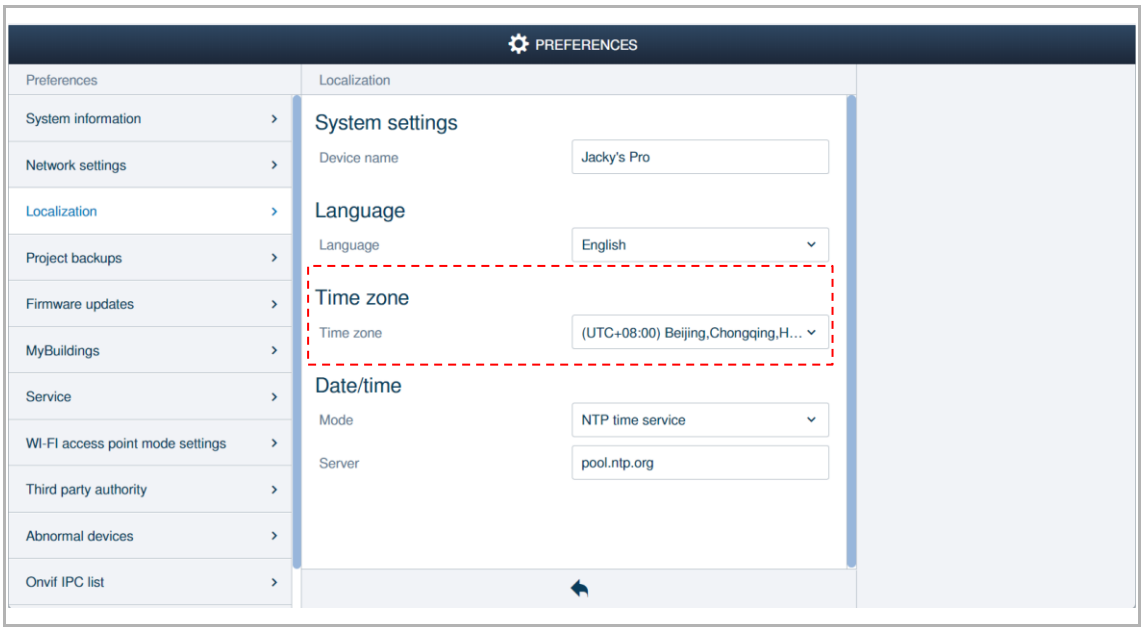
On the "Preferences", "Localization" screen, select the language from the drop-down list.



8.7.7 Time settings

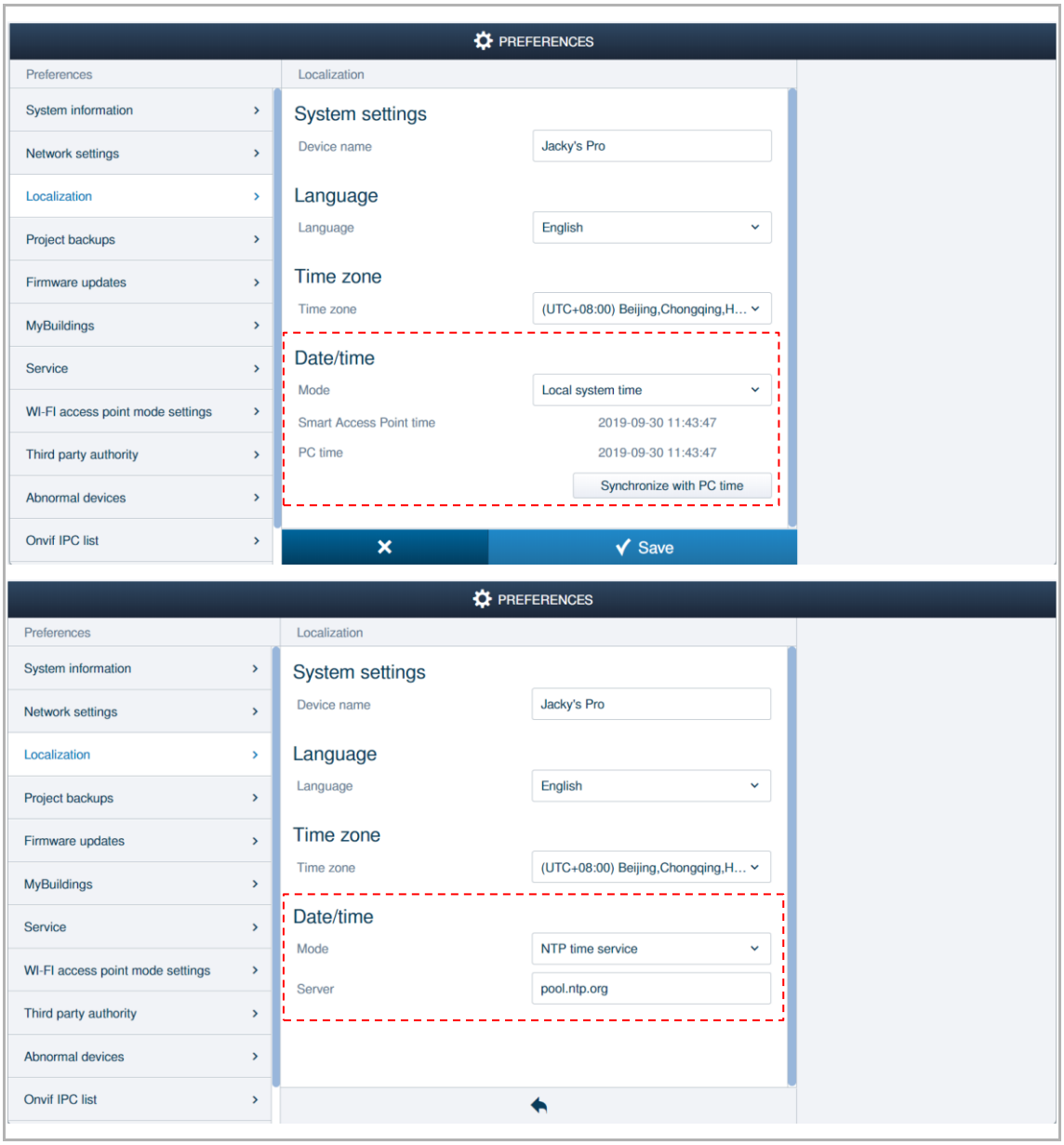
Time zone setting

On the "Preferences", "Localization" screen, select time zone from the drop-down list



Sync "Smart Access Point" time with local system or NTP server

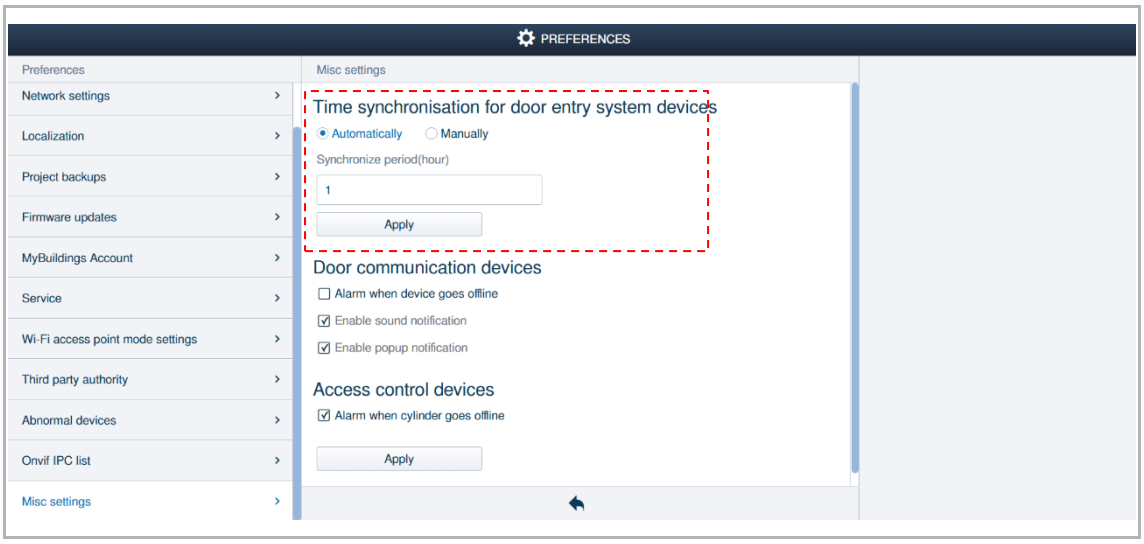
On the "Preferences", "Localization" screen, "Smart Access Point" time can be set to sync from "Local system time" or from "NTP time service".



Sync "Smart Access Point" time with Door Entry System devices

Note
This function is only used for Door Entry System devices.

On the "Preferences", "Misc settings" screen, you can select "Automatically" to sync "Smart Access Point" time with other devices on the system regularly. You need to click "Apply" before the change is effective.

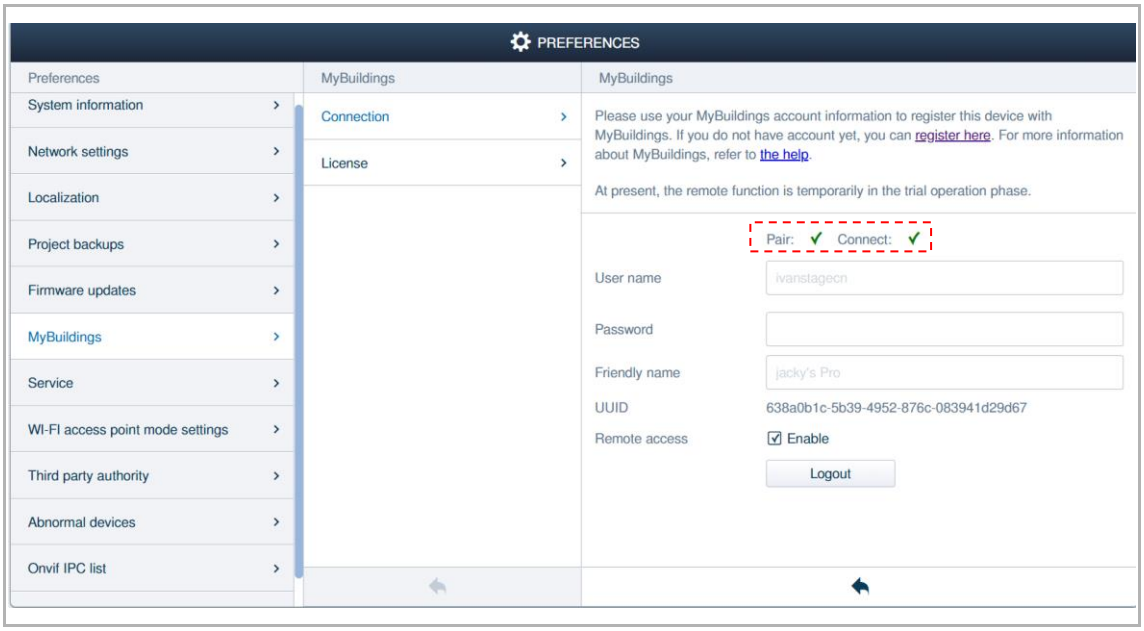


8.7.8 MyBuildings settings

"Pair" is displayed when the account and password are correct.

"Connect" is displayed when "Smart Access Point" is connected to the MyBuildings portal successfully.

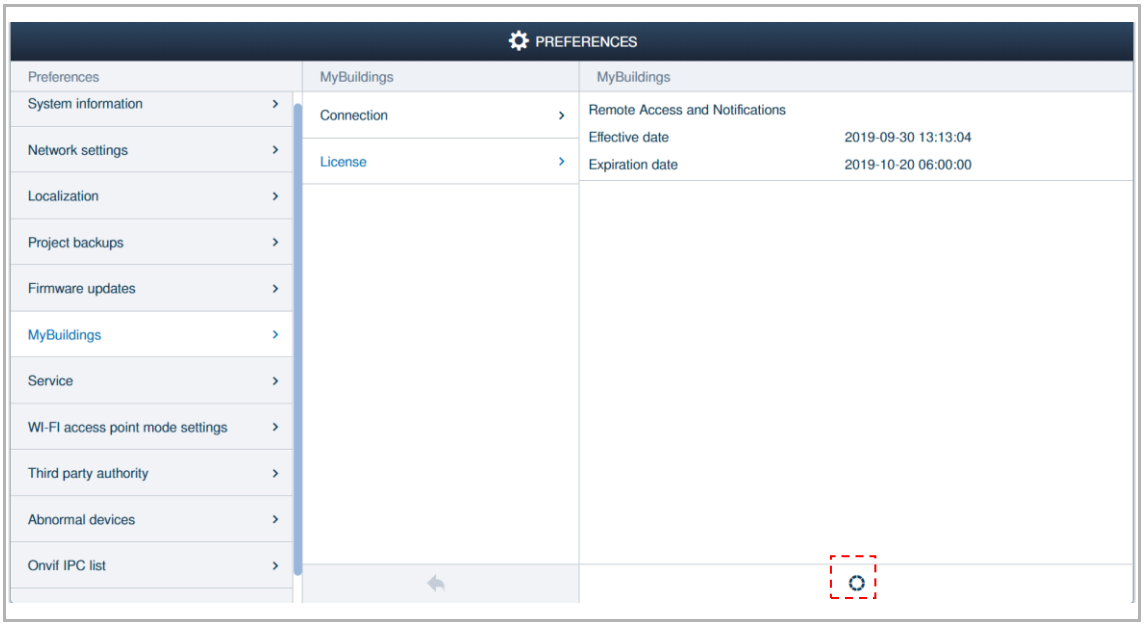
If "Remote access" is enabled, you can access "Smart Access Point" on the MyBuildings portal. But you need to subscribe to the "Remote access" service on the MyBuildings portal before this function is used.



Refresh the license

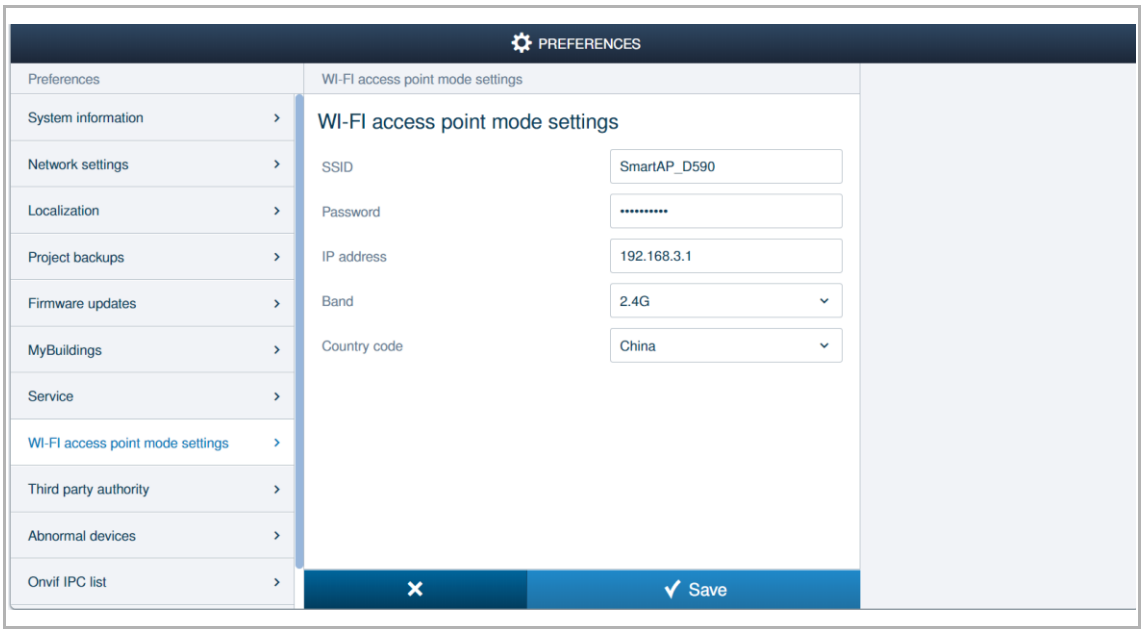
You can refresh the license after the remote service is subscribed.

On the "Preferences", "MyBuildings", "License" screen, click " ○ " to refresh the license.



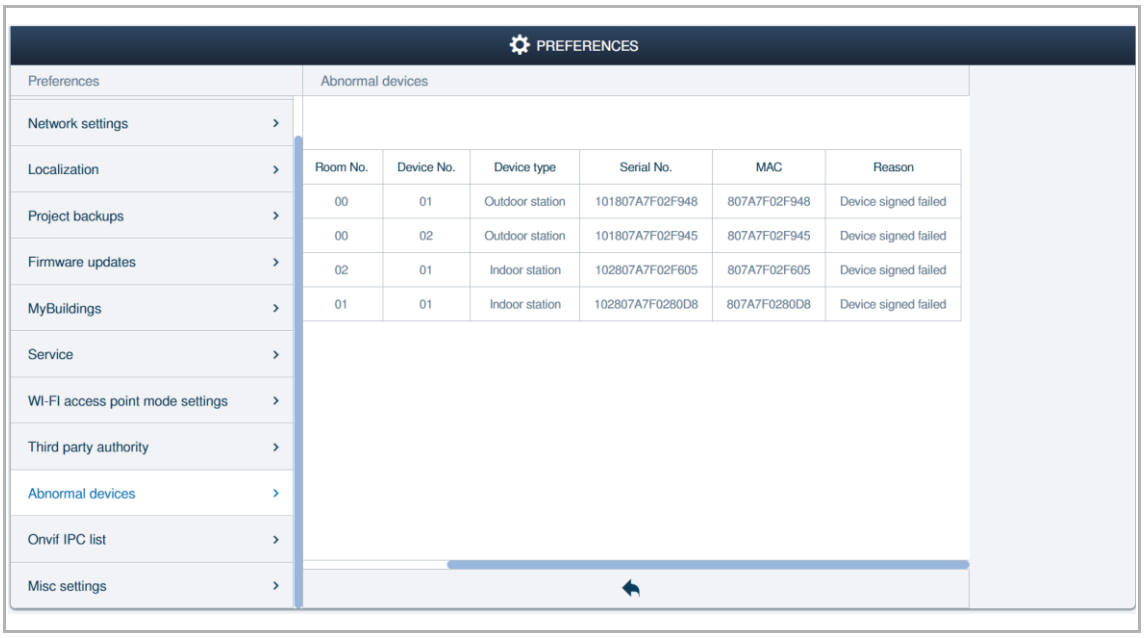
8.7.9 WiFi Access Point mode settings

On the "Preferences", "Wi-Fi Access Point mode settings" screen, you can change the WiFi Access Point mode settings.



8.7.10 Abnormal devices

On the "Preferences", "Abnormal devices" screen, you can view the details of abnormal devices (e.g. device sign failed, communication failed etc.).



You can check the device when "Device signed failed" appears on the abnormal devices list.

- Has the device been signed before?
- Does the device work in safety mode?
- Does the IP address of the device conflict with other devices?

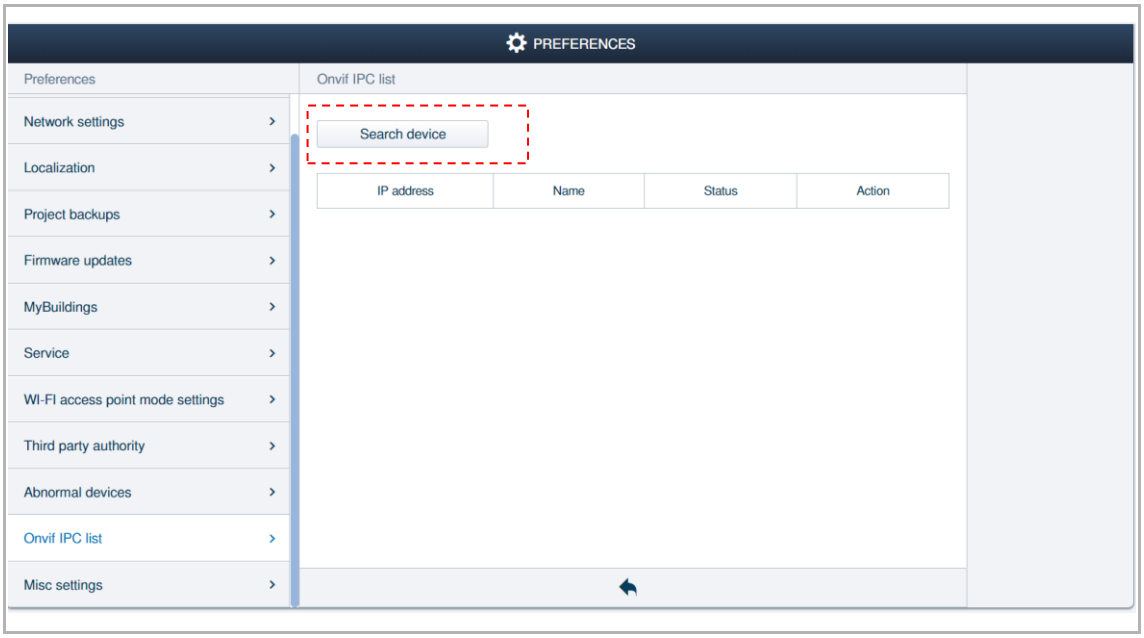
8.7.11 Onvif IP-Camera settings

Following settings need to be adjusted on your IP-Camera (Please check the manual of your IP-Camera).

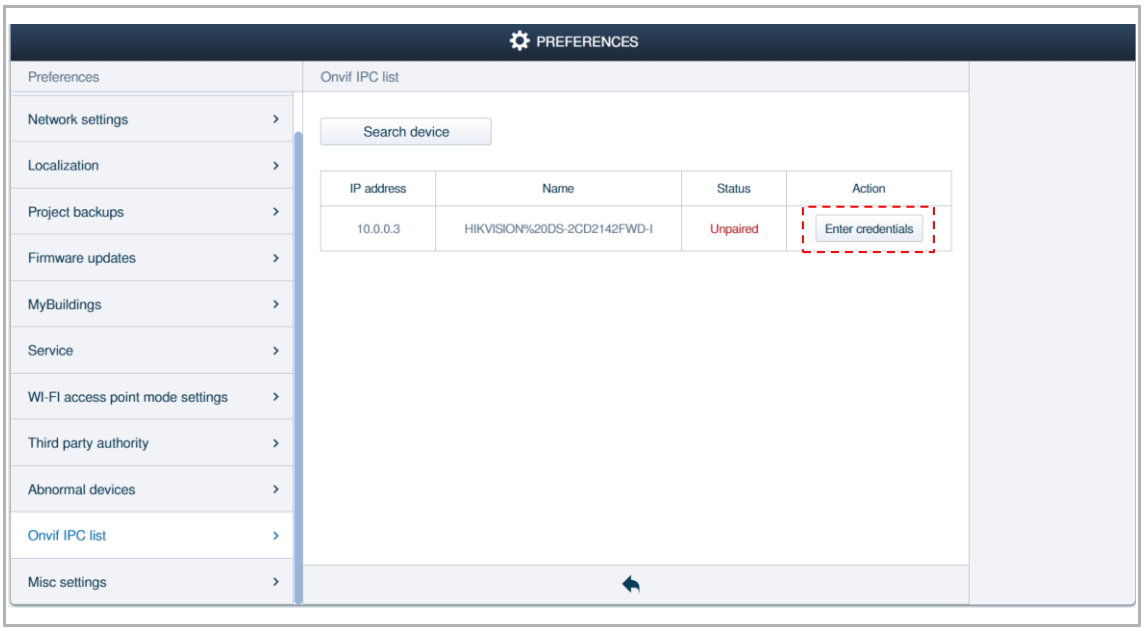
Protocol	Set as "ONVIF" or "ONVIF Profile S"
Video Encoding Type	Set as "H.264"
Resolution	Set to max. 1920x1080 (1080p)

For IP cameras the following addresses can be assigned in the community/functional network: - 10.0.3.1 … 10.0.3.254. In this address range also other devices, such as a computer, can use the 10-type addresses without coming into conflict with the ABB-Welcome IP address range.

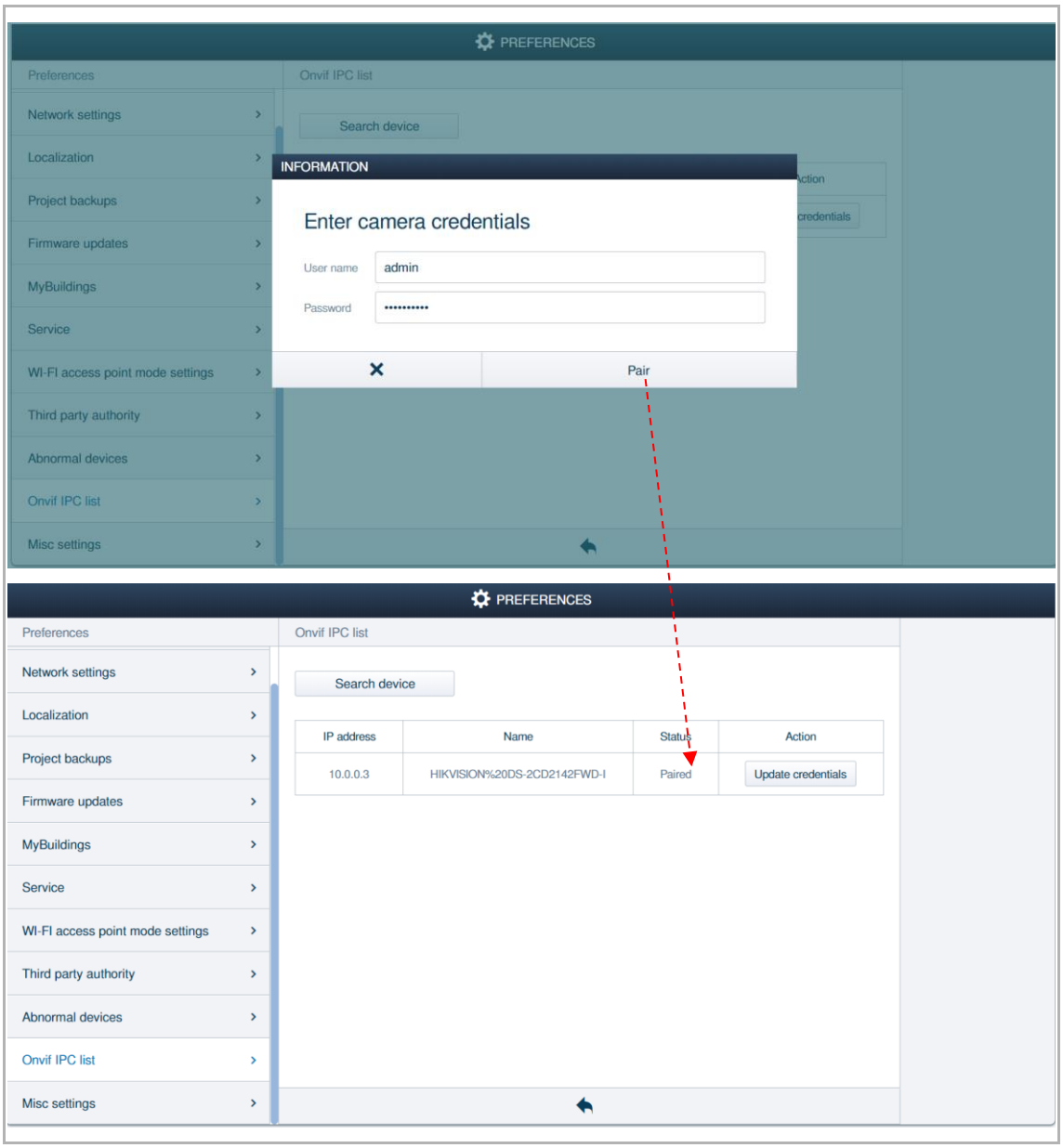
On the "Preferences", "Onvif IPC list" screen of "Smart Access Point", click "Search device" to search the IP-camera used for the public network.



Then click "Enter credentials" after the IP-camera is detected.

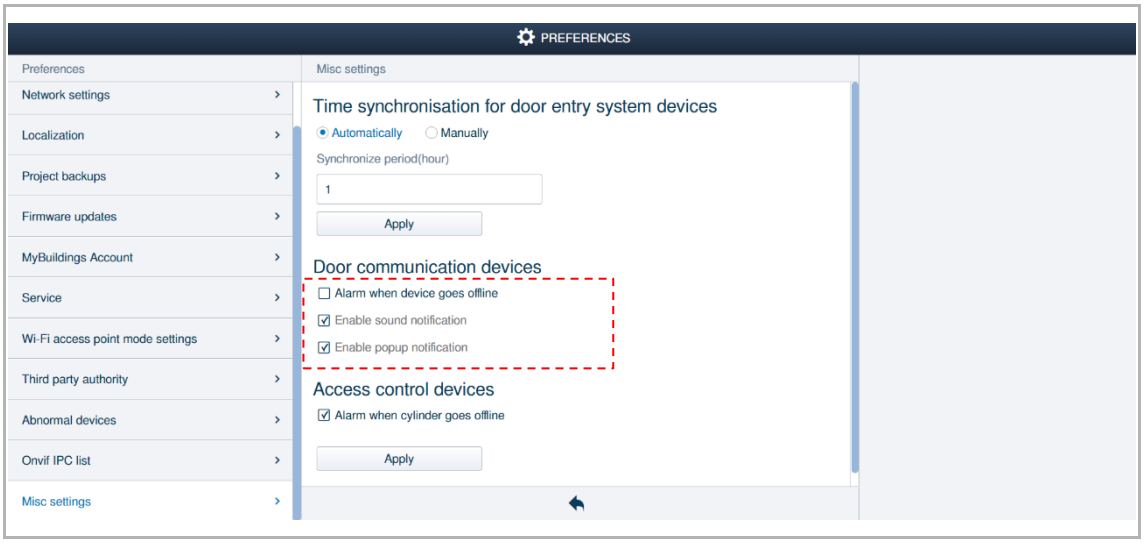


Enter the username and the password of the IP-camera, then click "Pair".



8.7.12 Alarm notification settings

On the "Preferences", "Misc settings" screen, the sound notification and popup notification are only available when the "Alarm when device goes offline" function is enabled.



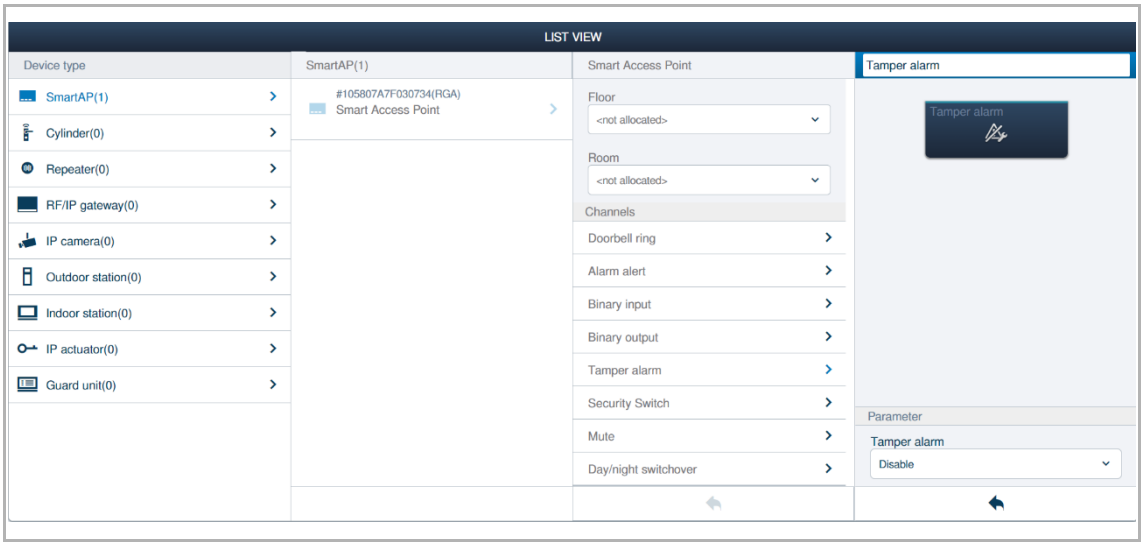
Note

The alarm is reported via outdoor station 1 (device ID=1) or via gate station 1 (device ID=1). If either of these two devices cannot be detected in the system, the alarm cannot be reported to "Smart Access Point" successfully.

8.7.13 Configuring "Smart Access Point"

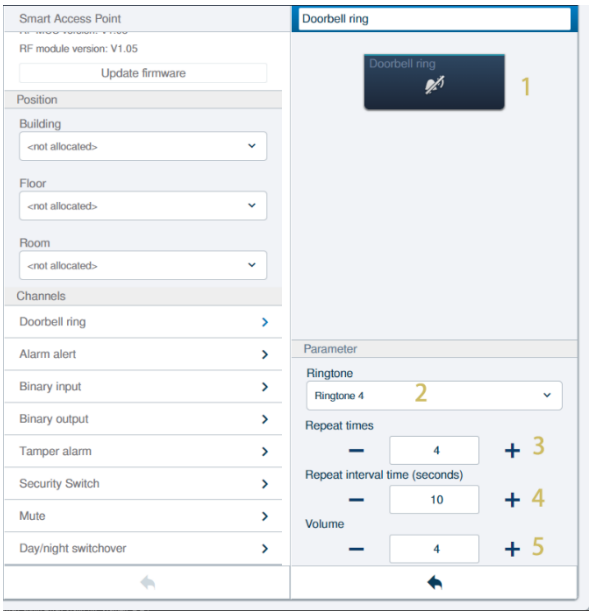
Access the setting screen

On the configuration screen, click "Device configuration", "SmartAP", designated "Smart Access Point" to access the configuration screen.



Doorbell ring

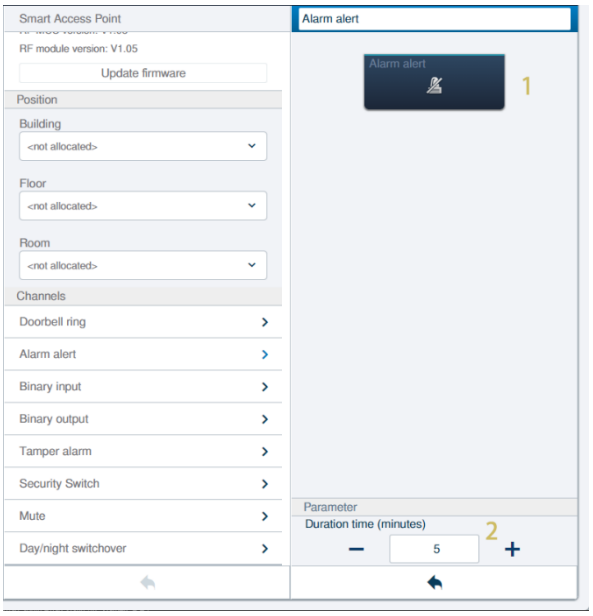
On the settings screen, click "Doorbell ring" to access the corresponding screen.



No.	Description
1	**Icon** Display the status of the channel. It can be triggered manually by pushing the icon.
2	**Ringtone** Click the drop-down list to select the ringtones for the "Smart Access Point" doorbell (built-in 4 ringtones).
3	**Repeat times** Adjust the repeat times of the ring tone.
4	**Repeat interval time (seconds)** Adjust the interval time of the ring tone.
5	**Volume** Adjust the volume of the ringtone.

Alarm alert

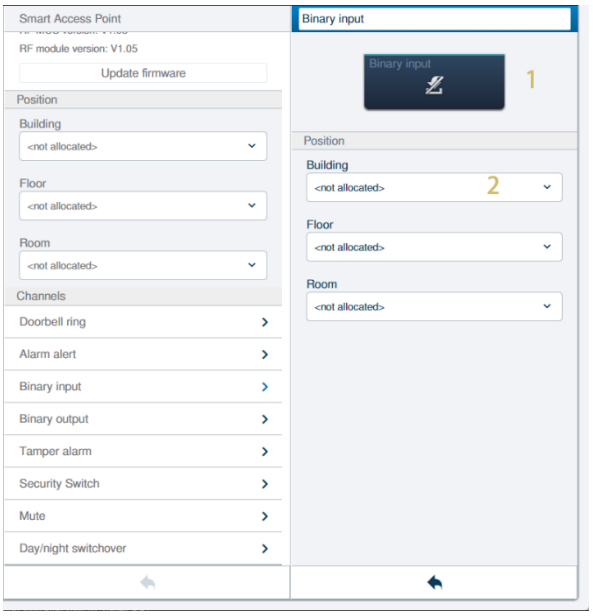
On the settings screen, click "Alarm alert" to access the corresponding screen.



No.	Description
1	**Icon** Display the status of the channel. It can be triggered manually by pushing the icon.
2	**Duration time (minutes)** Time duration of the alarm alert.

Binary input

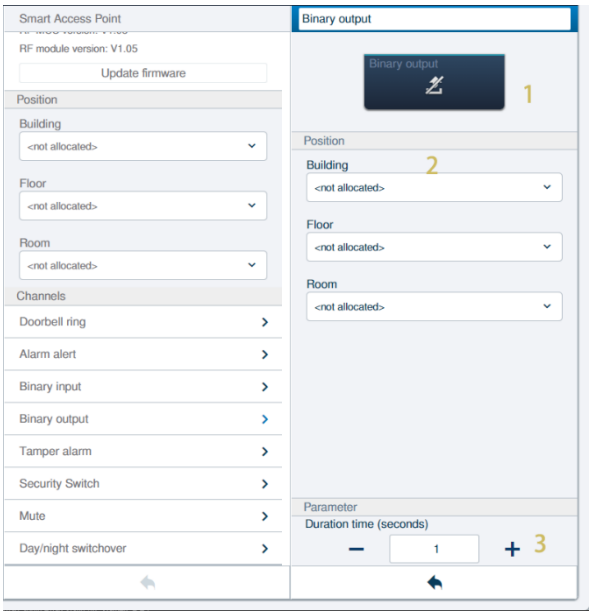
On the settings screen, click "Binary input" to access the corresponding screen.



No.	Description
1	**Icon** Display the status of the channel.
2	**Position** Assign the sensor connected to the binary input to the building structure (building, floor, room).

Binary output

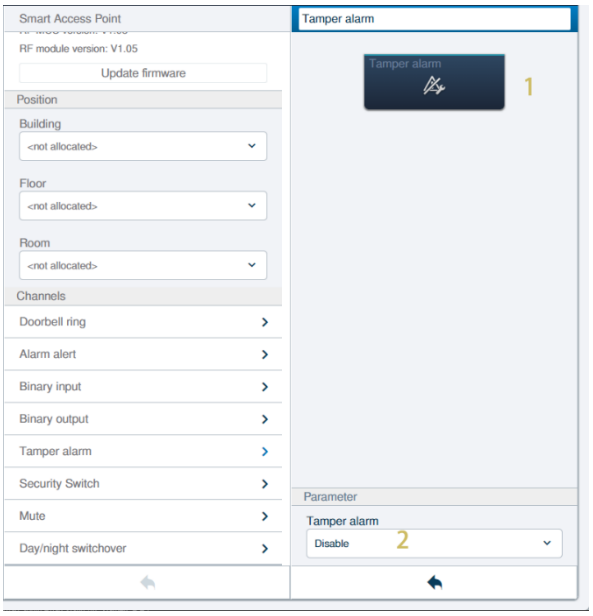
On the settings screen, click "Binary output" to access the corresponding screen.



No.	Description
1	**Icon** Display the status of the channel.
2	**Position** Assign the sensor connected to the binary input to the building structure (building, floor, room).
3	**Duration time (seconds)** Time duration of the binary output.

Tamper alarm

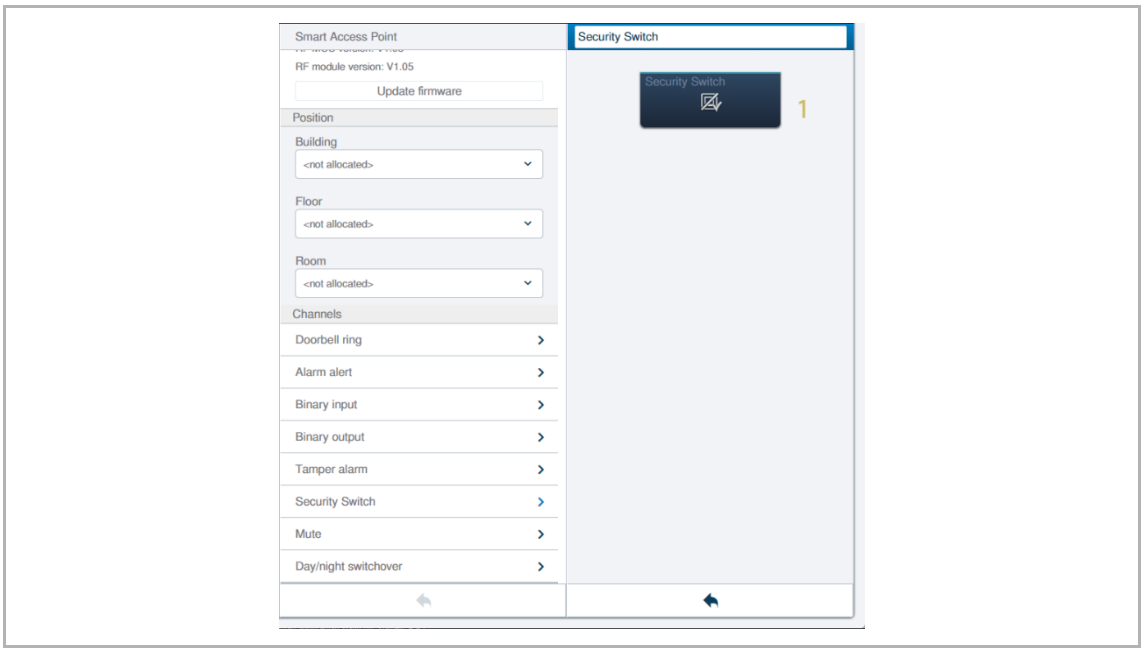
On the settings screen, click "Tamper alarm" to access the corresponding screen.



No.	Description
1	**Icon** Display the status of the channel.
2	**Enable/disable the function** Click the drop-down list to enable/disable the function.

Security switch

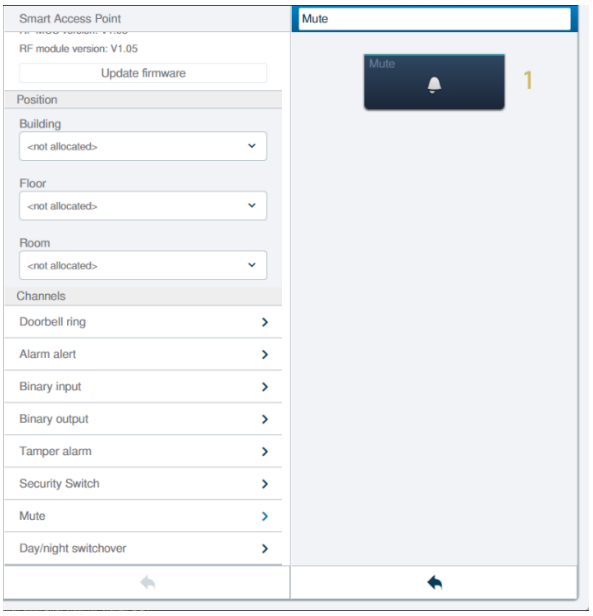
On the settings screen, click "Tamper alarm" to access the corresponding screen.



No.	Description
1	**Icon** Display the status of the channel.

Mute

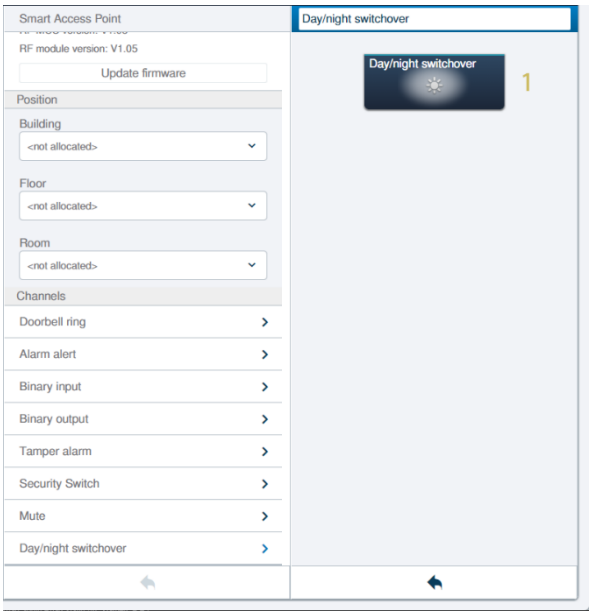
On the settings screen, click "Mute" to access the corresponding screen.



No.	Description
1	**Icon** Display the status of the channel. It can be triggered manually by pushing the icon.

Day/night switchover

On the settings screen, click "Day/night switchover" to access the corresponding screen.

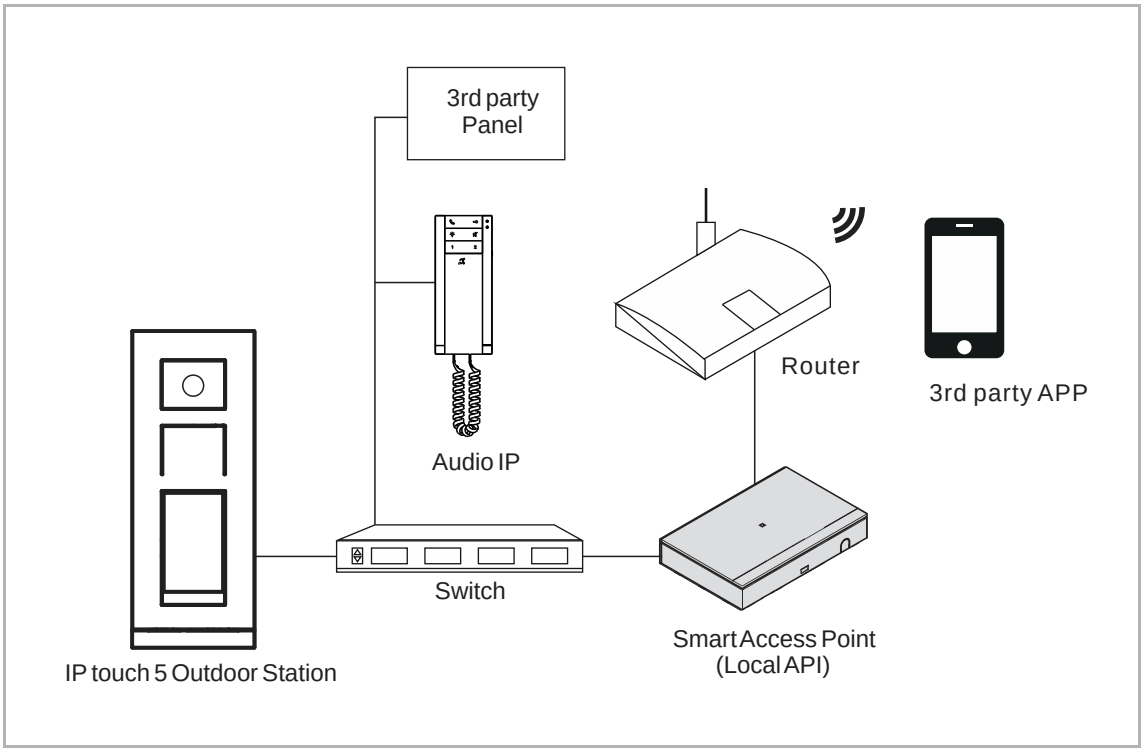


No.	Description
1	**Icon** Display the status when it is day or when it is night. The day and night switch is triggered by the internal astro function.

8.8 Configuring Welcome IP API

8.8.1 Configuring local API

Topology



Precondition

- Ensure the version of "Smart Access Point" should be 6.36 or above.
- Local API is enabled.
- A local API user is created.

Enable local API

Please follow the steps below:

[1] On the "Preference" screen, click "Connections & APIs" to access the corresponding screen.

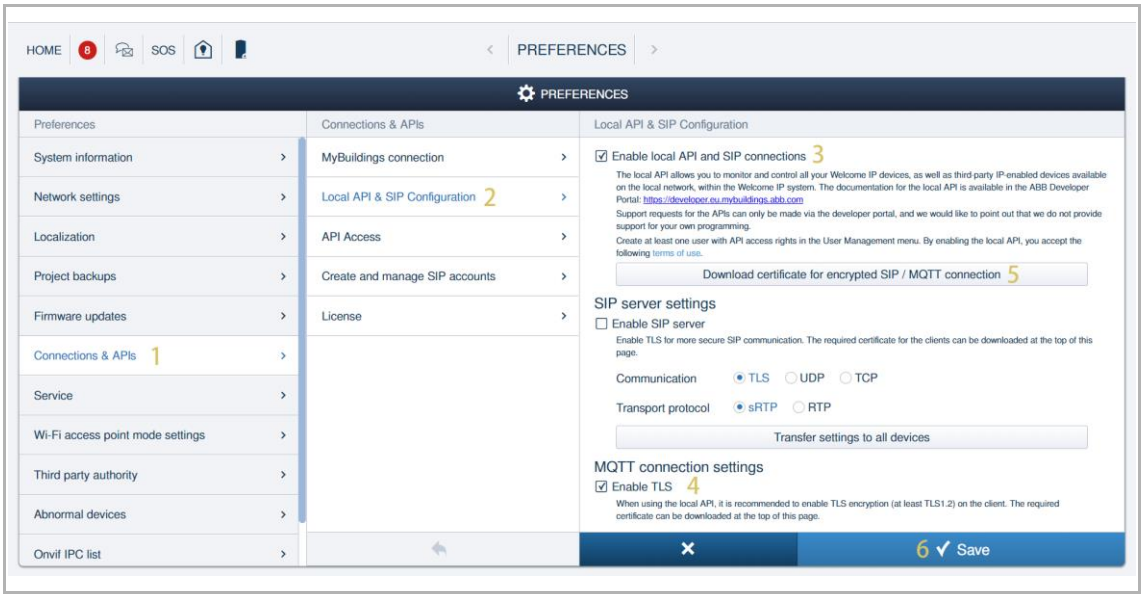
[2] Click "Local API & SIP Configuration".

[3] Tick the check box to enable the local API function.

[4] It is recommended to tick the check box to enable TLS encryption. [5] If "Enable TLS" is activated, please download the certificate for encryption.

[6] Click "Save".

If communication security is not considered, step 4 and step 5 can be ignored.



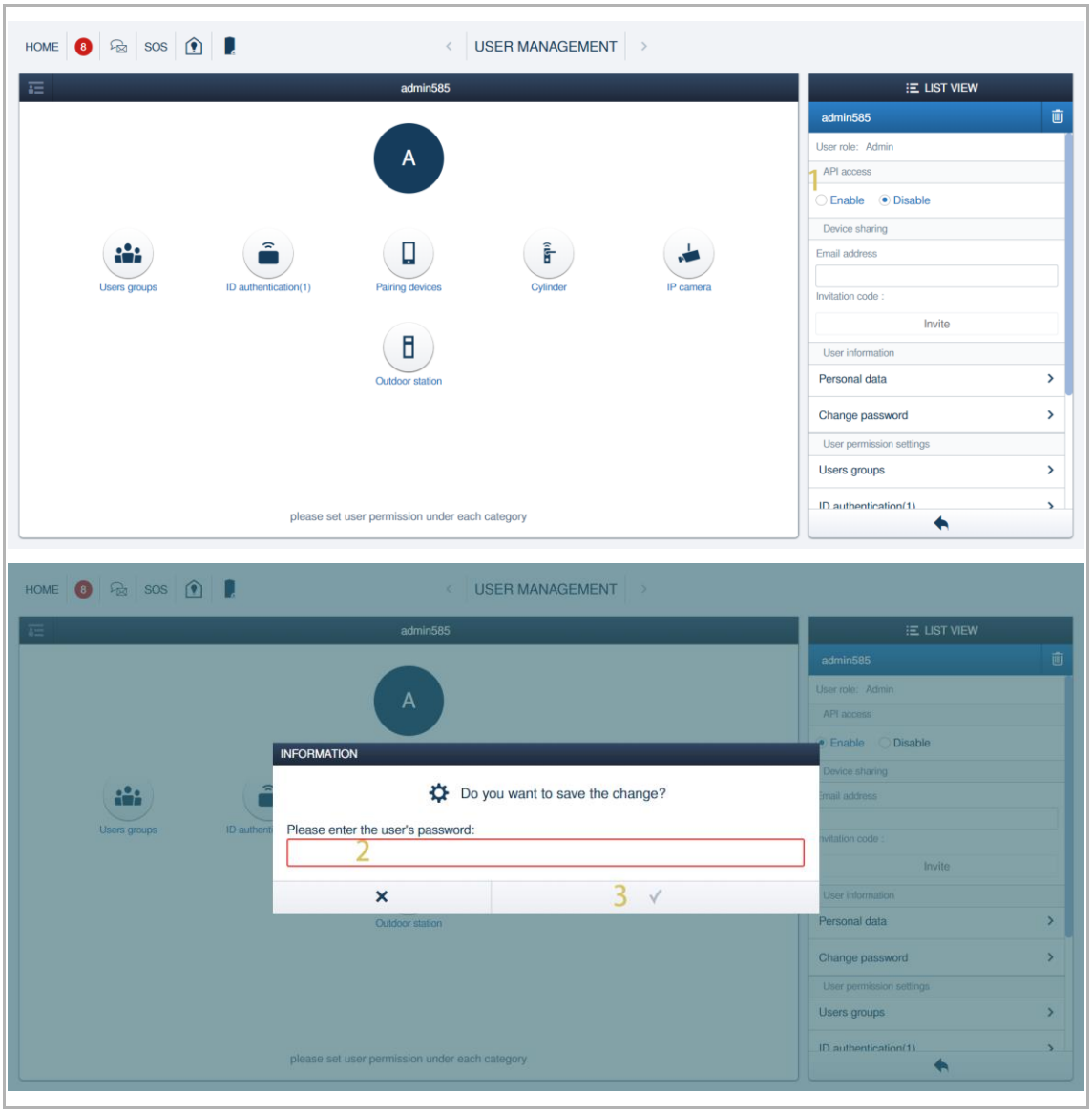
Create a local API user

Please follow the steps below:

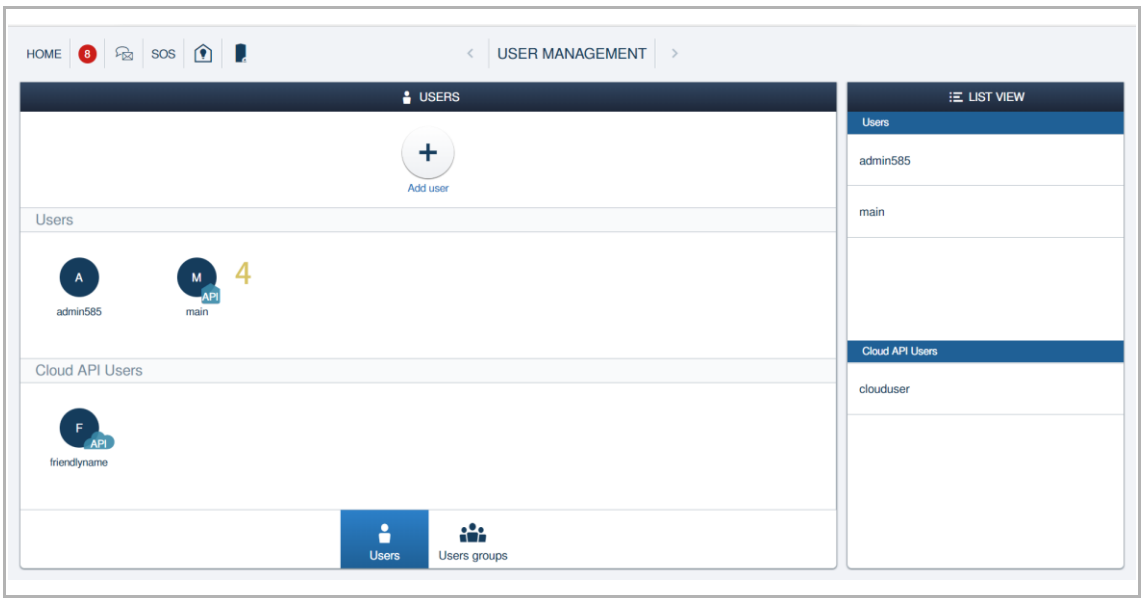
[1] On the designated user screen, click "Enable" for API access.

[2] Enter the user's password. If the user has not previously set a password, the password entered here will be used as the password to login into local API.

[3] Click "√".

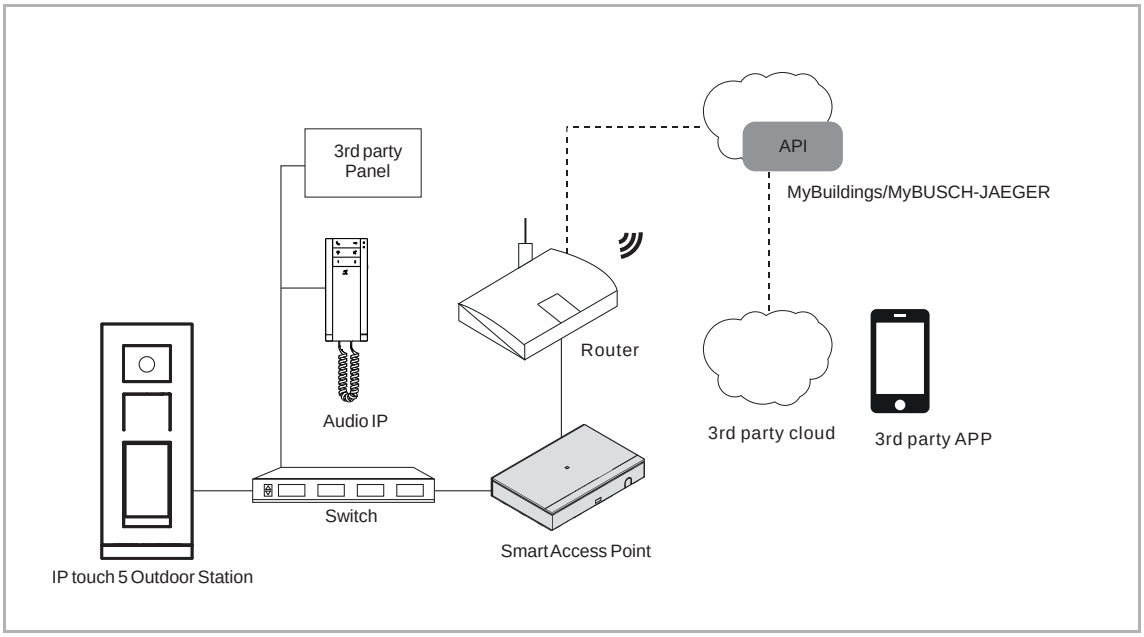


[4] Local API user is displayed on the screen.



8.8.2 Configuring cloud API

Topology



Precondition

- Ensure the version of "Smart Access Point" is 6.36 or above.
- MyBuildings portal can be accessed with a registered account.
- A cloud API user is created.

Access MyBuildings portal

Please follow the steps below:

[1] On the "Preference" screen, click "Connections & APIs" to access the corresponding screen.

[2] Click "MyBuildings connection".

[3] If MyBuildings account has not been registered, click "register here" to register an account.

[4] Enter the registered MyBuildings account, password and set an alias.

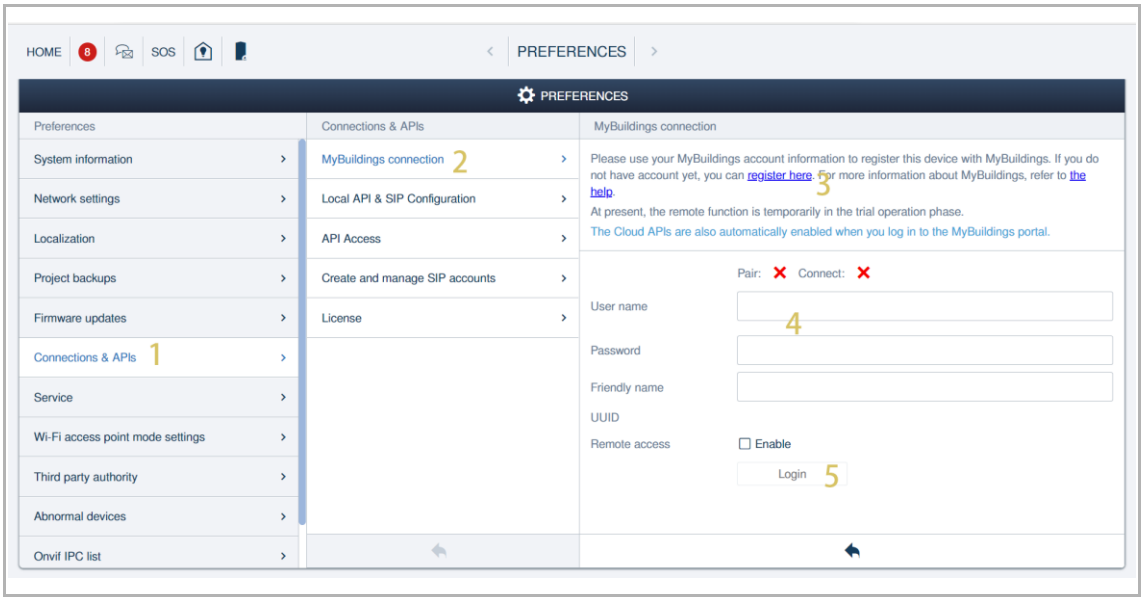
[5] Click "Login".

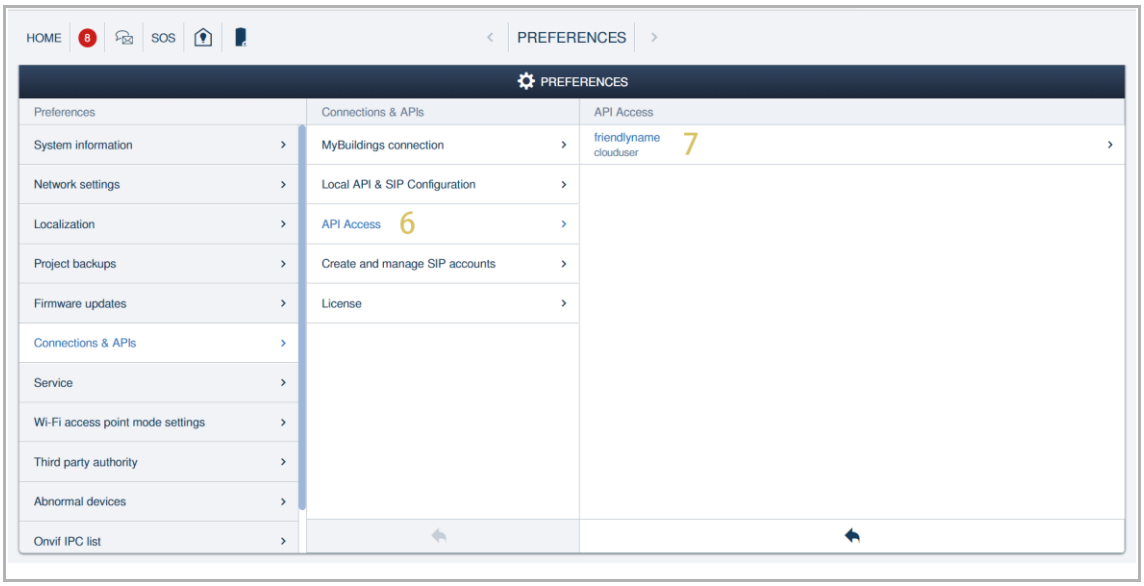
- "Pair" is displayed when the account and password are correct.
- "Connect" is displayed when "Smart Access Point" is connected to the MyBuildings portal successfully.
- If "Remote access" is enabled, you can access "Smart Access Point" on the MyBuildings portal. But you need to subscribe to the "Remote access" service on the MyBuildings portal before this function is used.

The cloud API is enabled automatically after login the portal successfully.

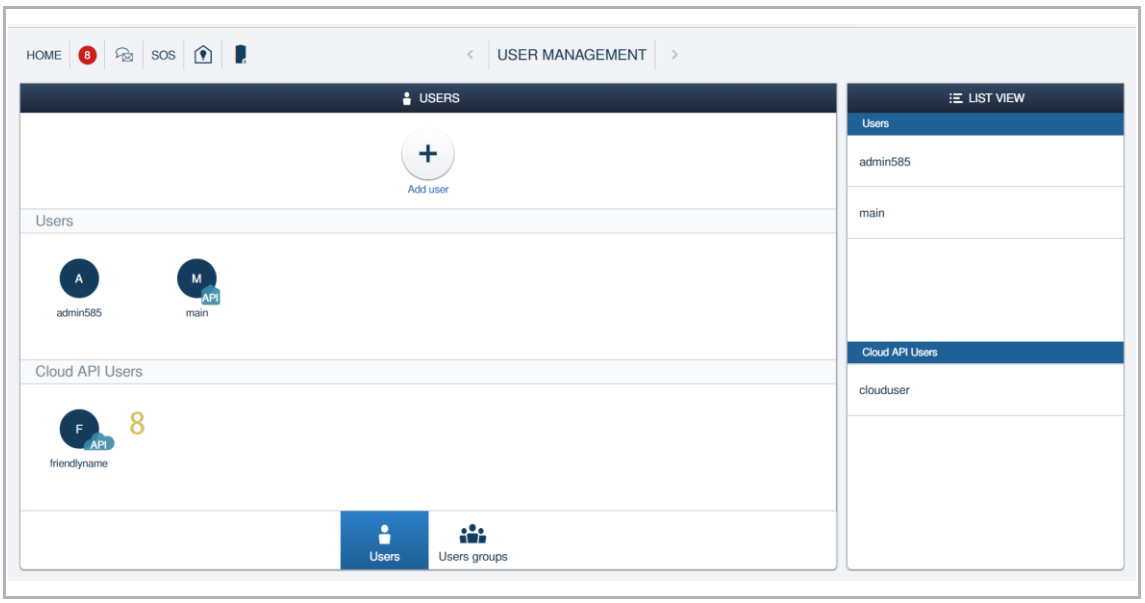
[6] Click "API Access".

[7] Could API user is displayed on the screen.



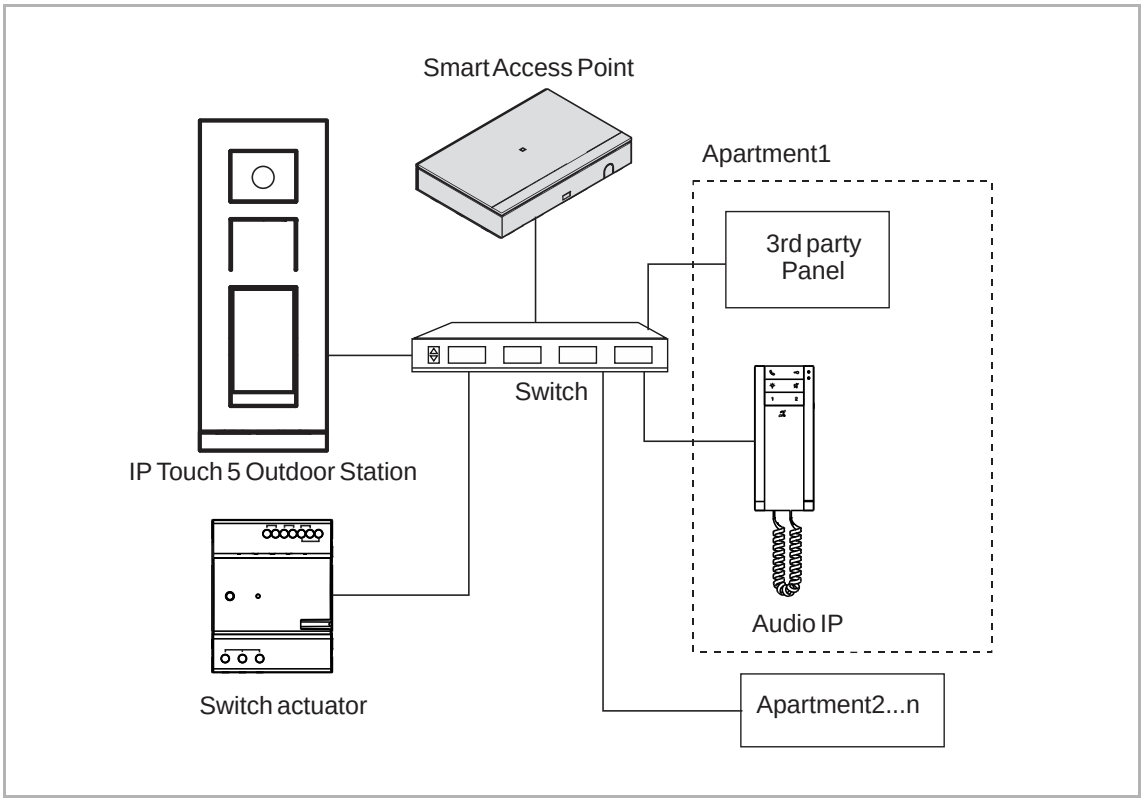

HOME
8
SOS
PREFERENCES
PREFERENCES
Preferences
System information
Network settings
Localization
Project backups
Firmware updates
Connections & APIs
Service
Wi-Fi access point mode settings
Third party authority
Abnormal devices
Onvif IPC list
Connections & APIs
MyBuildings connection
Local API & SIP Configuration
API Access
6
Create and manage SIP accounts
License
API Access
friendlyname
clouduser
7

[8] On the designated user screen, cloud API user is also displayed on the screen.



8.9 Configuring Welcome IP SIP

8.9.1 SIP application topology



The above topology supports 2 scenarios.

Scenario1: When IP touch 5 outdoor station initiates a call to a specific apartment, the 3rd party panel in the same apartment will ring. The 3rd party panel receive the call and release the door by sending a command.

Scenario2: The 3rd party panel initiates a call to IP touch 5 outdoor station.

*Usually, one Audio IP works with one 3rd party panel in the same apartment. When IP touch 5 outdoor station calls Audio IP, the related 3rd party panel also rings.

In order to achieve the scenarios above, the following settings need to be configured first.

[1] Accessing "APIs" screen on Smart Access Point.

[2] Configuring Smart Access Point as SIP server.

[3] Creating an SIP account for each 3rd party panel.

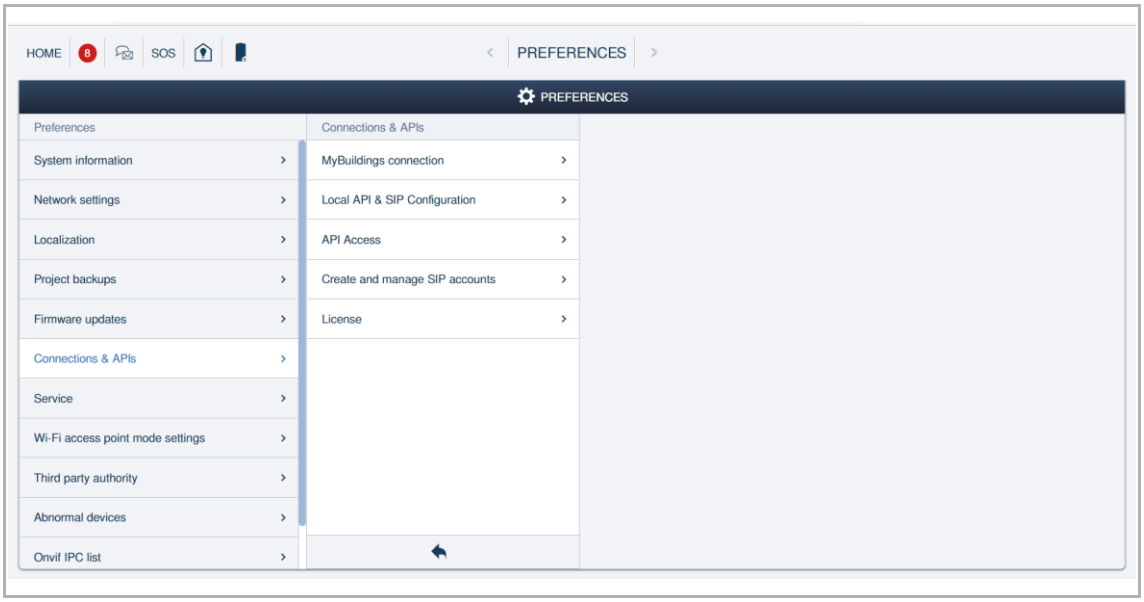
[4] Configuring the 3rd party panel.

[5] Configuring IP touch 5 outdoor station.

[6] Configuring Audio IP.

8.9.2 Accessing "APIs" screen on Smart Access Point

On the "Preference" screen, click "Connections & APIs" to access the corresponding screen.



8.9.3 Configuring Smart Access Point as SIP server

Please follow the steps below:

[1] On the "Connections & APIs" screen, click "Local API & SIP Configuration".

[2] Tick the check box to enable the "Local API and SIP connections" function.

[3] Tick the check box to enable "Smart Access Point" as SIP server.

[4] Select communication protocol.

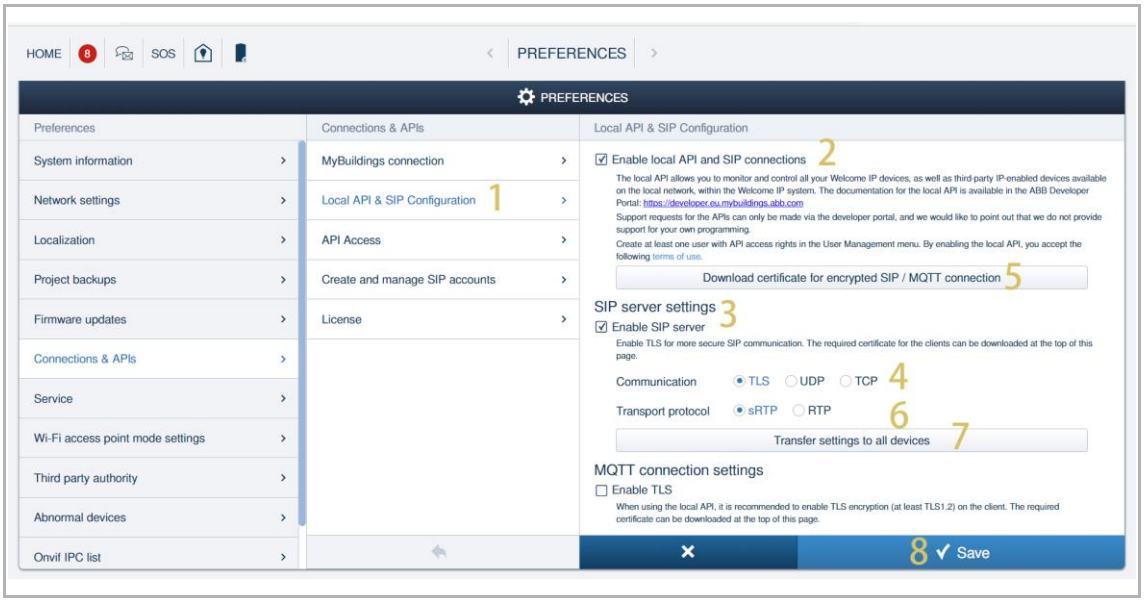
[5] If communication protocol is set to "TLS", a certificate should be download before use.

[6] Select a transport protocol.

[7] When "Transfer settings to all devices" is clicked, "Smart Access Point" will push related SIP settings to all devices (including IP Touch 5 Outdoor Station and Audio IP, but not including the 3rd party panel).

It is recommended to carry out this operation when SIP settings are changed or some device doesn't work normally.

[8] Click "Save".



8.9.4 Creating a SIP account for each 3rd party panel

There are 2 ways to create SIP account for the 3rd party panel.

1. Create the SIP account one by one

Please follow the steps below:

[1] On the "Connections & APIs" screen, click "Create and manage SIP accounts".

[2] Click "+".

[3] The 3rd party panel will be set to "Indoor station" automatically and can't not be modified.

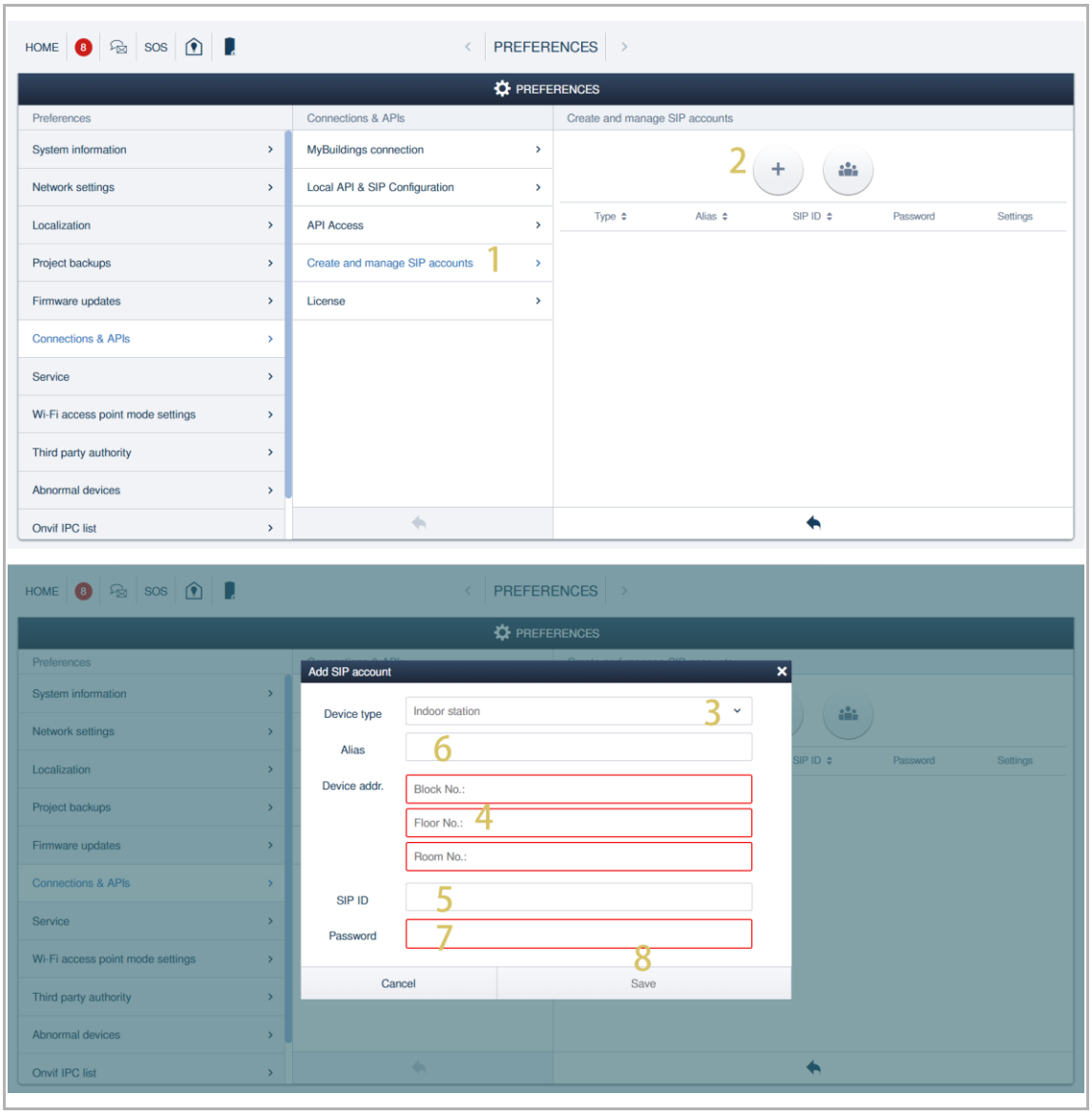
[4] Enter the device address (contains block no., floor no. and room no.).

[5] SIP ID will be generated automatically according to the rule and can't not be modified.

[6] Alias will be generated automatically according to the rule and it can be modified.

[7] Enter the password (6...15 digits).

[8] Click "Save".



2. Create SIP accounts in batch

SIP accounts for the 3rd party panel can be created in batch.

- At least one Audio IP is used in each apartment.
- The 3rd party panel should be in the same network with the designated Audio IP.
- The 3rd party panel uses the same SIP account as the designated Audio IP.

Please follow the steps below:

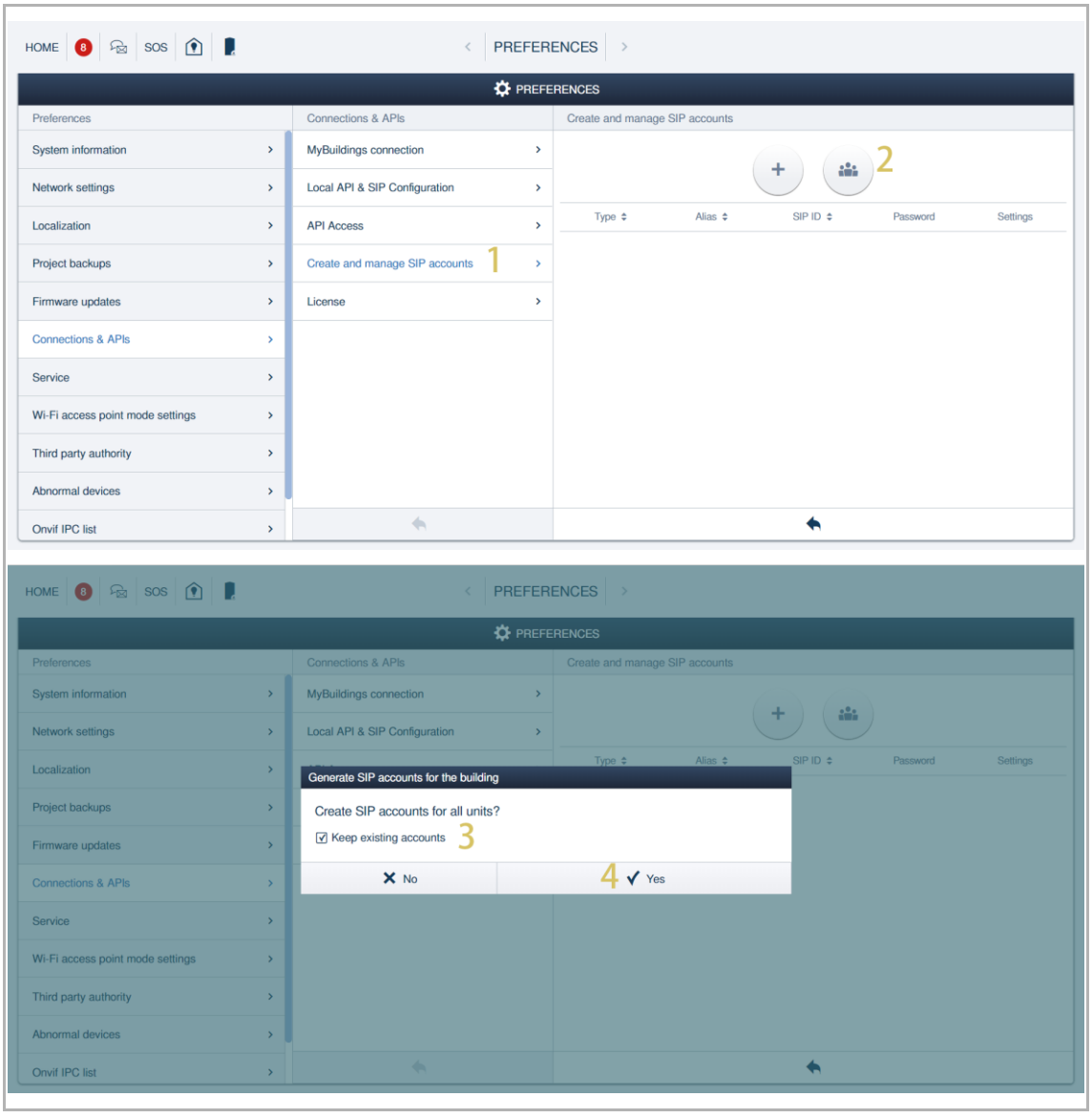
[1] On the "Connections & APIs" screen, click "Create and manage SIP accounts".

[2] Click " " ".

[3] If existing account need to be kept, tick the check box, otherwise all existing account will be clear and then new accounts will be created.

[4] Click "Yes".

SIP accounts of the 3rd party panels are generated based on the room numbers of Audio IPs which have registered in the system.



8.9.5 Configuring the 3rd party panel

Due to the diversity of the 3rd party panel, the following example is only for reference.

Please follow the steps below:

[1] Enter the SIP account.

[2] Enter the SIP password.

[3] Enter the server address 10.0.0.1.

[4] Select the transport protocol and enter the port.

- If "UDP/TCP" is selected, port should be set to "5060".
- If "TLS" is selected, port should be set to "5061".

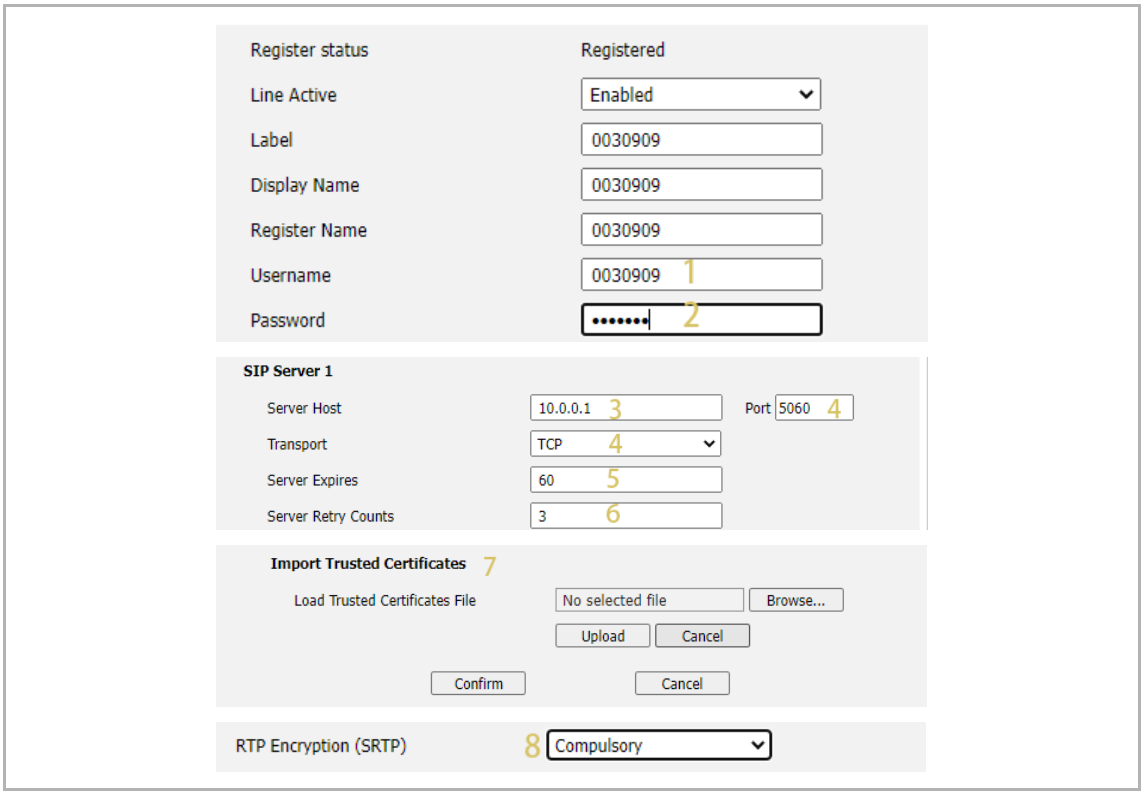
[5] Enter the server expire time (60...120 seconds).

[6] Enter the server retry counts.

[7] If communication protocol is set to "TLS", a certificate downloaded from "Smart Access Point" needs to be imported.

[8] Set the media stream transport protocol.

- Compulsory = SRTP
- Disabled = RTP



1.1.1 Configuring IP touch 5 outdoor station

IP touch 5 outdoor station needs to be configured before using SIP function.

1. SIP client settings

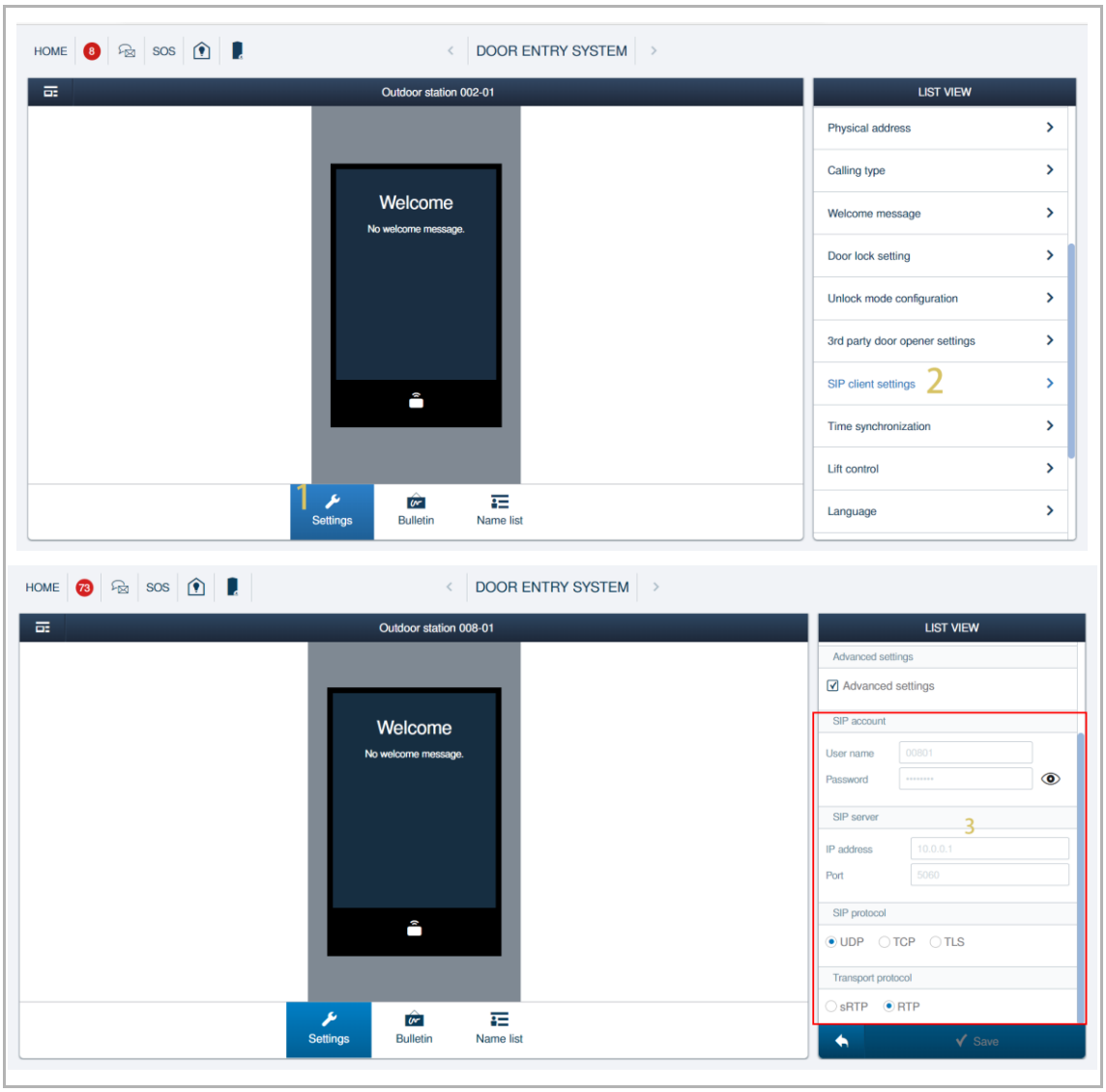
Please follow the steps below:

[1] On the designated IP touch 5 outdoor station screen, click "Settings".

[2] Click "SIP client settings".

[3] The following settings will be filled automatically when "Smart Access Point" is enabled as an SIP server and IP touch 5 has obtained the certification from "Smart Access Point".

- SIP account
- SIP server
- Communication protocol
- Transport protocol



2. 3rd party door opener settings

The 3rd party panel needs to set a button on the device to release the lock on IP touch 5 Outdoor Station.

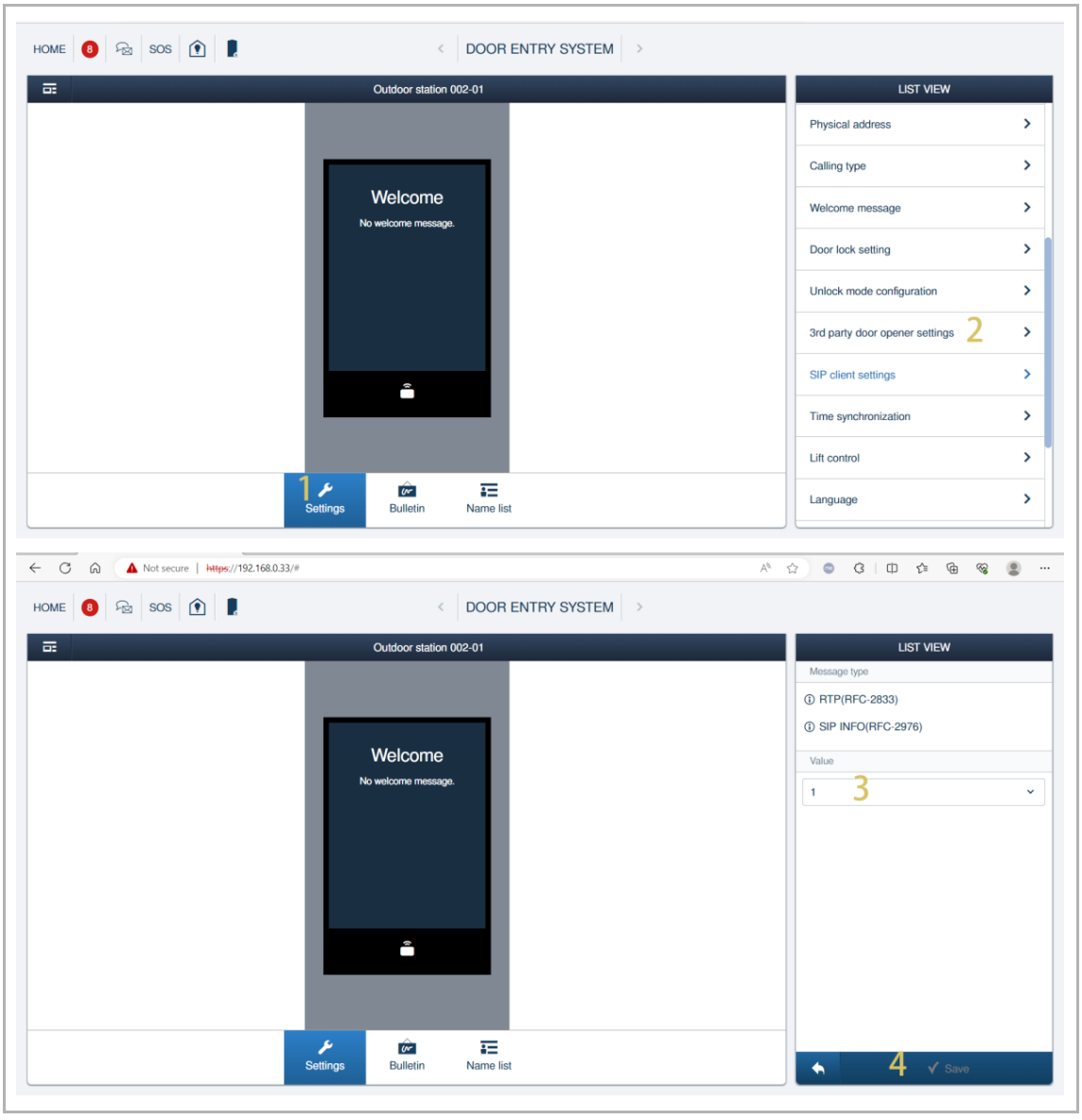
Please follow the steps below:

[1] On the designated IP touch 5 Outdoor Station screen, click "Settings".

[2] Click "3rd party door opener settings".

[3] Select a value from the drop-list as the command to release the lock. It can be set to "0~9" , "*" or "#".

[4] Click "Save".



3. Adding the 3rd party panels to the name list one by one

It is available for IP touch 5 outdoor station calls the 3rd party panel via keypad directly or name list.

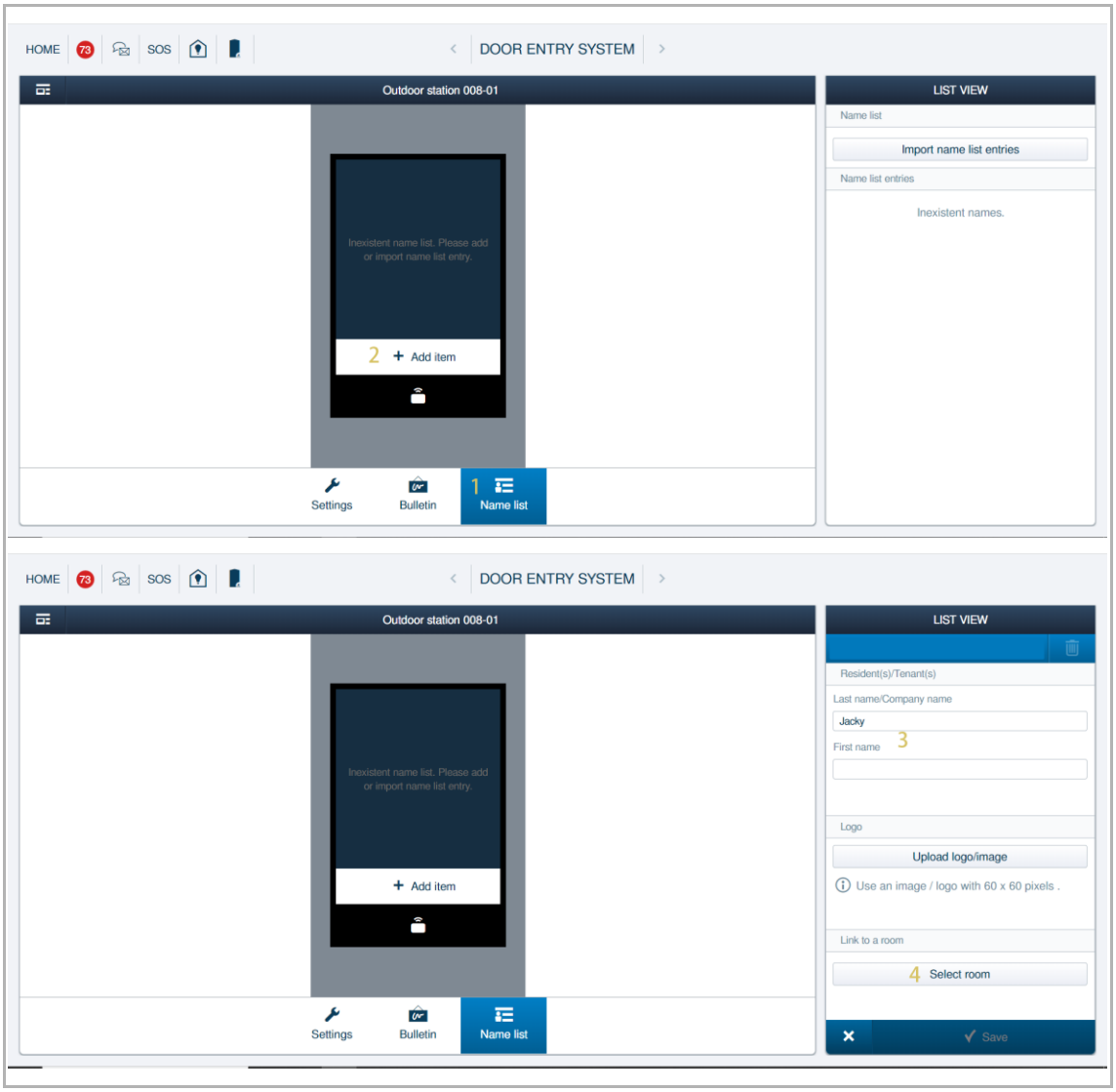
Please follow the steps to add the 3rd party panel to the name list:

[1] On the designated IP touch 5 outdoor station screen, click "Name list".

[2] Click "+ Add item".

[3] Enter the last name and the first name.

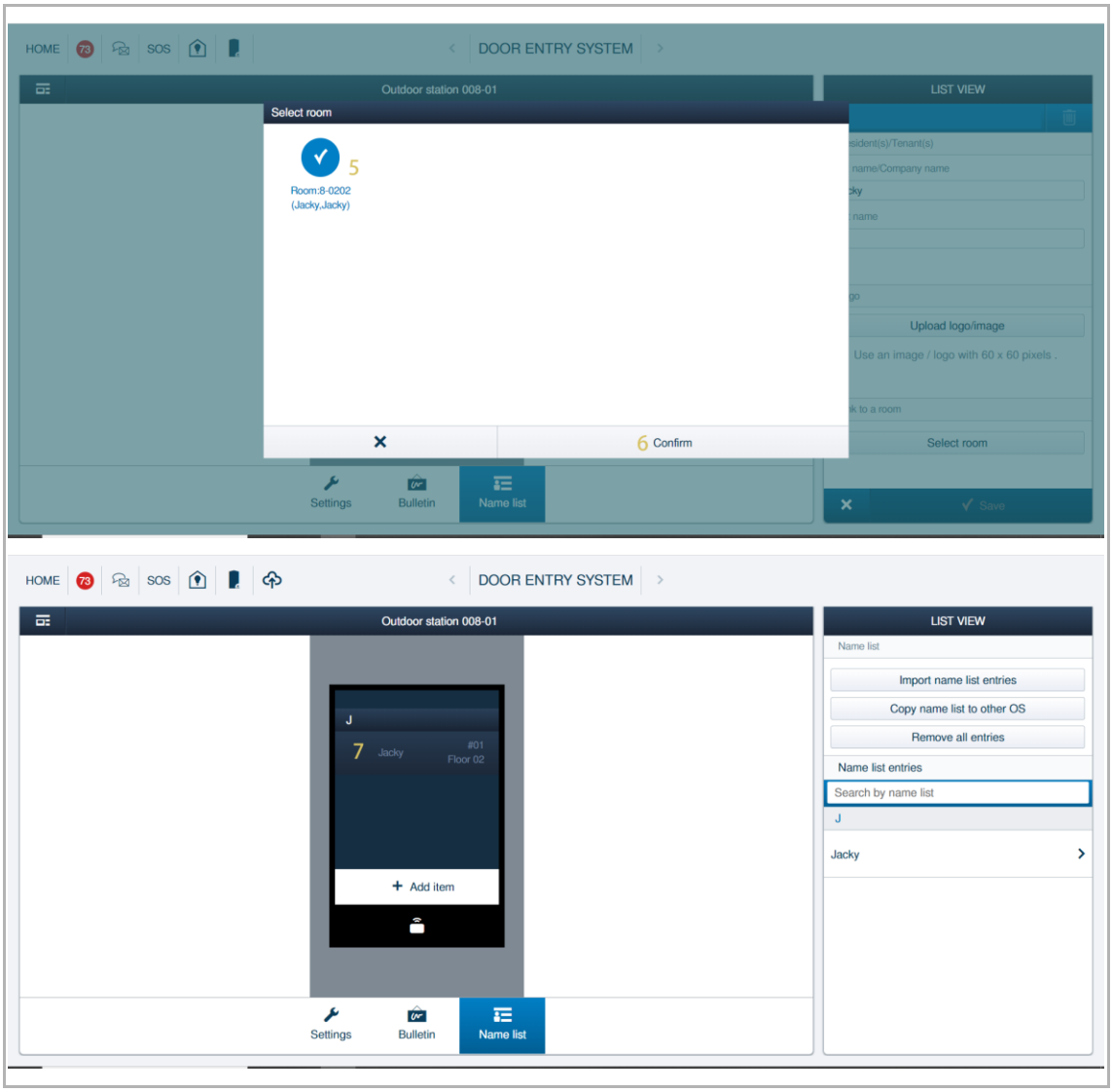
[4] Click "Select room".



[5] Select the designated room where the 3rd party panel is placed.

[6] Click "Confirm".

[7] The alias name has been displayed on the screen of IP touch 5 outdoor station.



4. Adding the 3rd party panels to the name list in batch

If there are many 3rd party panel need to be added to the name list. It is recommended to use importing function.

Please follow the steps to add the 3rd party panels to the name list in batch:

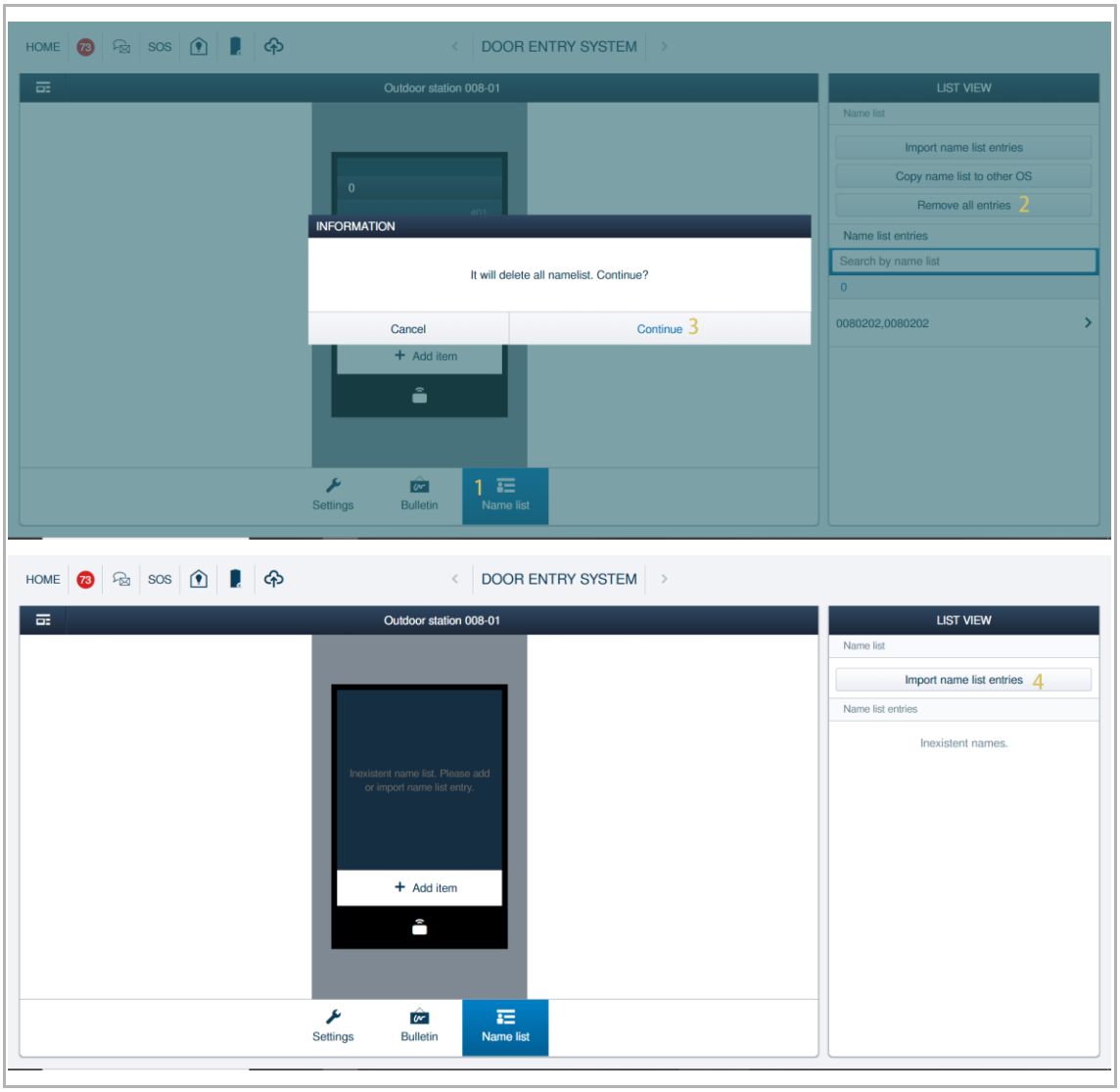
It is recommended remove all entries before importing.

[1] On the designated IP touch 5 outdoor station screen, click "Name List".

[2] Click "Remove all entries".

[3] Click "Continue".

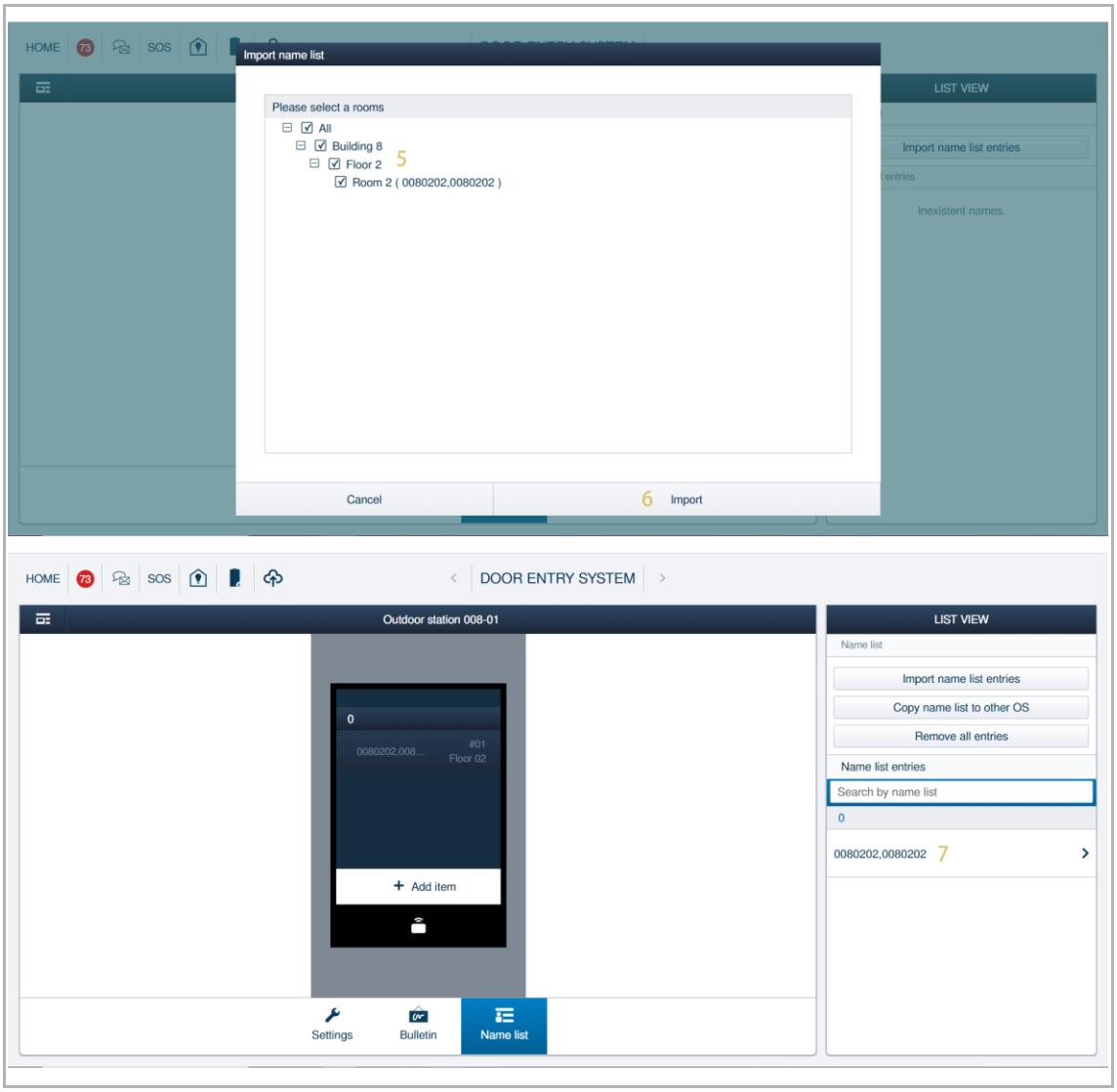
[4] Click "Import name list entries".



[5] Select the designated rooms.

[6] Click "Import".

[7] The alias name has been displayed on the screen. Click the name to set the alias name.



8.9.6 Configuring Audio IP

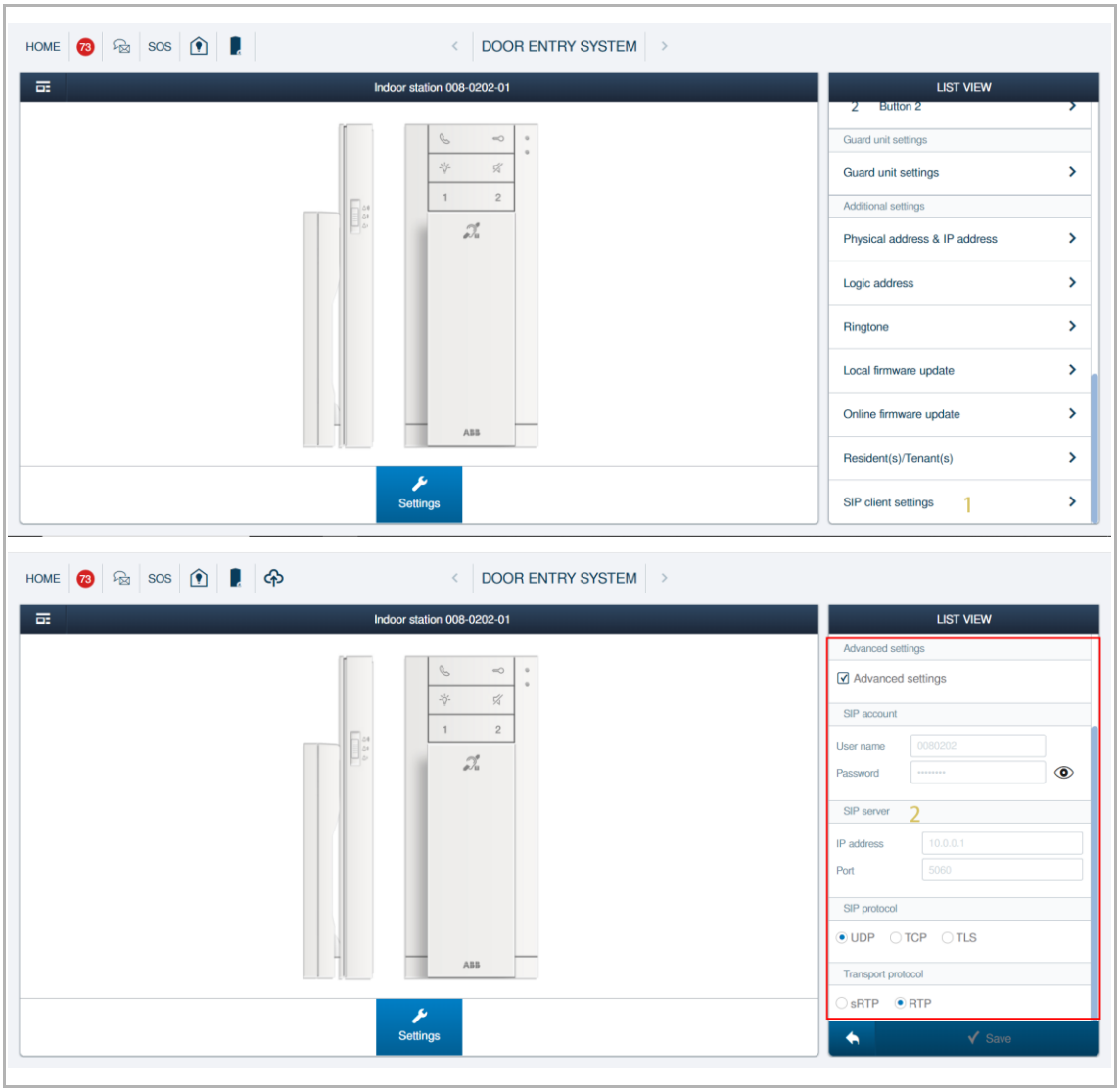
Audio IP needs to be configured before using SIP function.

Please follow the steps below:

[1] On the designated Audio IP "Settings" screen, click "SIP client settings".

[2] The following settings will be filled automatically when "Smart Access Point" is enabled as an SIP server and Audio IP has obtained the certification from "Smart Access Point".

- SIP account
- SIP server
- Communication protocol
- Transport protocol



9 Operating Door Entry System devices

9.1 Door Entry System topology

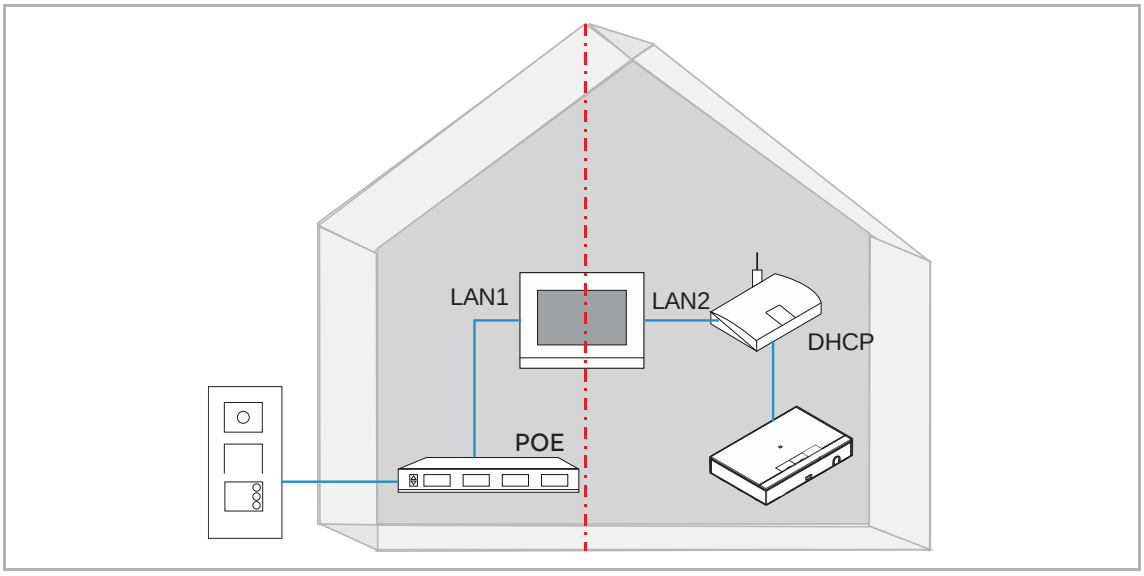
Topology1: Single-family house

In an ABB-Welcome IP system in a private building the building network is disconnected from the unit network. This prevents unauthorized access to the private unit network via the outdoor station.

An IP Touch 7/10 is installed.

In this type of installation, the IP Touch 7/10 additionally meets the function of an IP gateway.

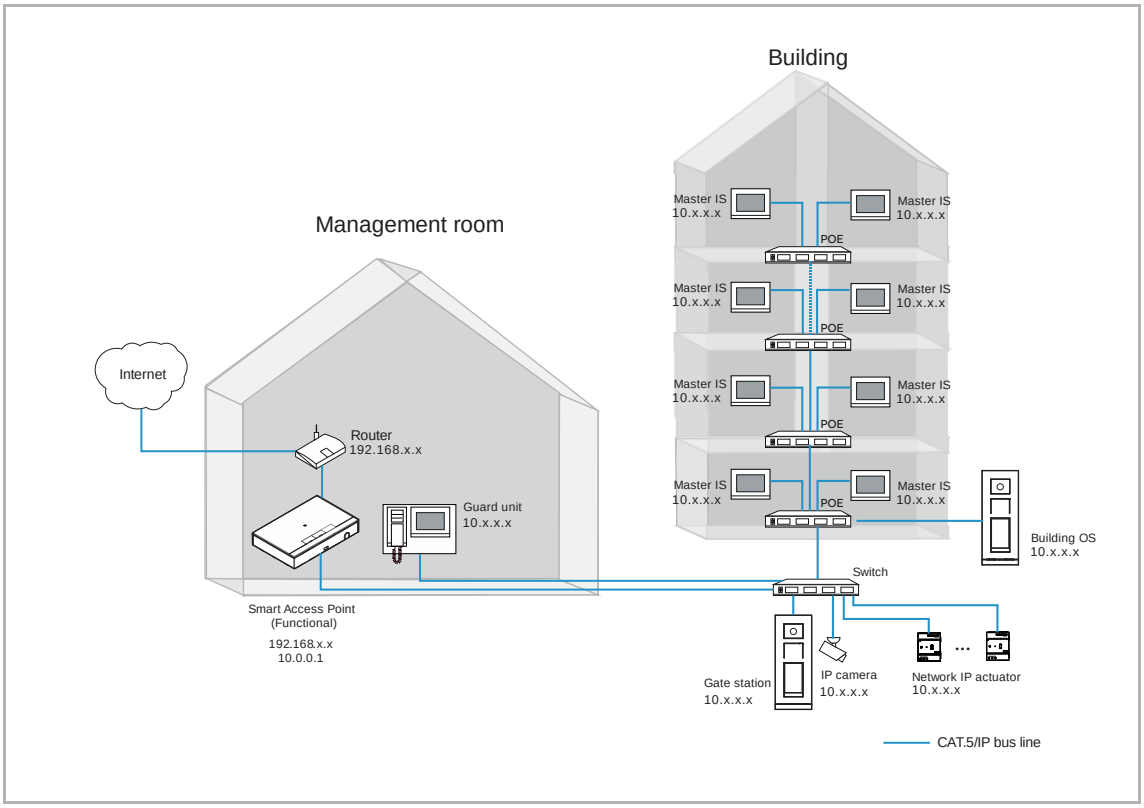
"Smart Access Point" should be set to "Commercial Mode" on the initial Setup.



Topology 2: High rise building

In this case, "Smart Access Point" should be set to "Functional mode" on the initial setup. see chapter 8.3 “Initial setup“ on page 26.

In this case, "Smart Access Point" is used to manage all the devices in the building.

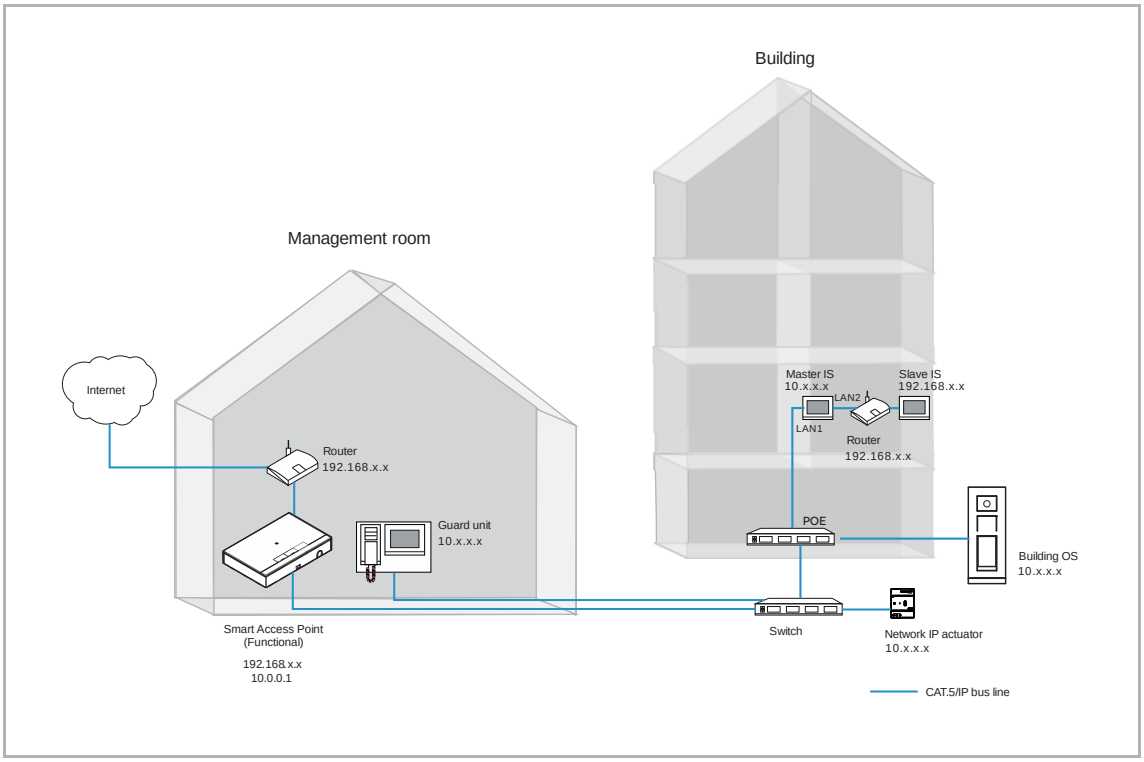


Demo case for operating Door Entry System devices

The following demo case refers to topology 2.

This demo case is used to familiarise yourself with the operations of Door Entry system devices.

You need to adjust your operations when you operate an actual project.



9.2 Adding devices

Note

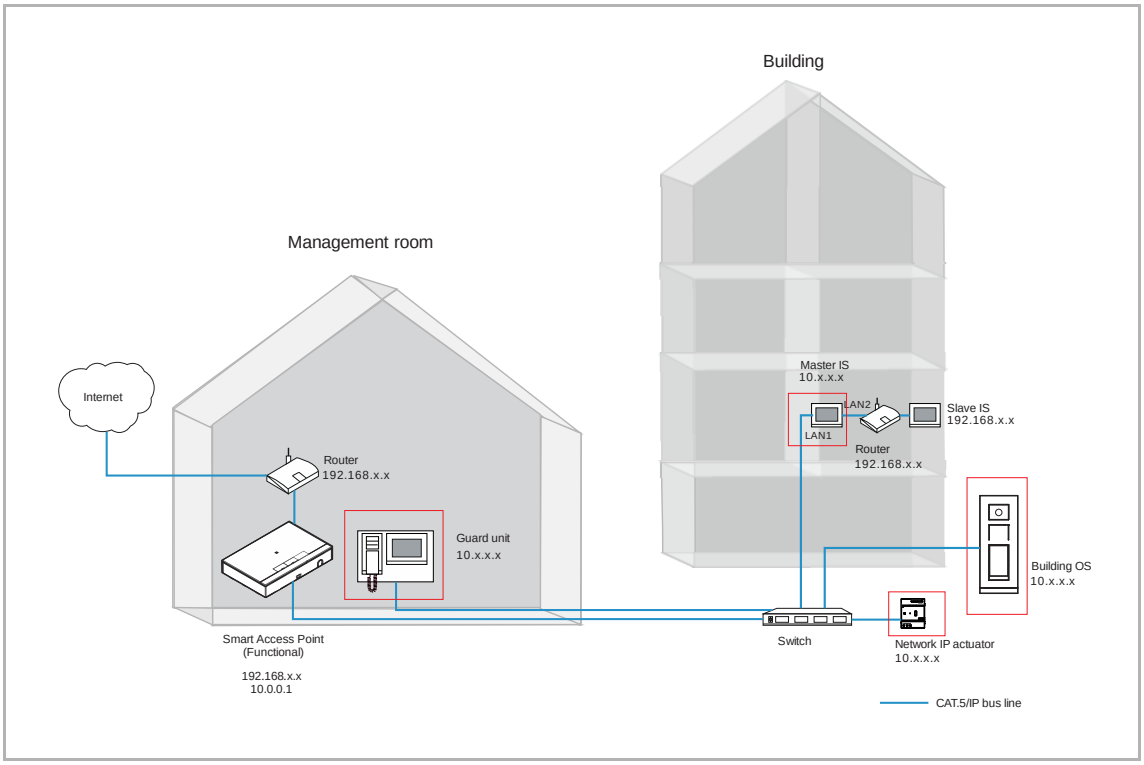
- All the Door Entry System devices need a signature on "Smart Access Point" before use.
- "Smart Access Point" will assign a signature to the devices automatically when adding them.
- If the device has already been signed by current "Smart Access Point", it will not be signed again.
- If the device has already been signed by other "Smart Access Point", it will not be signed and "Sign failed" will be displayed on the "Abnormal devices" screen. see chapter 8.7.10 “Abnormal devices“ on page 57.

9.2.1 Adding devices via scan

Note

Only the devices on the same network segment as "Smart Access Point" can be added via scan. Please see the devices surrounded by a red box on the diagram below.

"Slave indoor station "cannot be added via scan. see chapter 9.2.2 “Adding devices manually“ on page 100



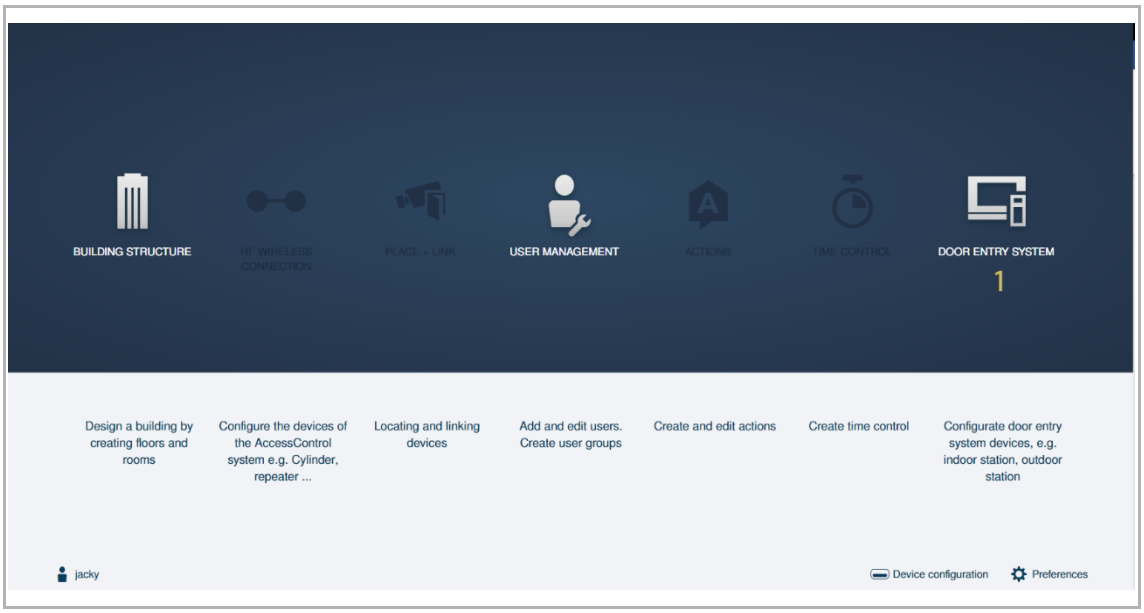
Precondition

- All the devices must be powered on.
- All the devices must be set a different physical address.
- None of the devices should be signed by another "Smart Access Point". If the devices have been signed by another "Smart Access Point", you will need to clear the signature e.g. by changing the physical address of the device.

Adding the devices via scan

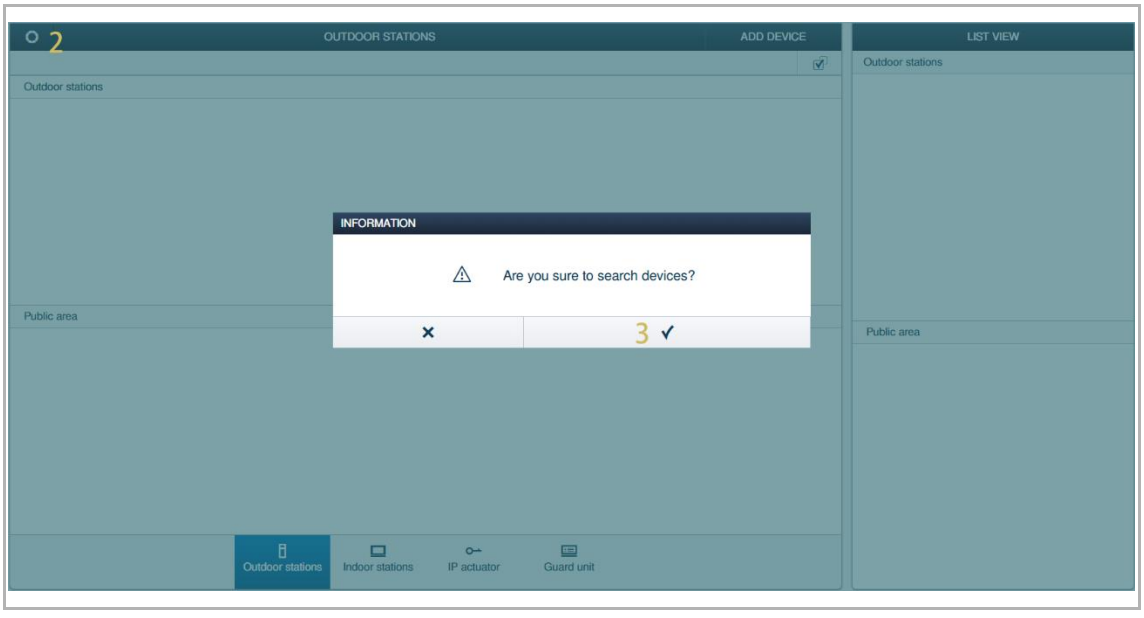
Please follow the steps below:

[1] On the configuration screen, click "Door entry system" to access the "Door Entry System" screen.

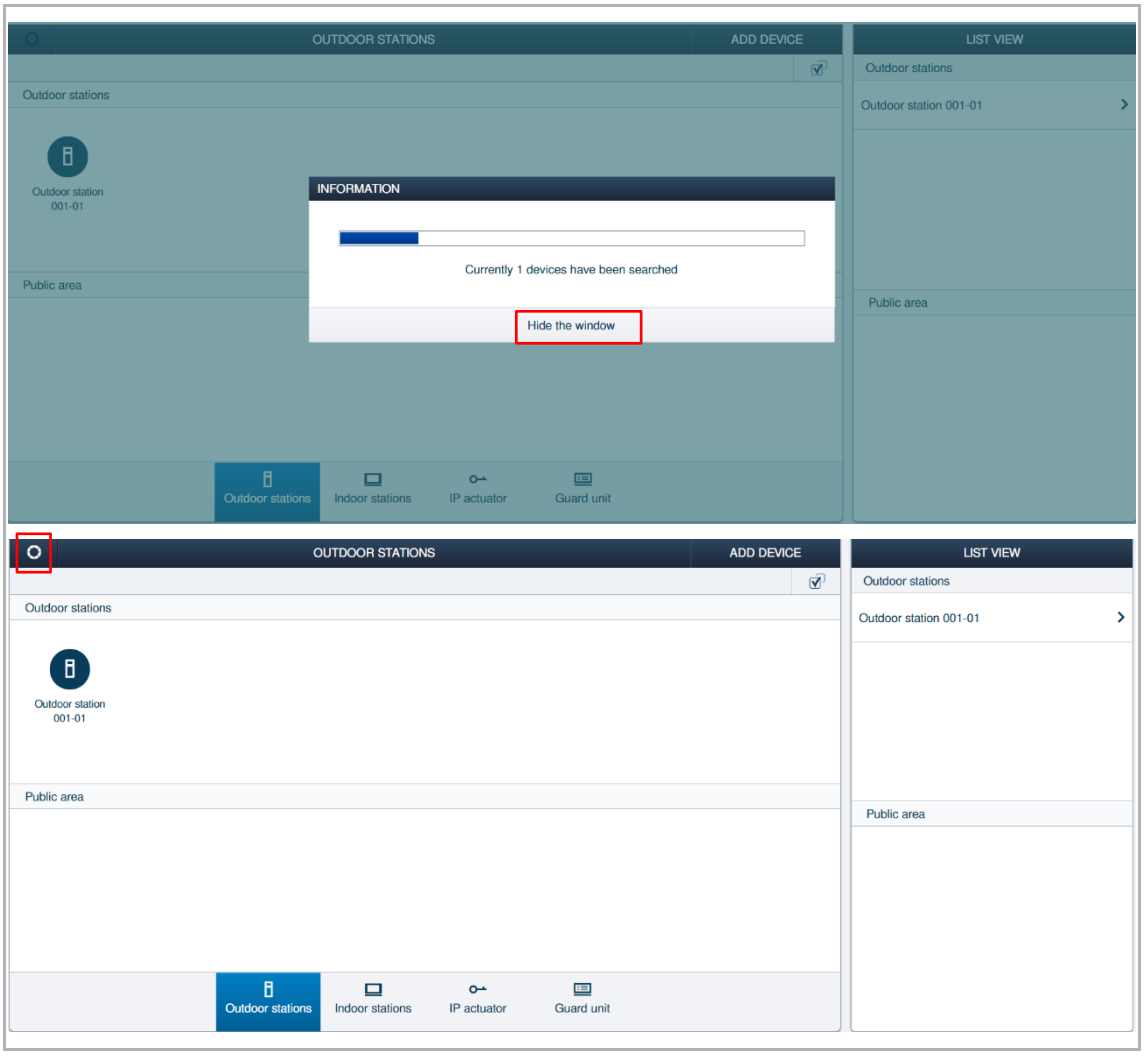


[2] On the "Door Entry System" screen, click " ".

[3] Click " √ " to continue.

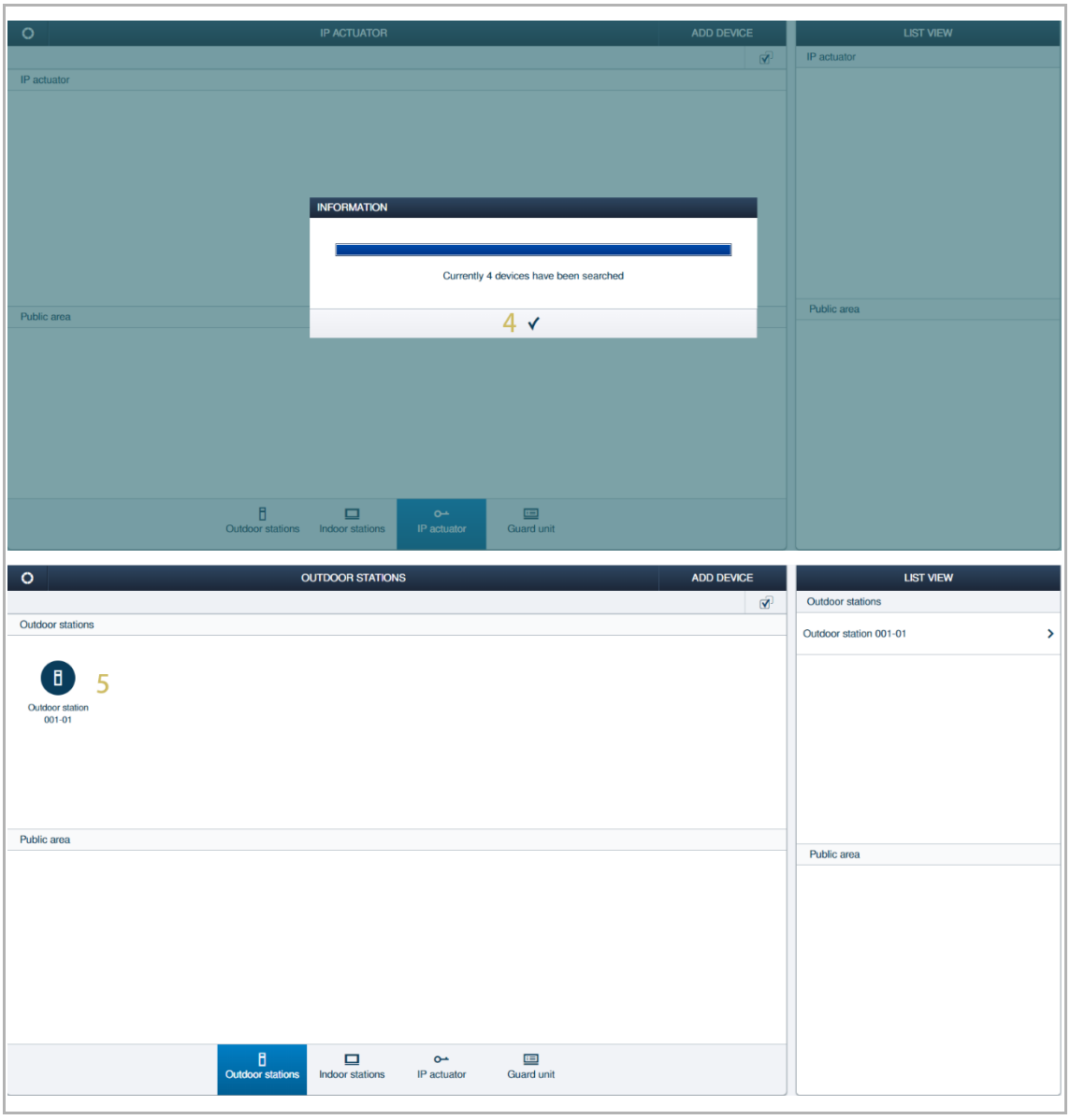


During the search, click "Hide the window" to hide the current pop-up window and " " will flash to indicate the search status.



[4] Search result is displayed on the screen; click " √ " to continue.

[5] The devices are displayed on the screen if successful.



9.2.2 Adding devices manually

Note
All the devices can be added on "Smart Access Point" manually.
"Slave indoor stations" can be added in this way.

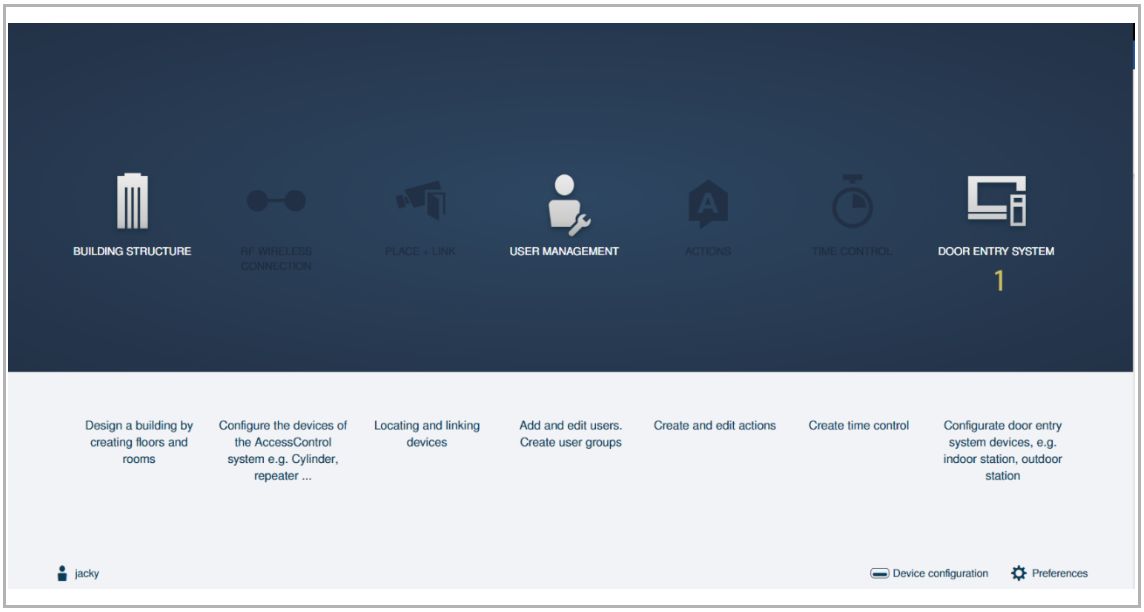
Precondition

- All the devices to be added manually must be powered on.
- None of the devices to be added manually should be signed by other "Smart Access Point". It the devices have been signed by other "Smart Access Point", you need to clear the signature e.g. changing the physical address of the device.

Adding the devices manually

Please follow the steps below:

[1] On the configuration screen, click "Door entry system" to access the "Door Entry System" screen.



[2] On the "Door Entry System" screen, click "Add device".

Note

The following operations show you to add a slave indoor station. Please adjust your operations according to the actual devices.

[3] Select a device type from the drop-down list (e.g. "Indoor station").

[4] Enter block number.

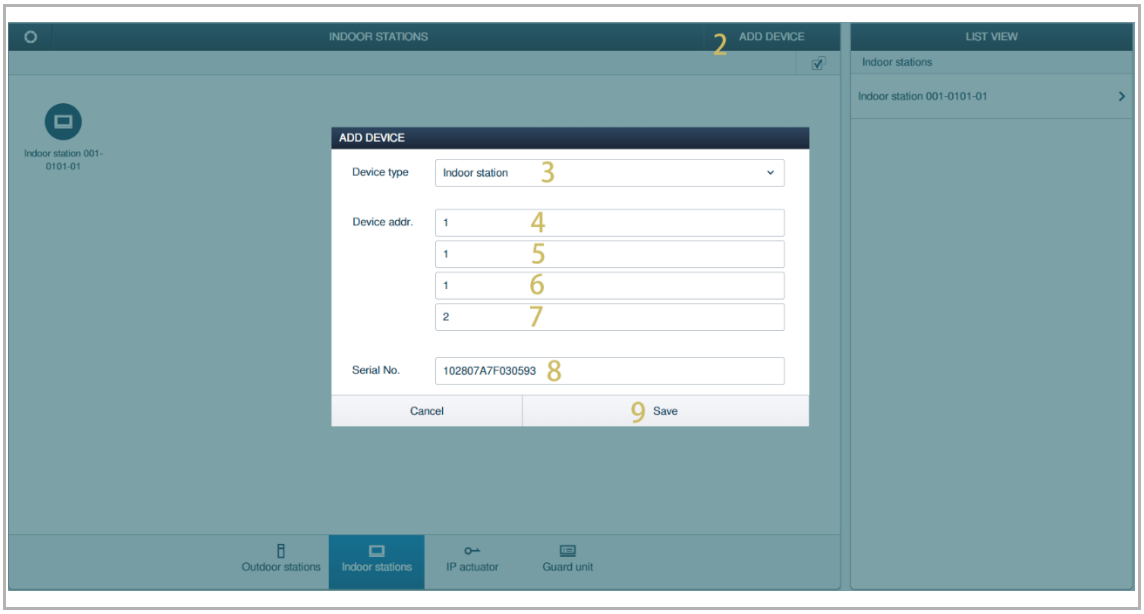
[5] Enter floor number

[6] Enter room number.

[7] Enter device number.

[8] Enter serial number.

[9] Click "Save" to save.



[10]The device is displayed on the screen if successful.

Note

If the device has already been signed by other "Smart Access Point", it will not be signed and "Sign failed" will be displayed on the "Abnormal devices" screen. see chapter 8.7.10 “Abnormal devices“ on page 57.

9.3 Managing the trusted devices

9.3.1 Managing the trusted devices for outdoor station

If you want to release the lock on the outdoor station, you need to check:

- If the indoor station and the outdoor station are signed on "Smart Access Point".
- If the indoor station was added on the trusted list on the outdoor station.

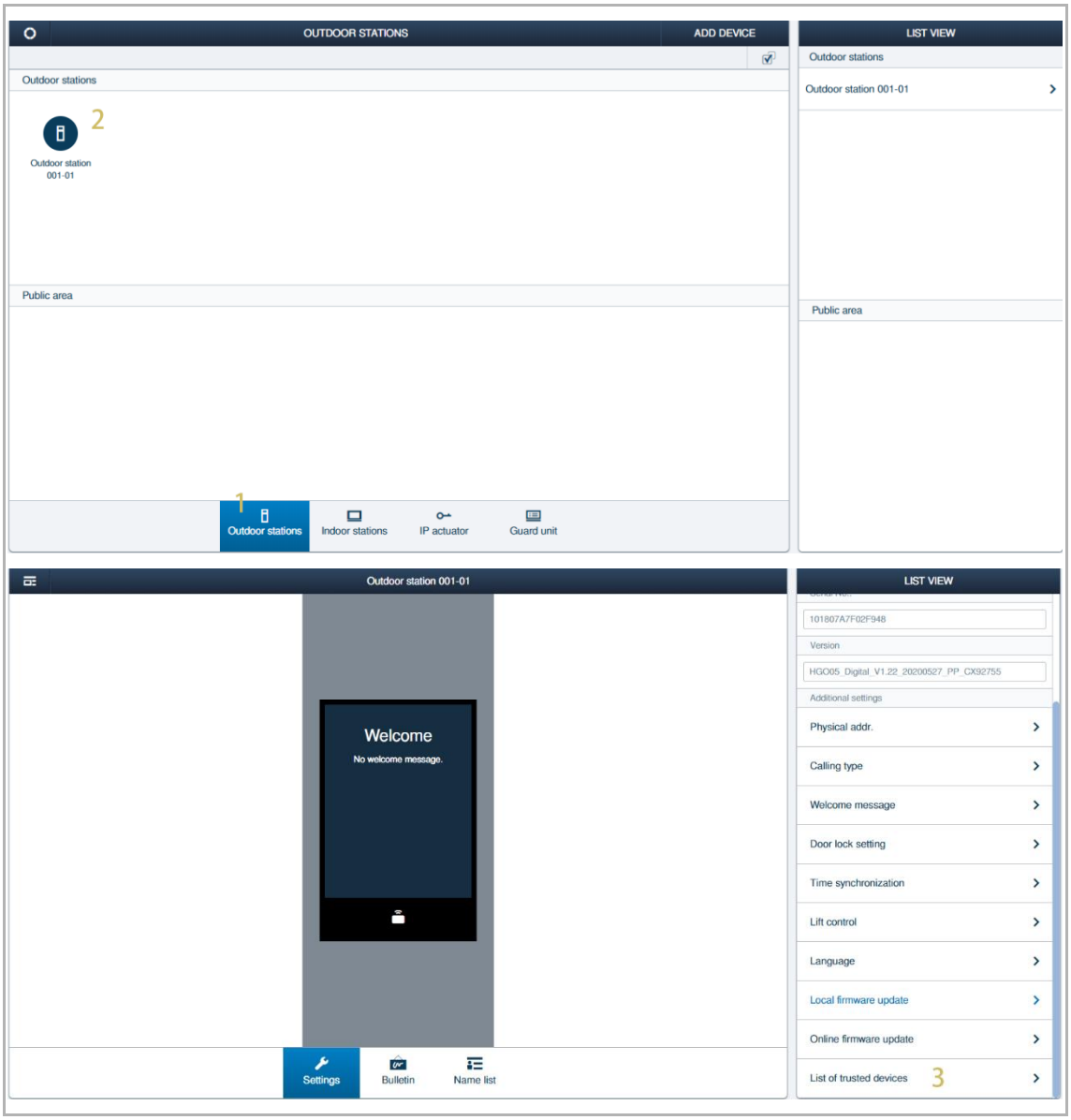
1. Adding the trusted devices

Please follow the steps below:

[1] On the "Door Entry System" screen, click "Outdoor stations".

[2] Click the designated outdoor station.

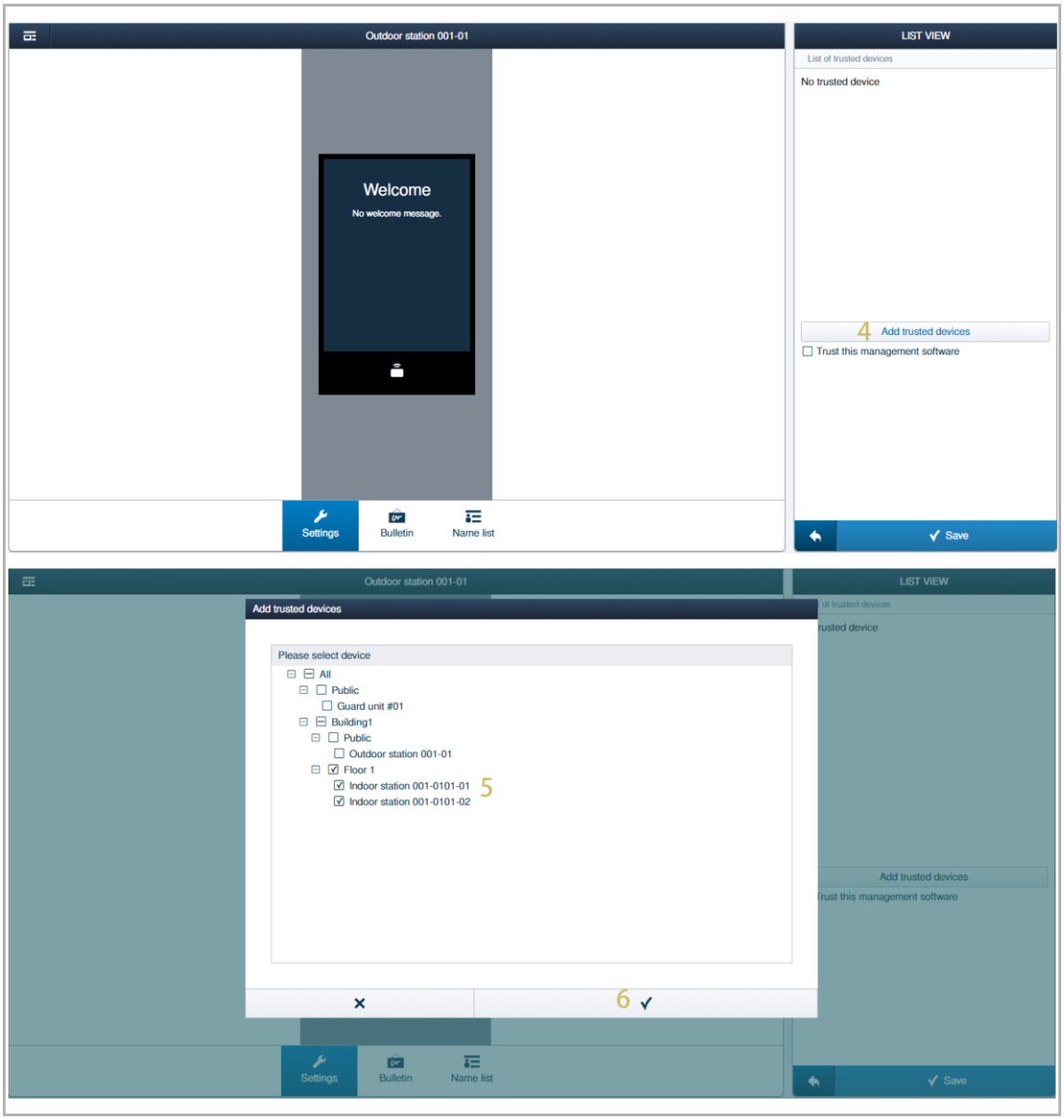
[3] Scroll down the list and click "List of trusted devices".



[4] Click "Add trusted devices".

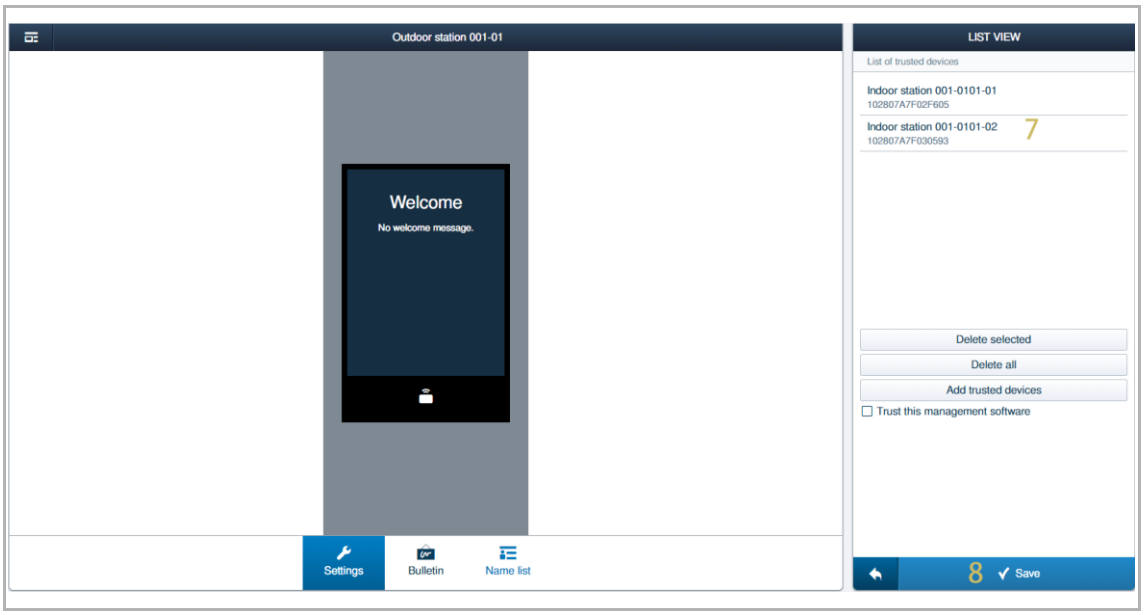
[5] Tick the check boxes to select the devices to be trusted.

[6] Click " √ " to confirm.



[7] The result is displayed on the screen.

[8] Click "Save" to save.



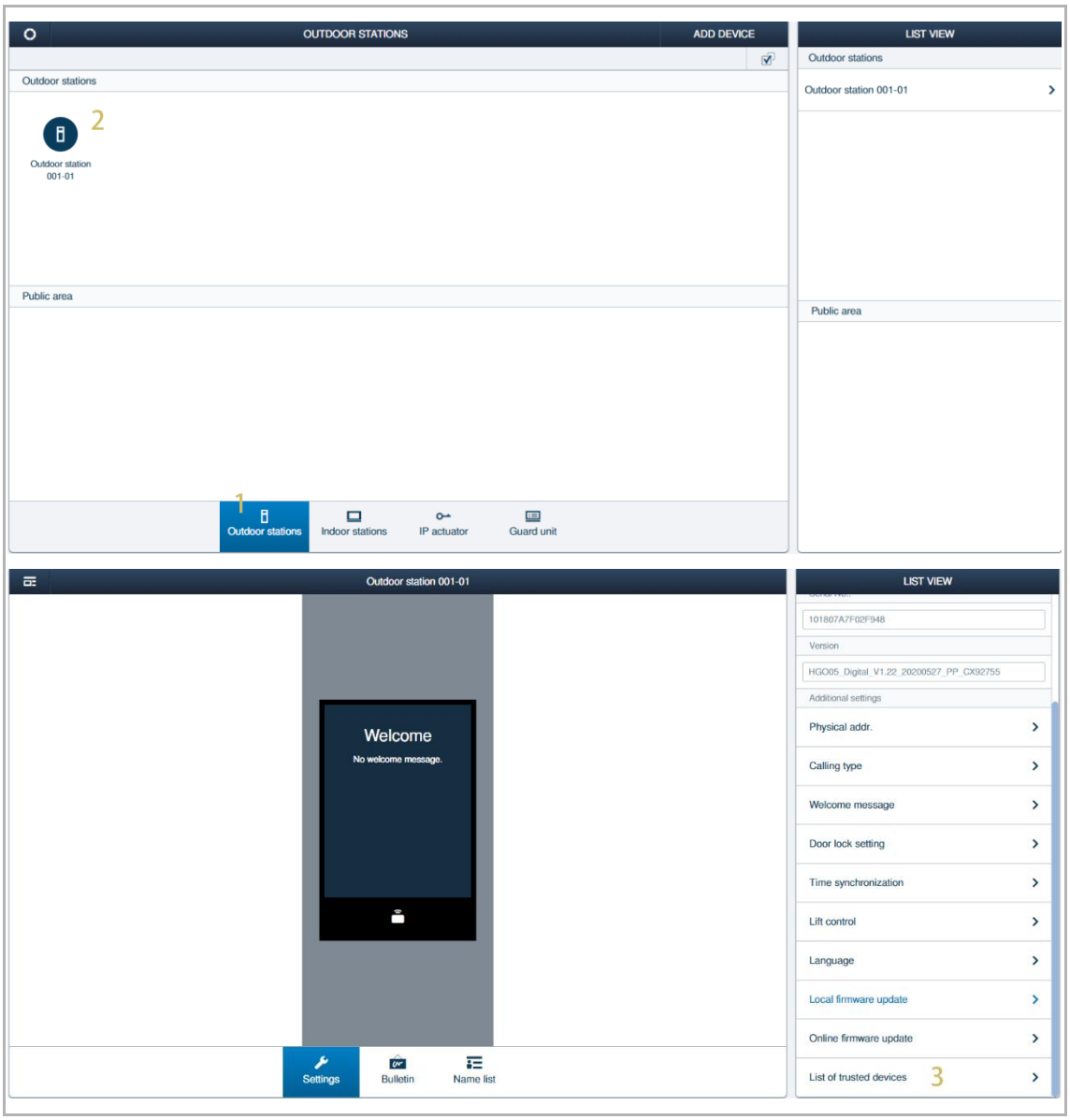
2. Removing the trusted devices

Please follow the steps below:

[1] On the "Door Entry System" screen, click "Outdoor stations".

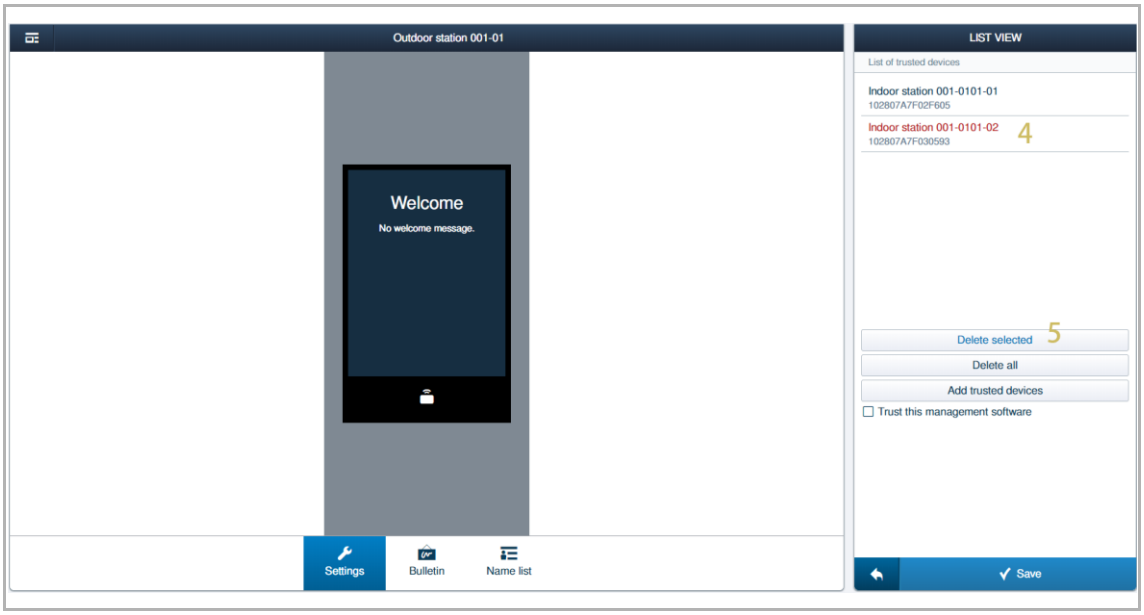
[2] Click the designated outdoor station.

[3] Scroll down the list and click "List of trusted devices".



[4] Click the designated device to select one by one (the selected devices are highlighted in red).

[5] Click "Delete selected".



9.3.2 Managing the trusted devices for IP actuator

If you want to release the lock on the IP actuator, you need to check:

- If the indoor station and the IP actuator are signed on "Smart Access Point".
- If the indoor station has been added to the trusted list on the IP actuator.

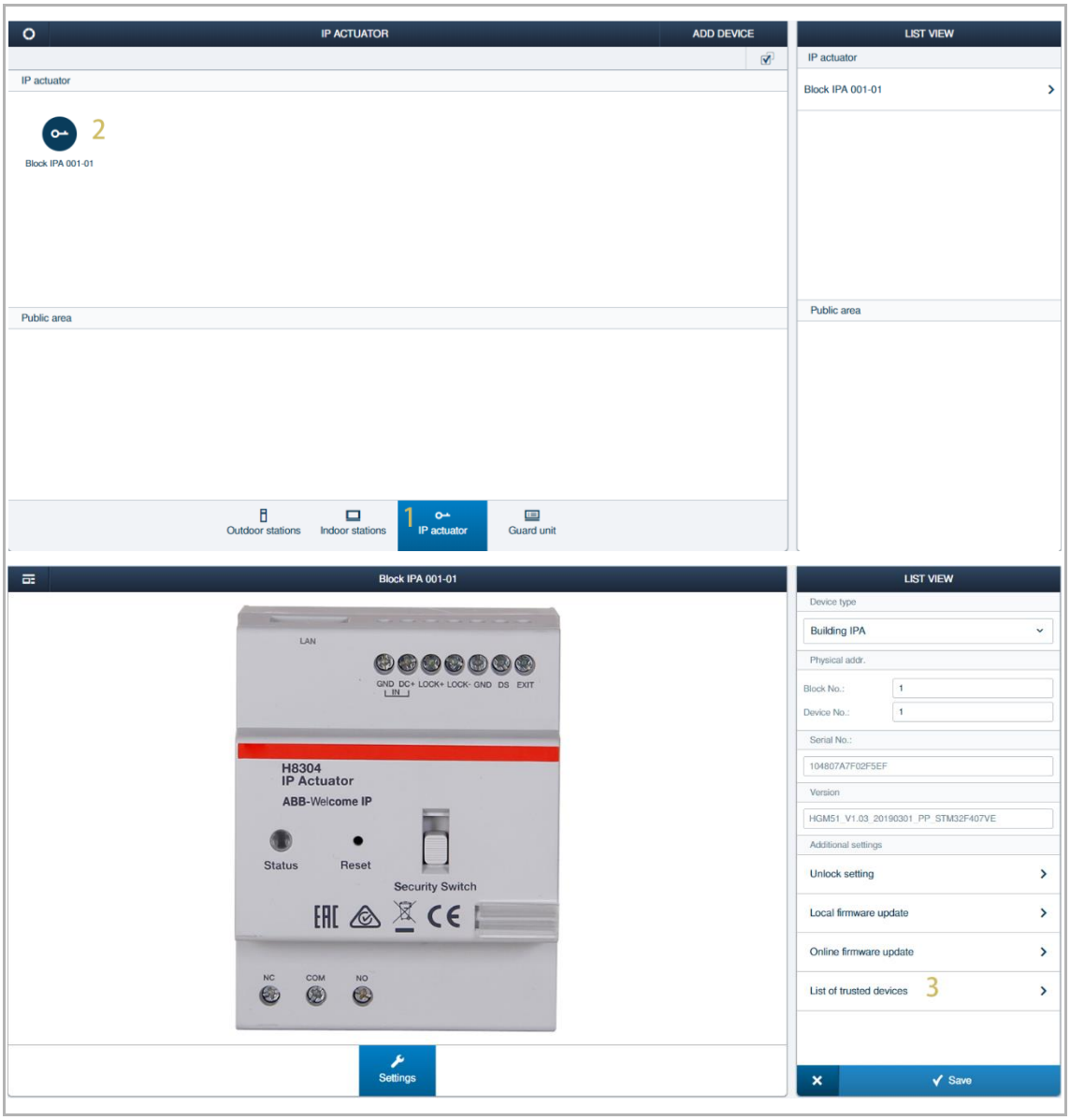
1. Adding the trusted devices

Please follow the steps below:

[1] On the "Door Entry System" screen, click "IP actuator".

[2] Click the designated IP actuator.

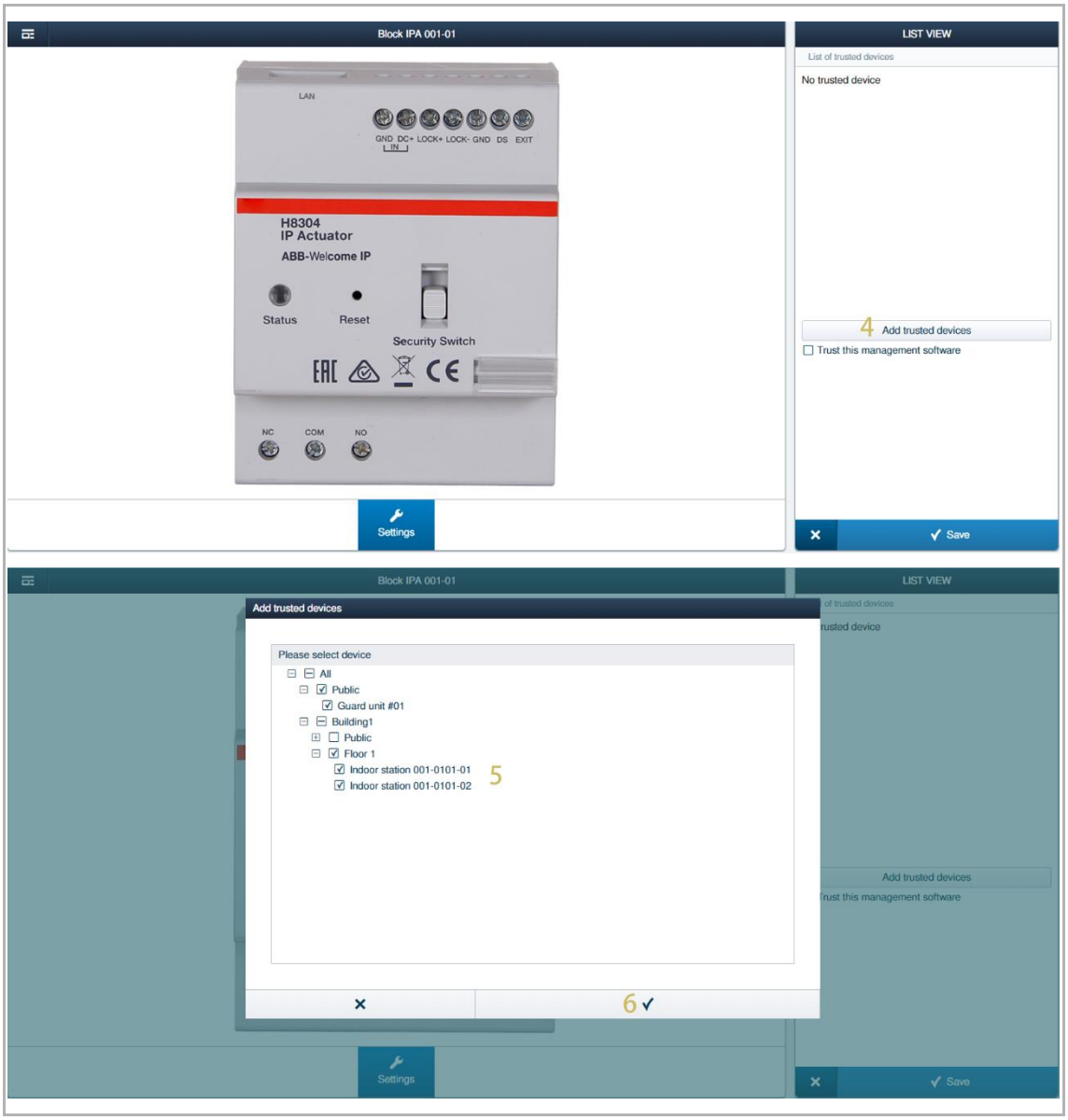
[3] Click "List of trusted devices".



[4] Click "Add trusted devices".

[5] Tick the check boxes to select the devices to be trusted.

[6] Click " √ " to confirm.



[7] The result is displayed on the screen.

[8] Click "Save" to save.

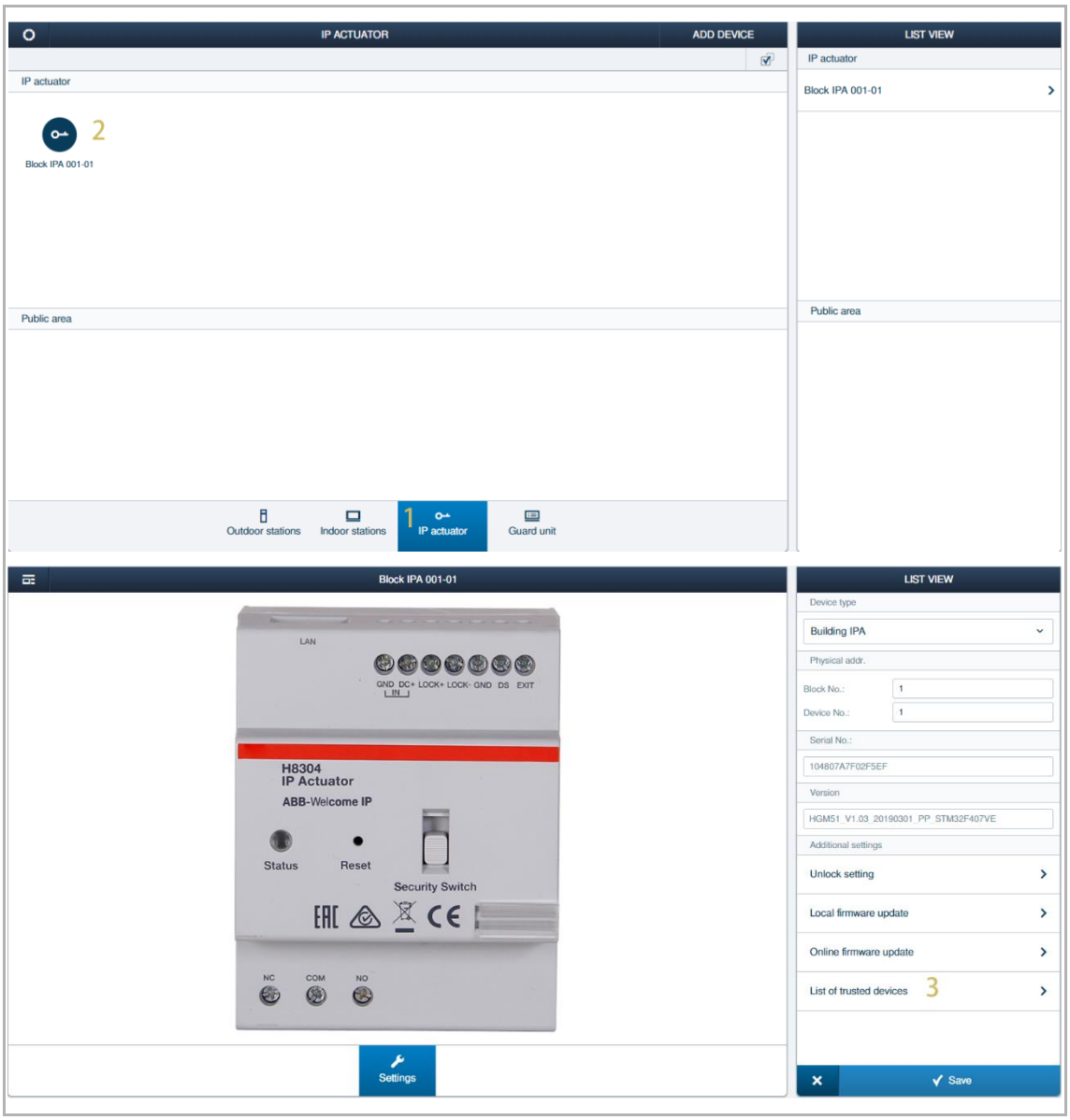
2. Removing the trusted devices

Please follow the steps below:

[1] On the "Door Entry System" screen, click "IP actuator".

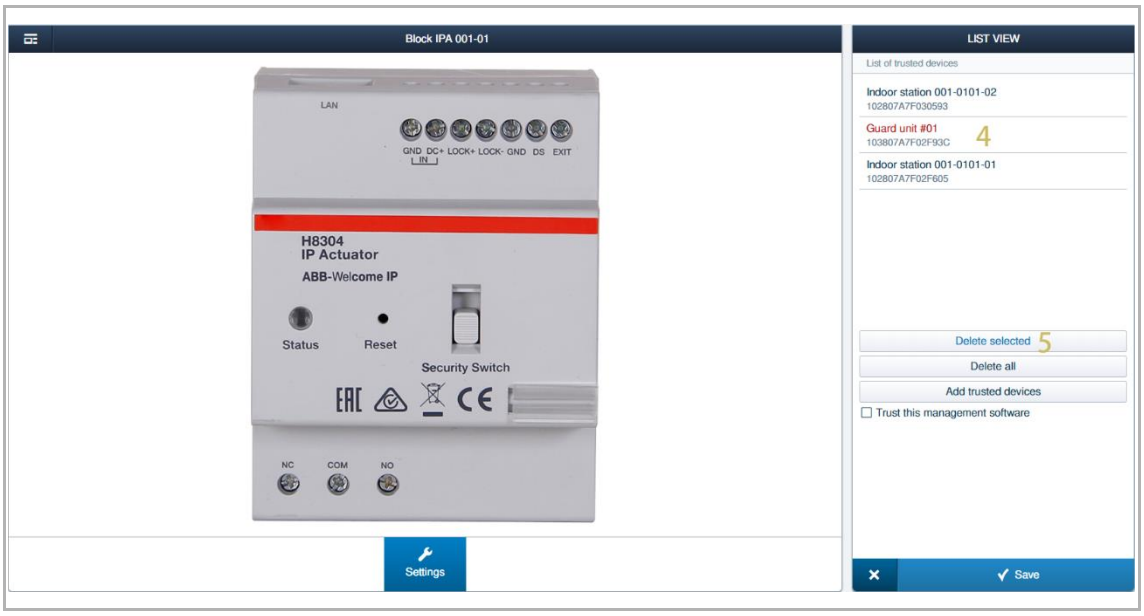
[2] Click the designated IP actuator.

[3] Click "List of trusted devices".



[4] Click the designated device to select one by one (the selected devices are highlighted in red).

[5] Click "Delete selected".



9.3.3 Managing the trusted devices for "Smart Access Point"

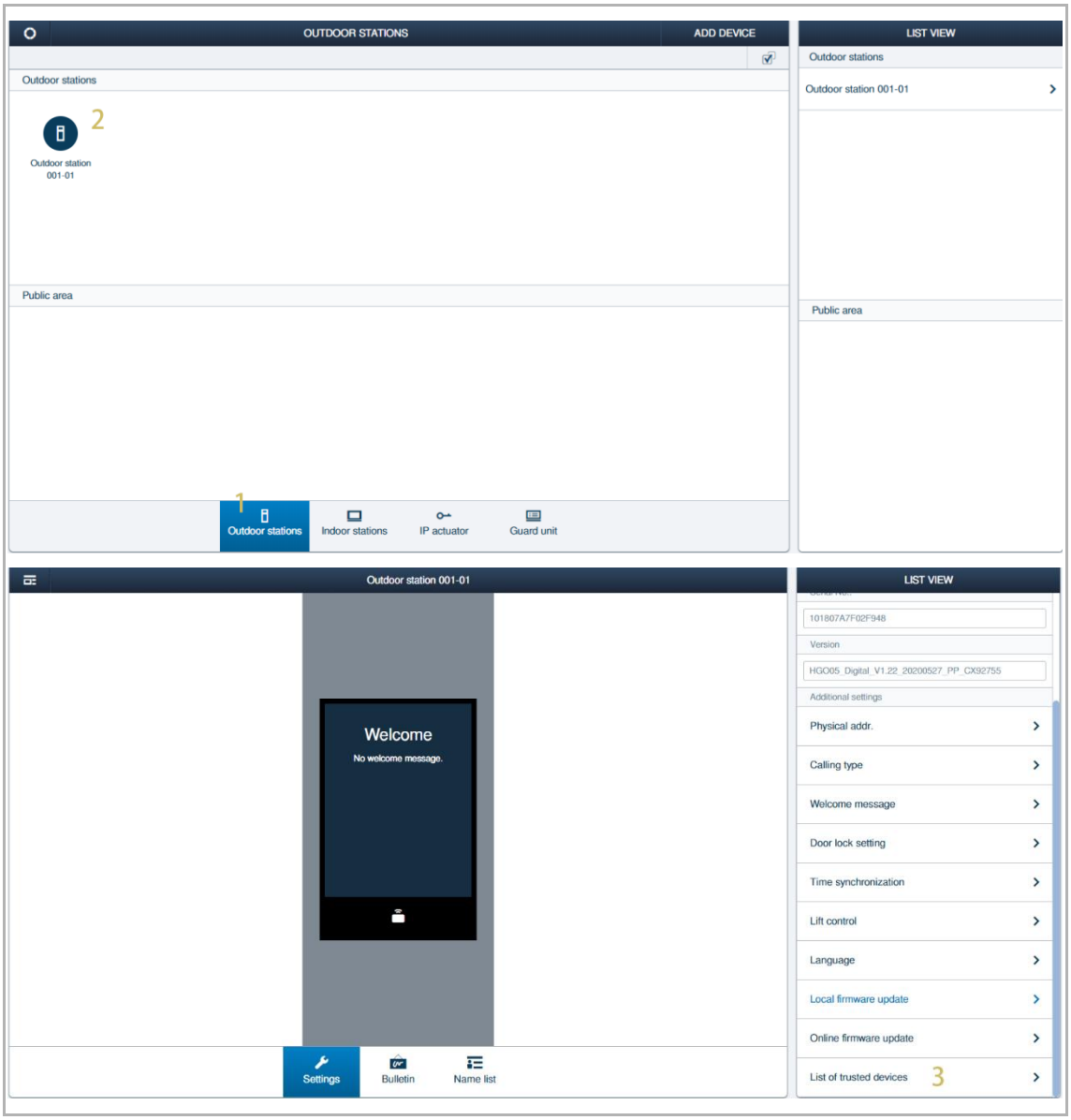
1. Trusting the designated outdoor stations

Please follow the steps below:

[1] On the "Door Entry System" screen, click "Outdoor stations".

[2] Click the designated outdoor station.

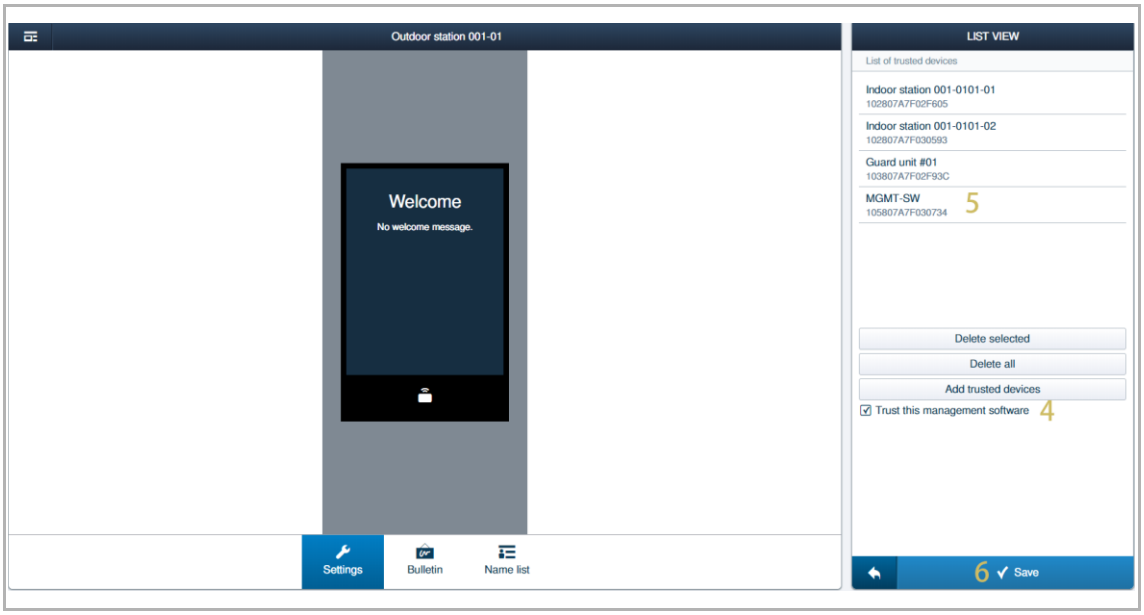
[3] Scroll down the list and click "List of trusted devices".



[4] Click "Trust this management software".

[5] The result is displayed on the list.

[6] Click " √ " to save.



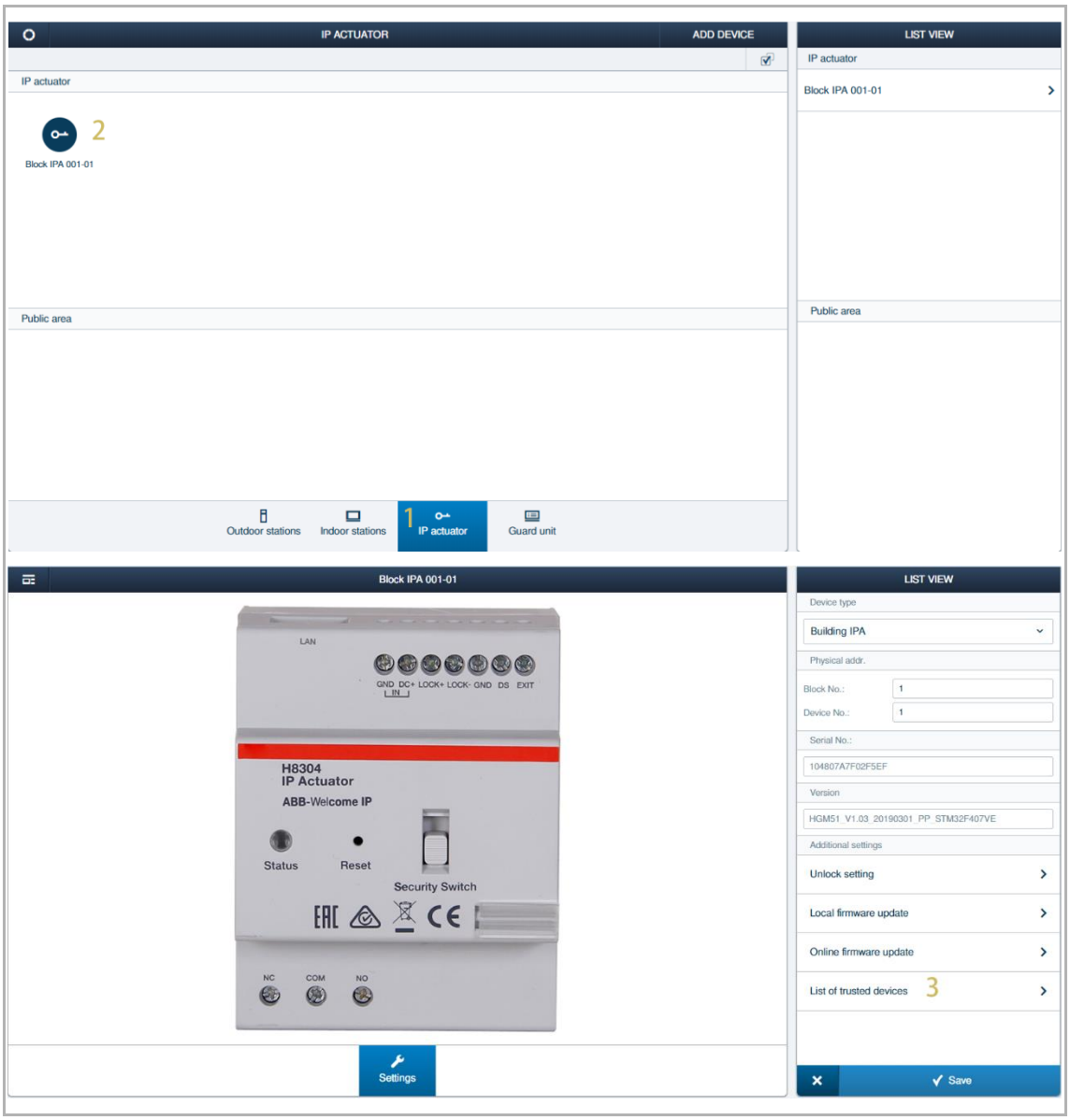
2. Trusting the designated IP Actuators

Please follow the steps below:

[1] On the "Door Entry System" screen, click "IP actuator".

[2] Click the designated IP actuator.

[3] Click "List of trusted devices".



[4] Click "Trust this management software".

[5] The result is displayed on the list.

[6] Click " √ " to save.

9.3.4 Emergency unlock

In some emergency cases, you may need to release all public doors. To achieve this, you need to add all outdoor stations and the all public IP actuators to "Smart Access Point".

see chapter 9.3.3 “Managing the trusted devices for "Smart Access Point"“ on page 112.

Release all public doors

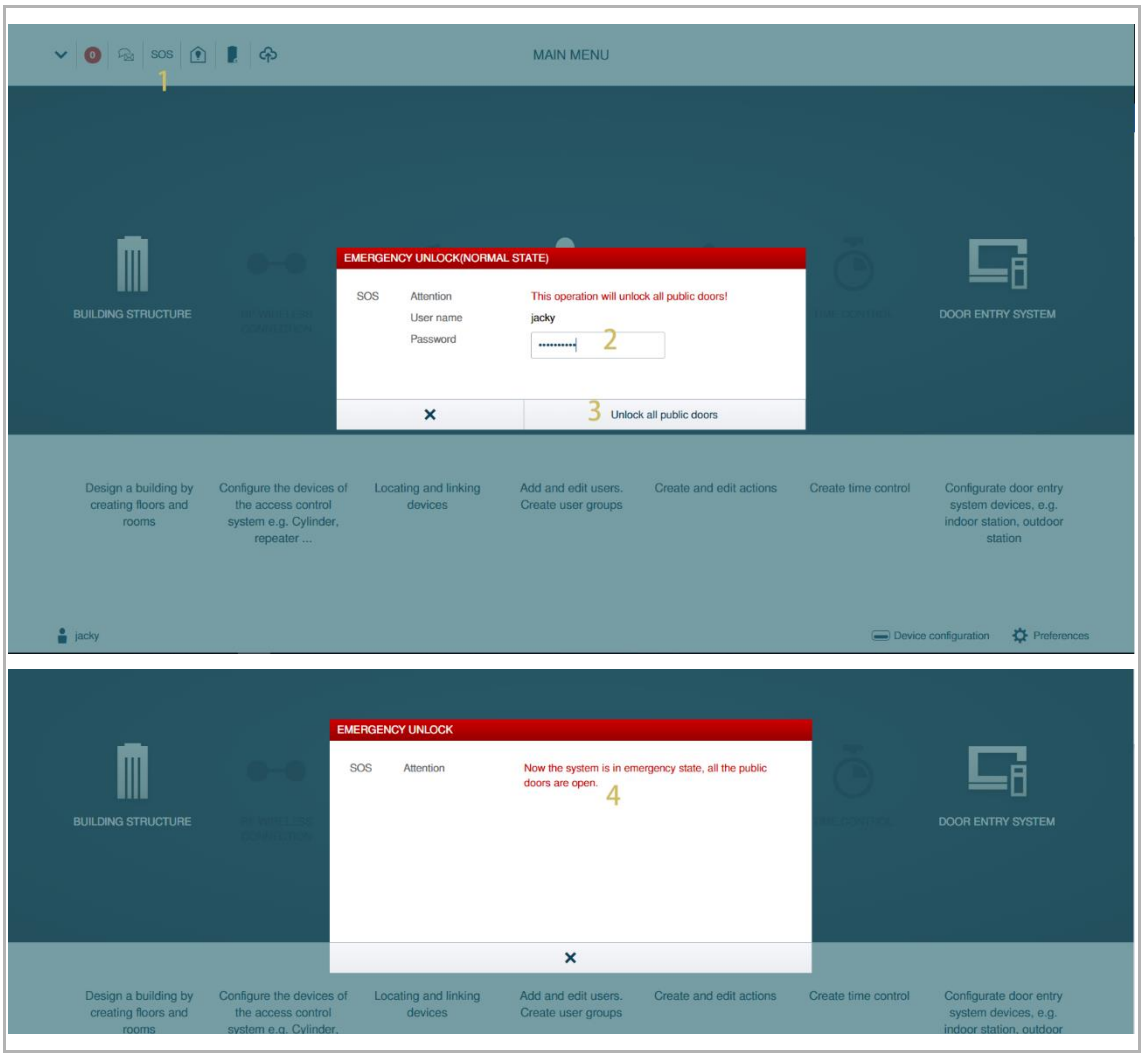
Please follow the steps below:

[1] On the configuration screen, click "SOS".

[2] Enter the password for current admin user.

[3] Click "Unlock all public doors".

[4] The result status is displayed on the screen.



Close all public doors

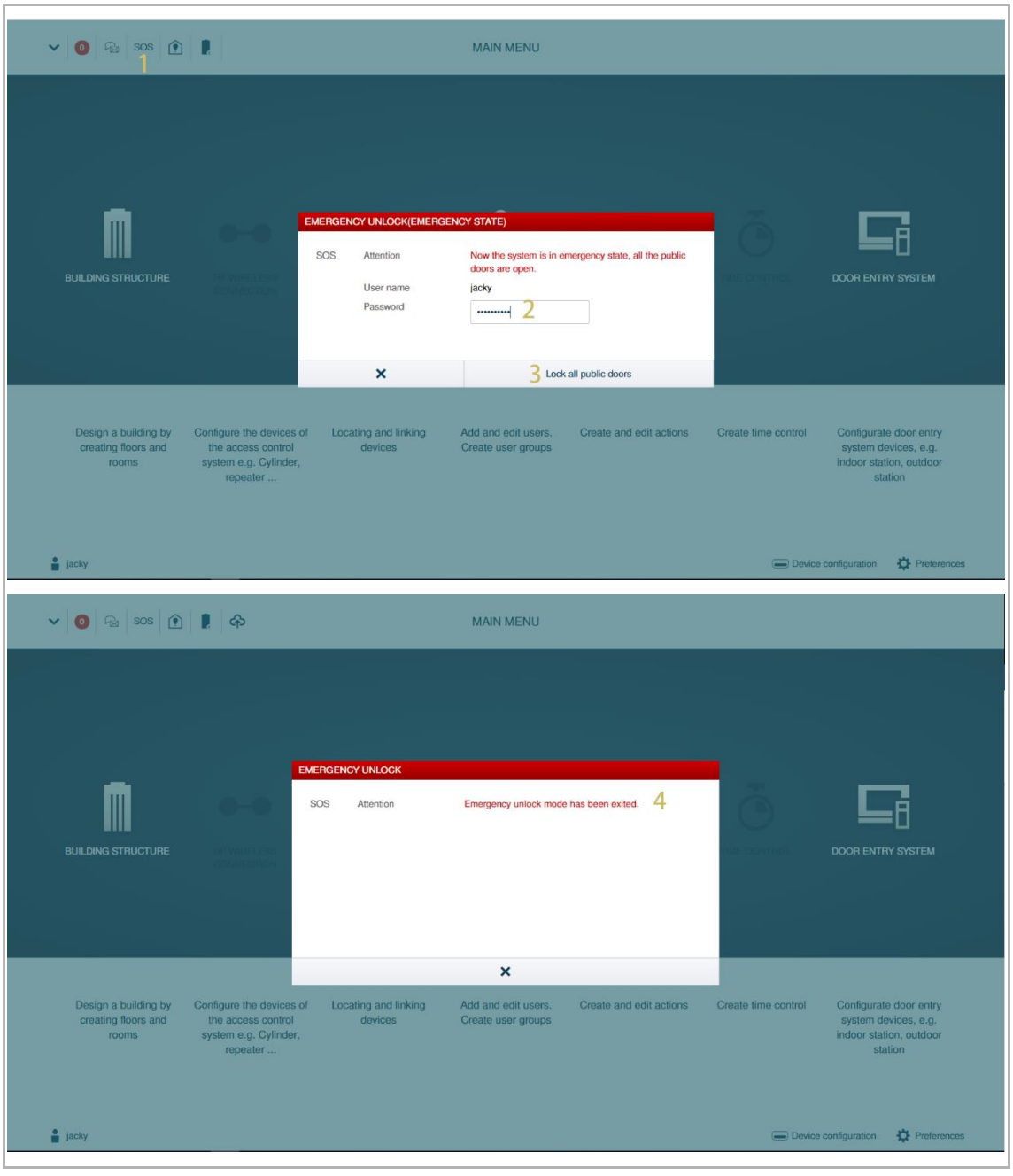
Please follow the steps below:

[1] On the configuration screen, click "SOS".

[2] Enter the password for the current admin user.

[3] Click "Lock all public doors".

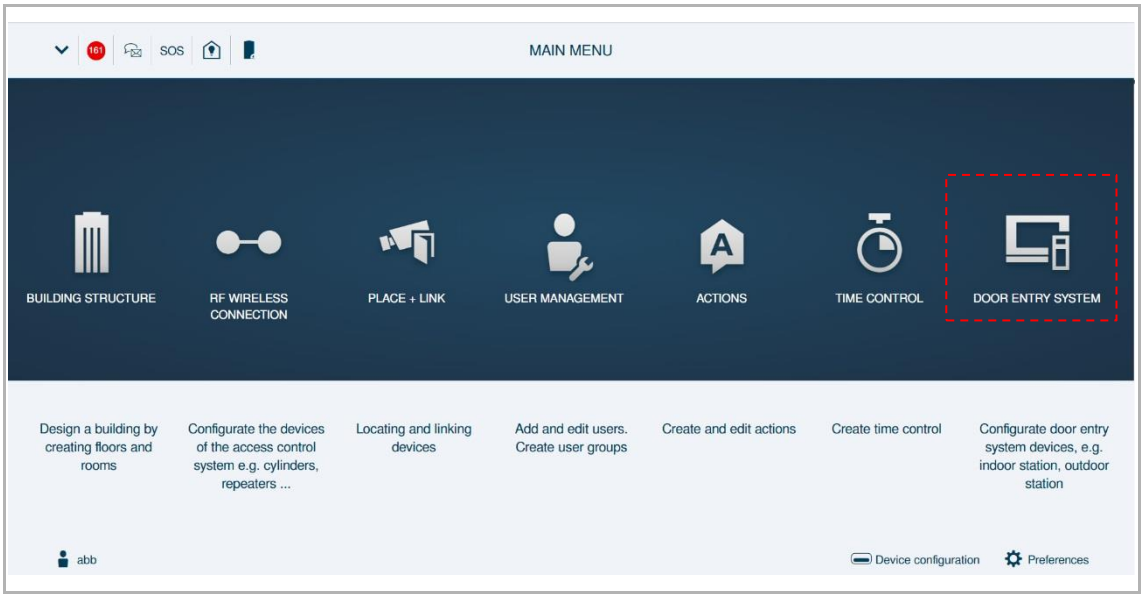
[4] The result status is displayed on the screen.



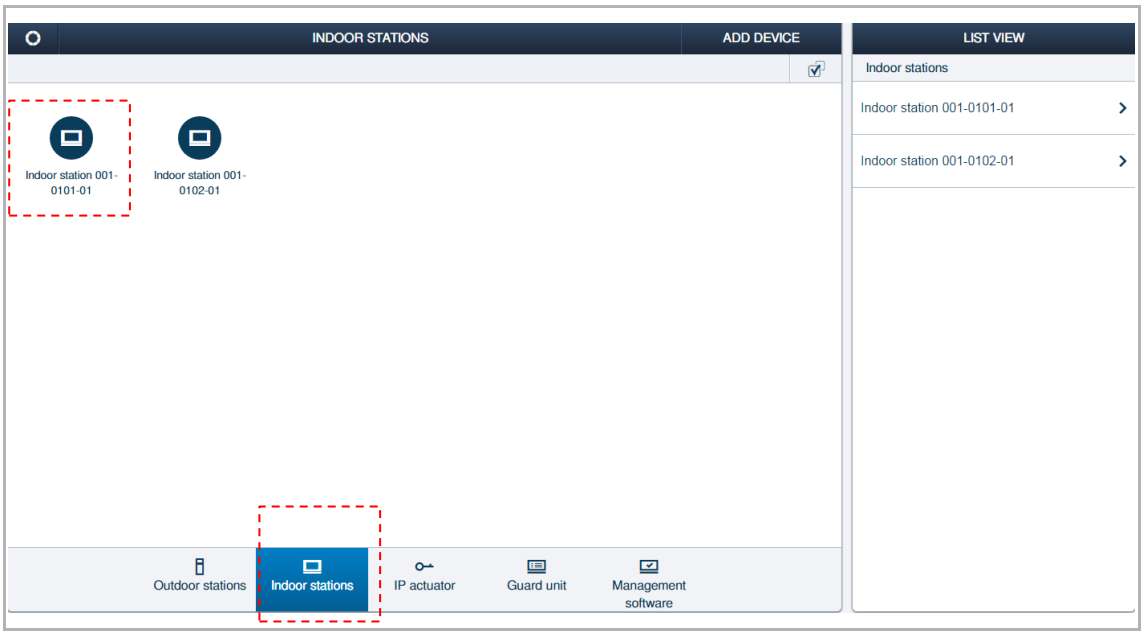
9.4 Configuring the indoor station

Access the designated Indoor station screen

On the configuration screen, click "Door entry system", followed by "Indoor stations" to access the "Indoor stations" screen.



On the "Indoor stations" screen, click the designated indoor station to access the designated indoor station screen.



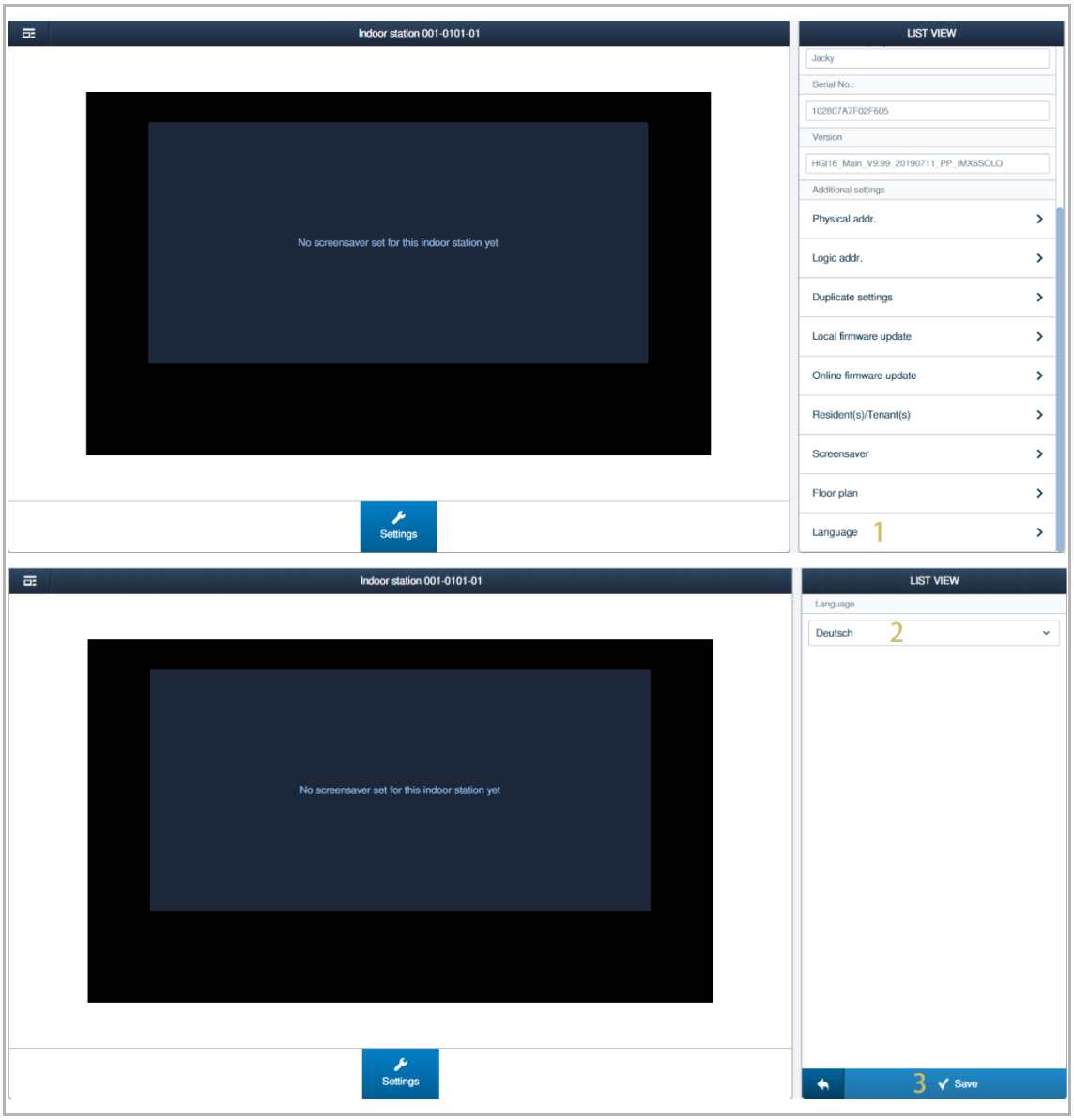
9.4.1 Changing the language

Please follow the steps below:

[1] On the designated indoor station screen, click "Language".

[2] Select the language from the drop-down list.

[3] Click " √ " to save.



9.4.2 Renaming the device

Please follow the steps below:

[1] On the designated indoor station screen, click "Resident(s)/Tenant(s)".

[2] Enter the first name.

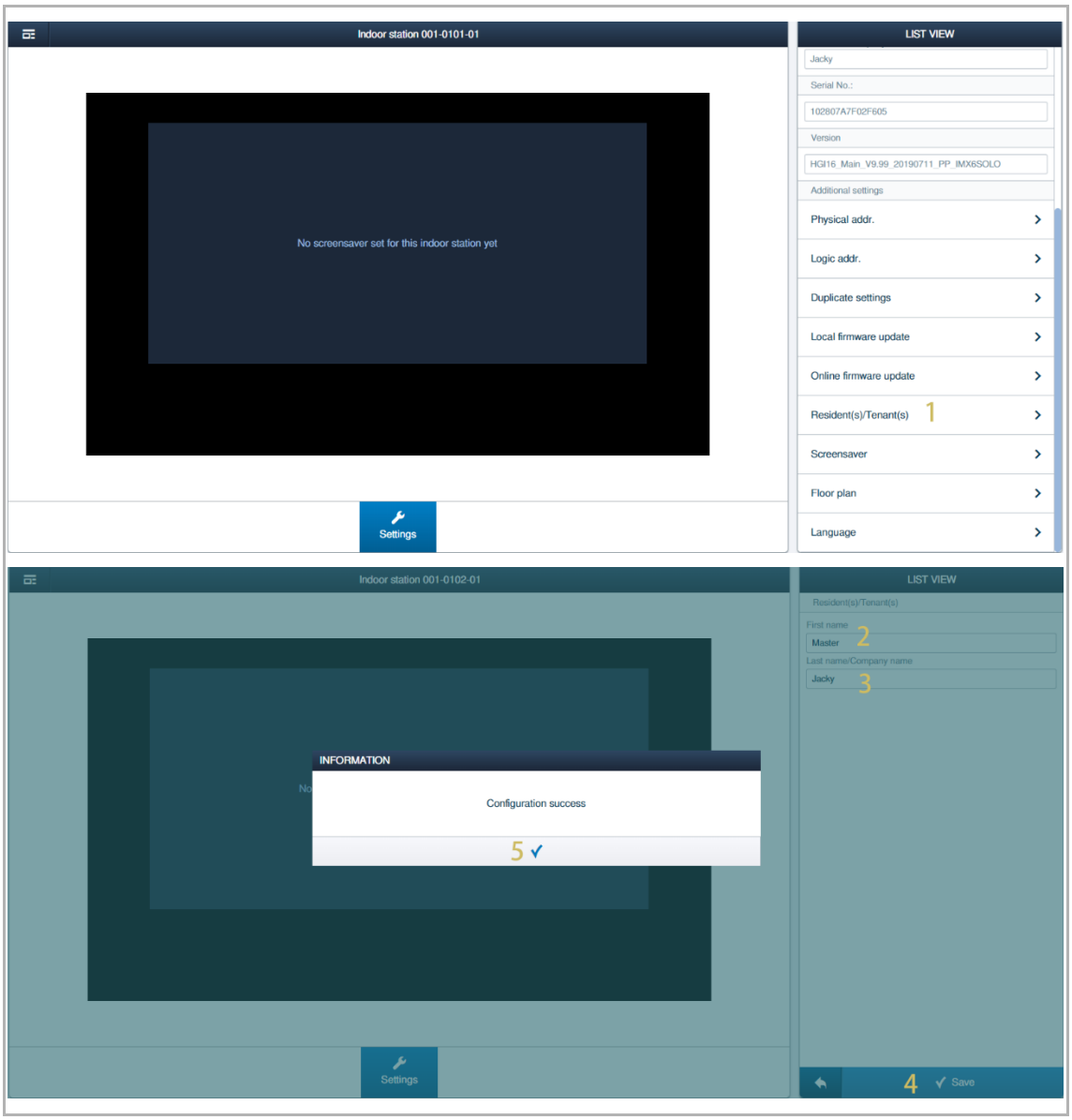
[3] Enter the last name or the company name.

Note

If the resident has multiple indoor stations in the apartment, it is recommended to use the appropriate name to show the association (e.g. "Master", "Slave 1" etc.).

[4] Click " √ " to save.

[5] Click " √ " to confirm.

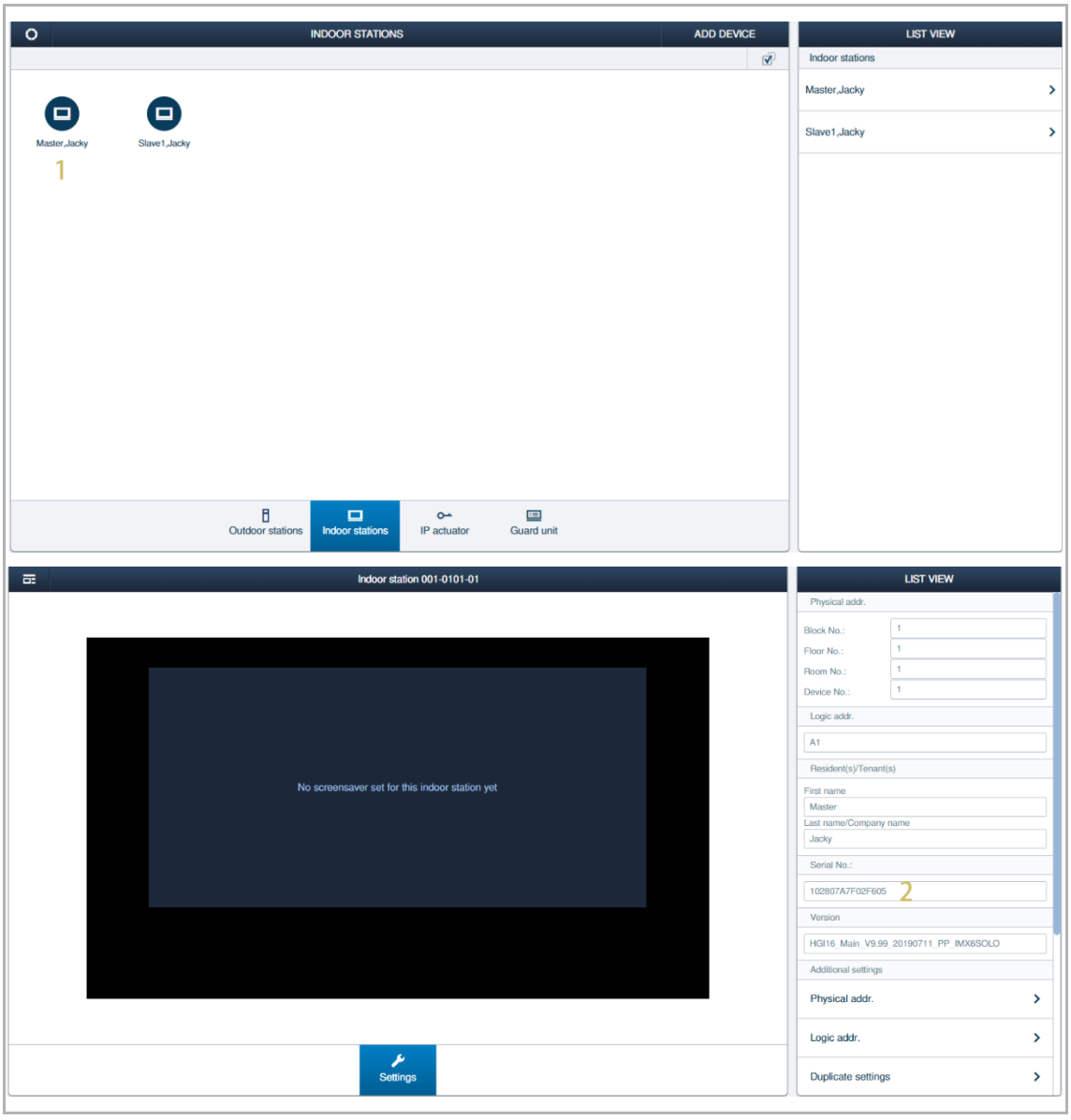


9.4.3 Viewing the serial number

Please follow the steps below:

[1] On the "Indoor stations" screen, click the designated indoor staiton.

[2] The serial number is displayed on the screen. It is recommended to write down the serial number for futher use.



9.4.4 Managing the physical address

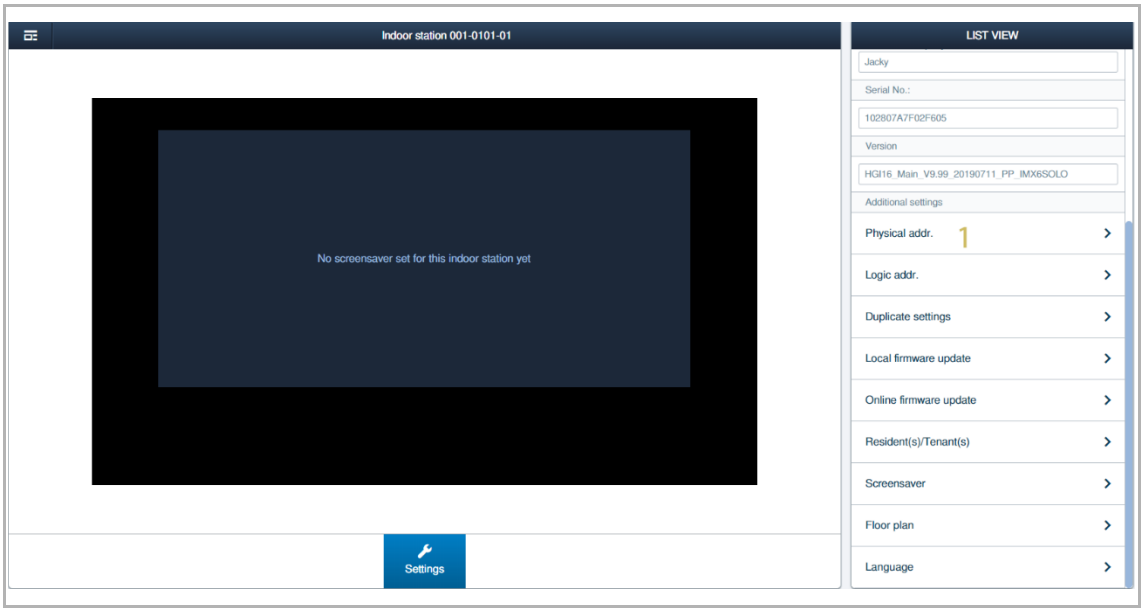
Note

If the master indoor station changes its physical address, the slave indoor stations need to obtain the signature again from "Smart Access Point".

Please write down the serial number of the slave indoor stations before changing the physical address. see chapter 9.4.3 “Viewing the serial number“ on page 121.

Please follow the steps below:

[1] On the master indoor station screen, click "Physical addr.".



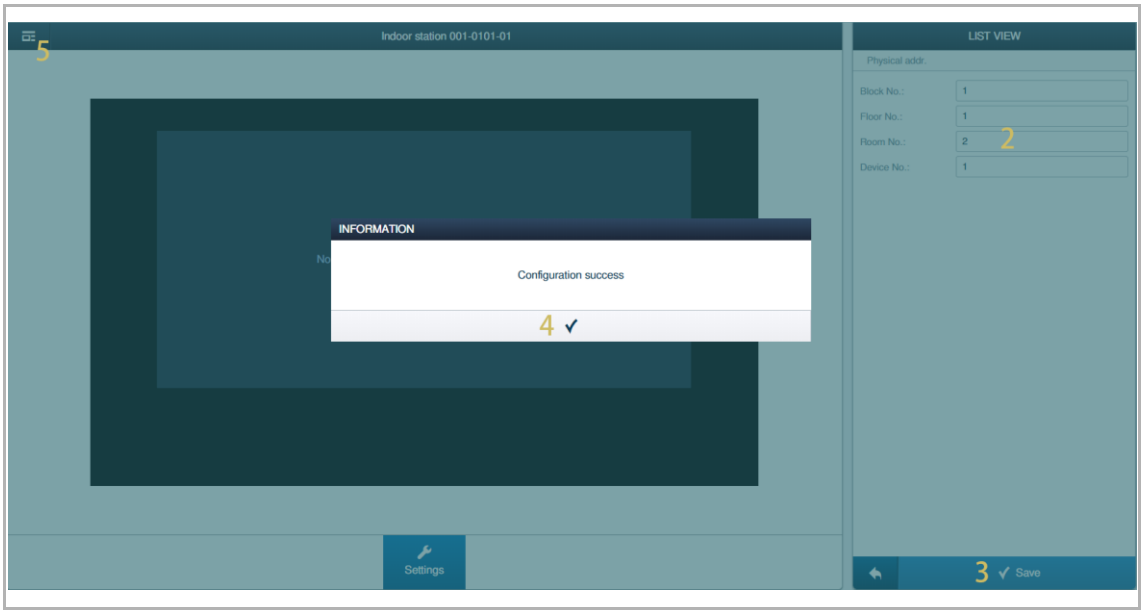
[2] Change the physical address.

[3] Click " √ " to save.

[4] Click " √ " to confirm.

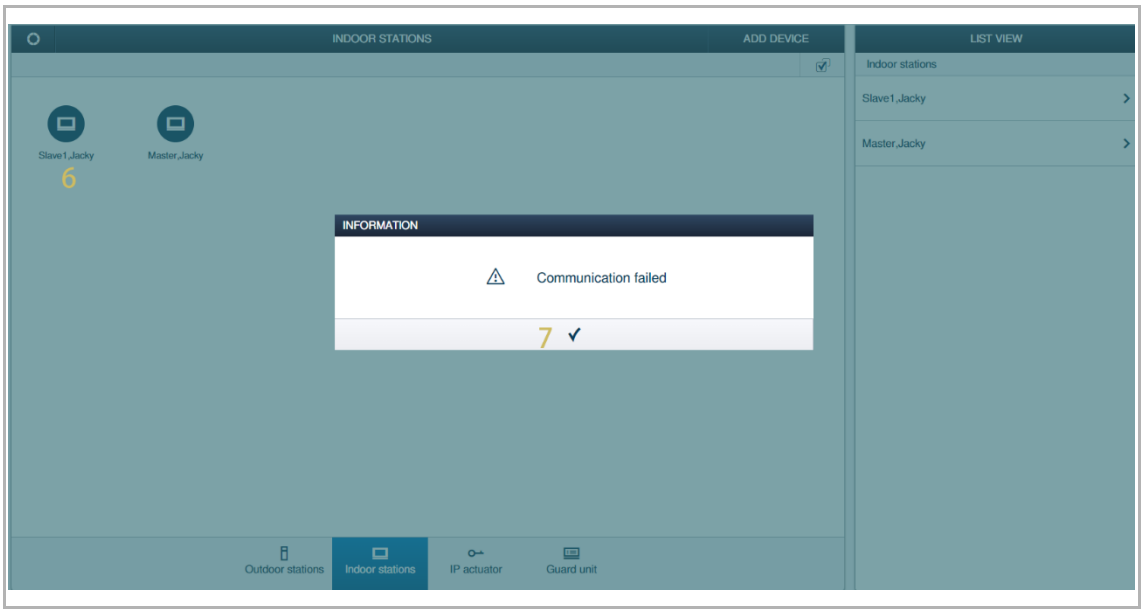
It there are no slave indoor stations, the change process is completed at step 4. Otherwise, please continue with the next steps.

[5] Click "  " to turn back to "Indoor stations" screen.

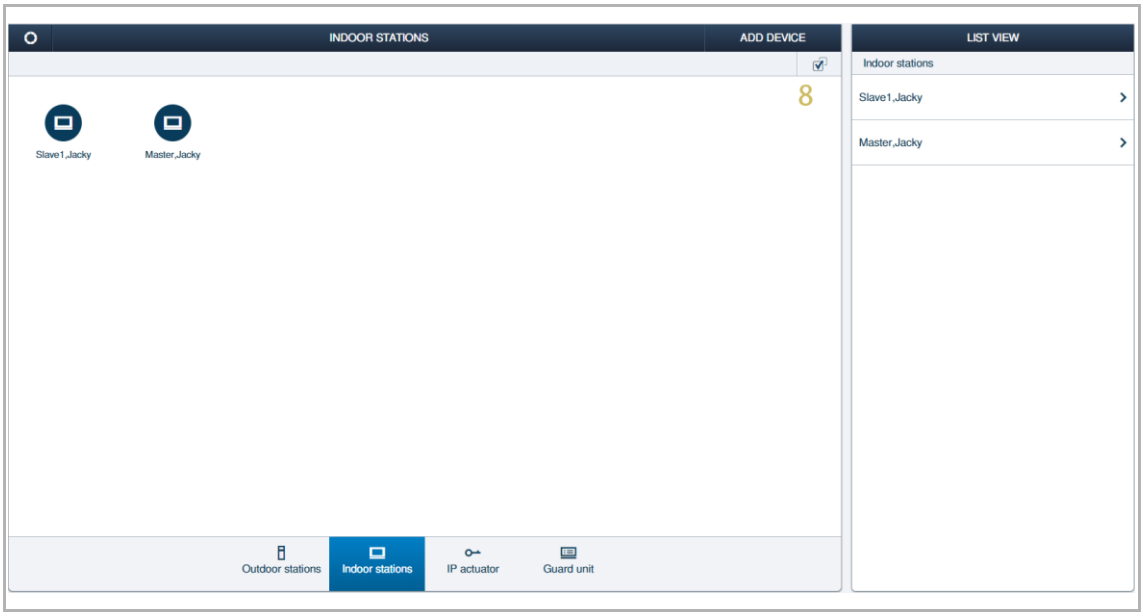


[6] Click the slave indoor station.

[7] The slave indoor station failed to access the screen due to the signature is removed automatically. Click " √ " to continue.



[8] On the "Indoor stations" screen, click "  ".



[9] Click the slave indoor station.

[10]Click "Delete".

[11]Click "Confirm", followed by " √ ".

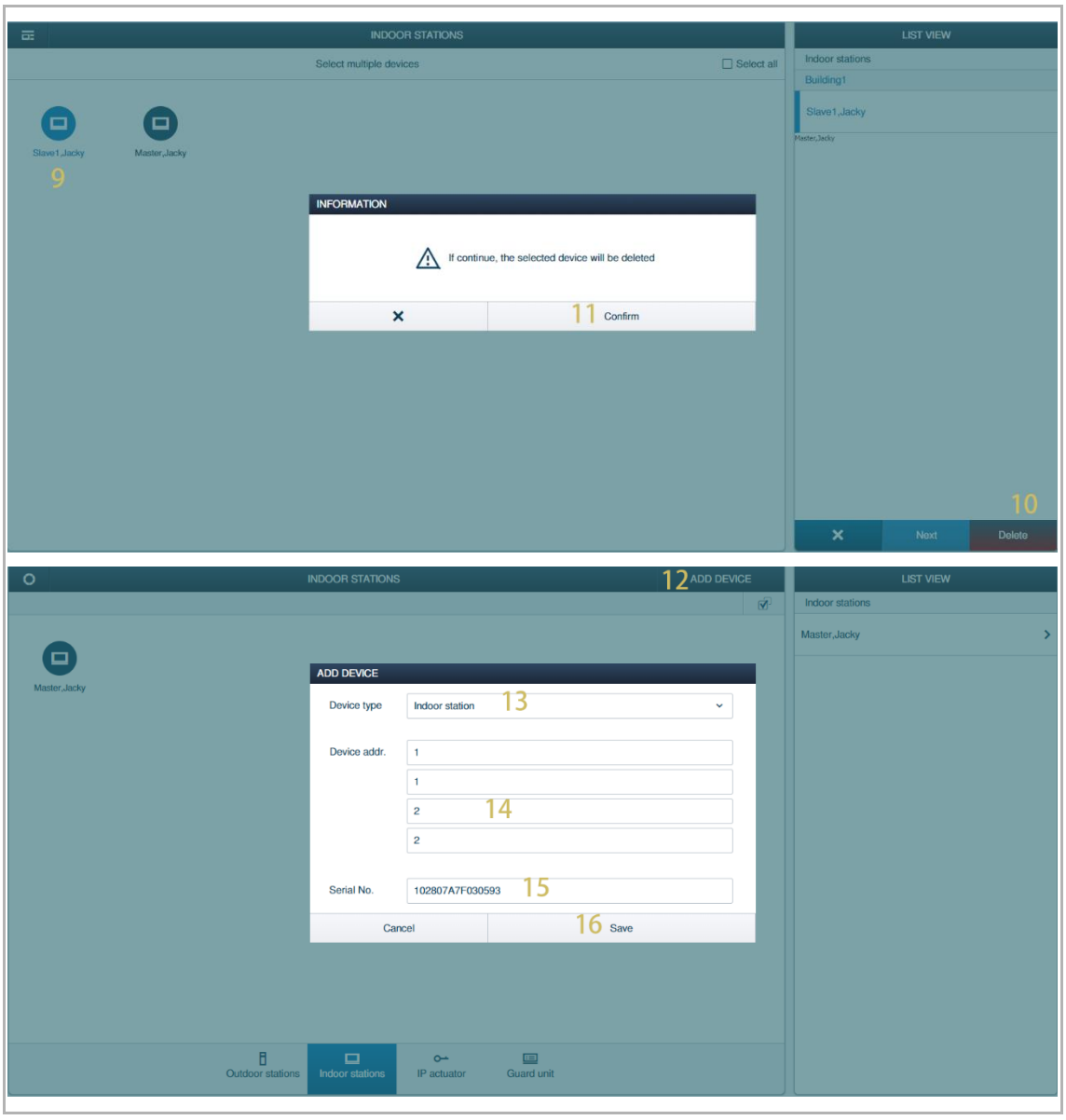
[12]On the "Indoor stations" screen, click "Add device".

[13]Set "Device type" to "Indoor station".

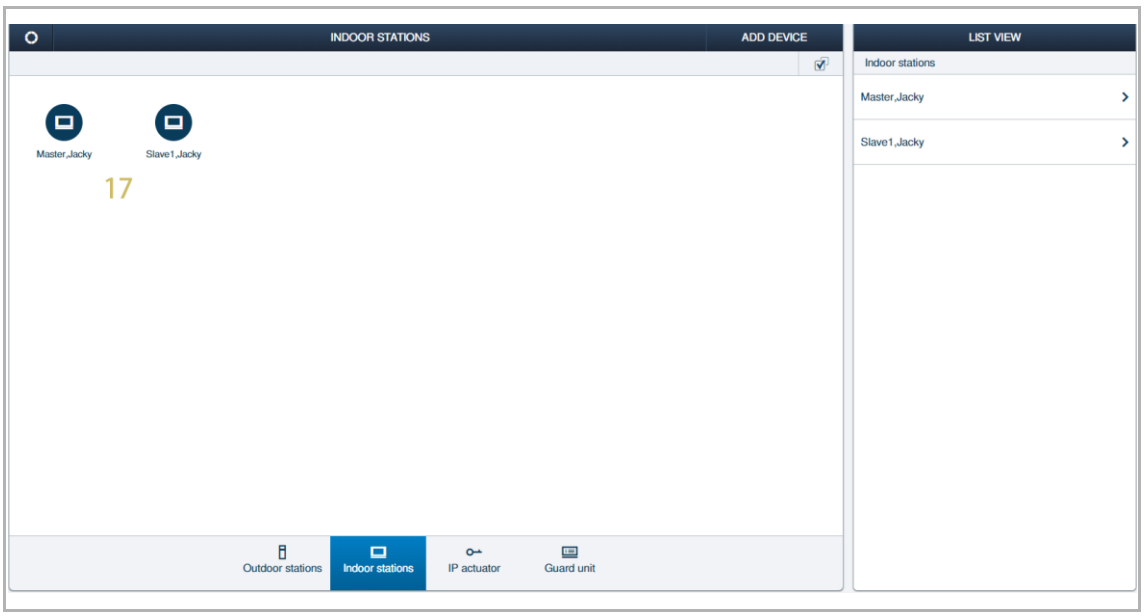
[14]Enter the new physical address of the slave indoor station.

[15]Enter the serial number of the slave indoor station.

[16]Click "Save", followed by " √ ".



[17]Rename the slave indoor station. see chapter 9.4.2 “Renaming the device“ on page 120.



9.4.5 Managing the logic address

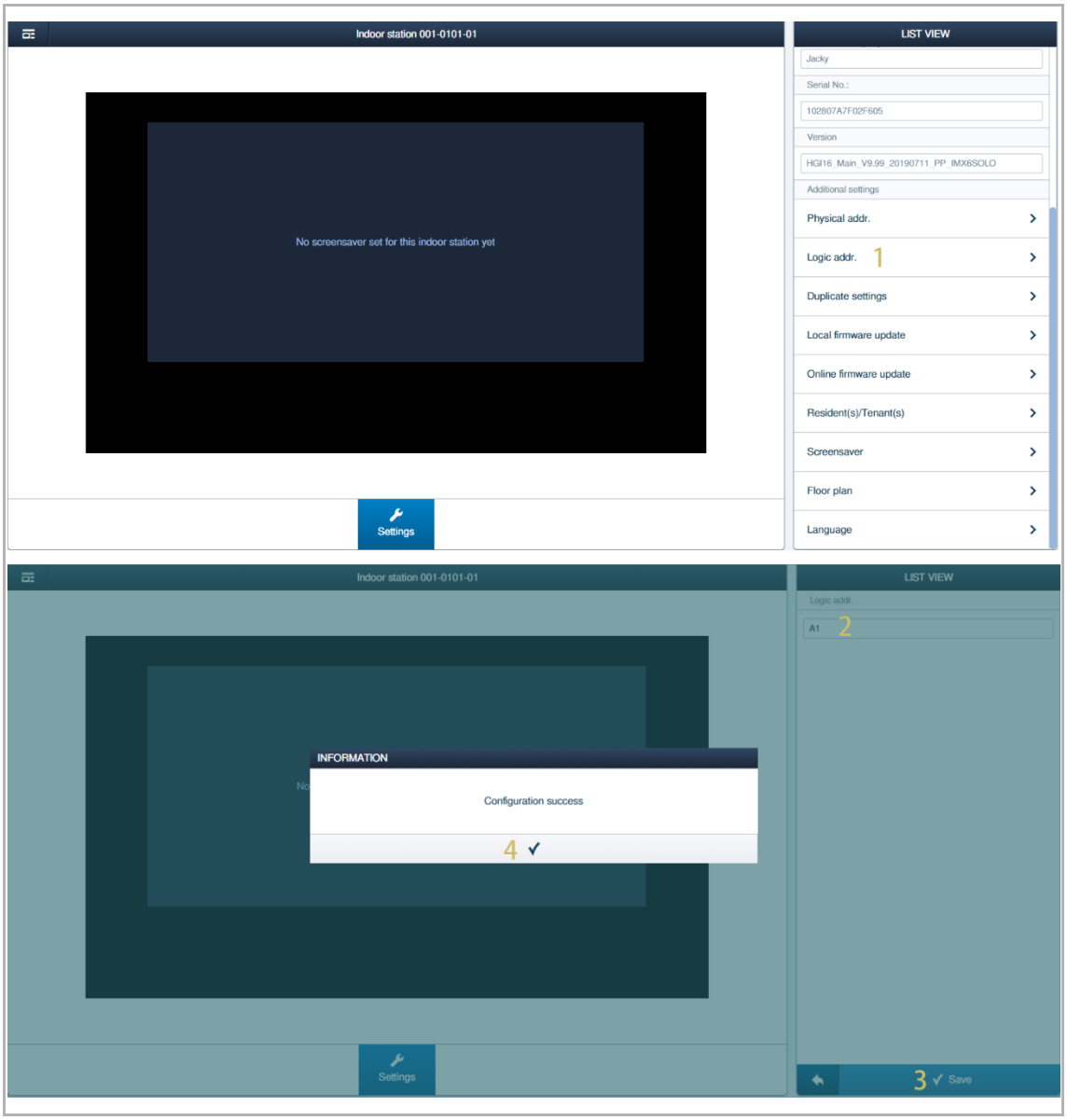
Please follow the steps below:

[1] On the master indoor station screen, click "Logic addr.".

[2] Enter the logic address. The address could not be the same to the exist one on "Smart Access Point".

[3] Click "√" to save.

[4] Click "√" to confirm.



Note

The logic address set on the indoor station can be used on the outdoor station.
see chapter 9.4.5 “Managing the logic address“ on page 127.

9.4.6 Managing the screensaver

Please follow the steps below:

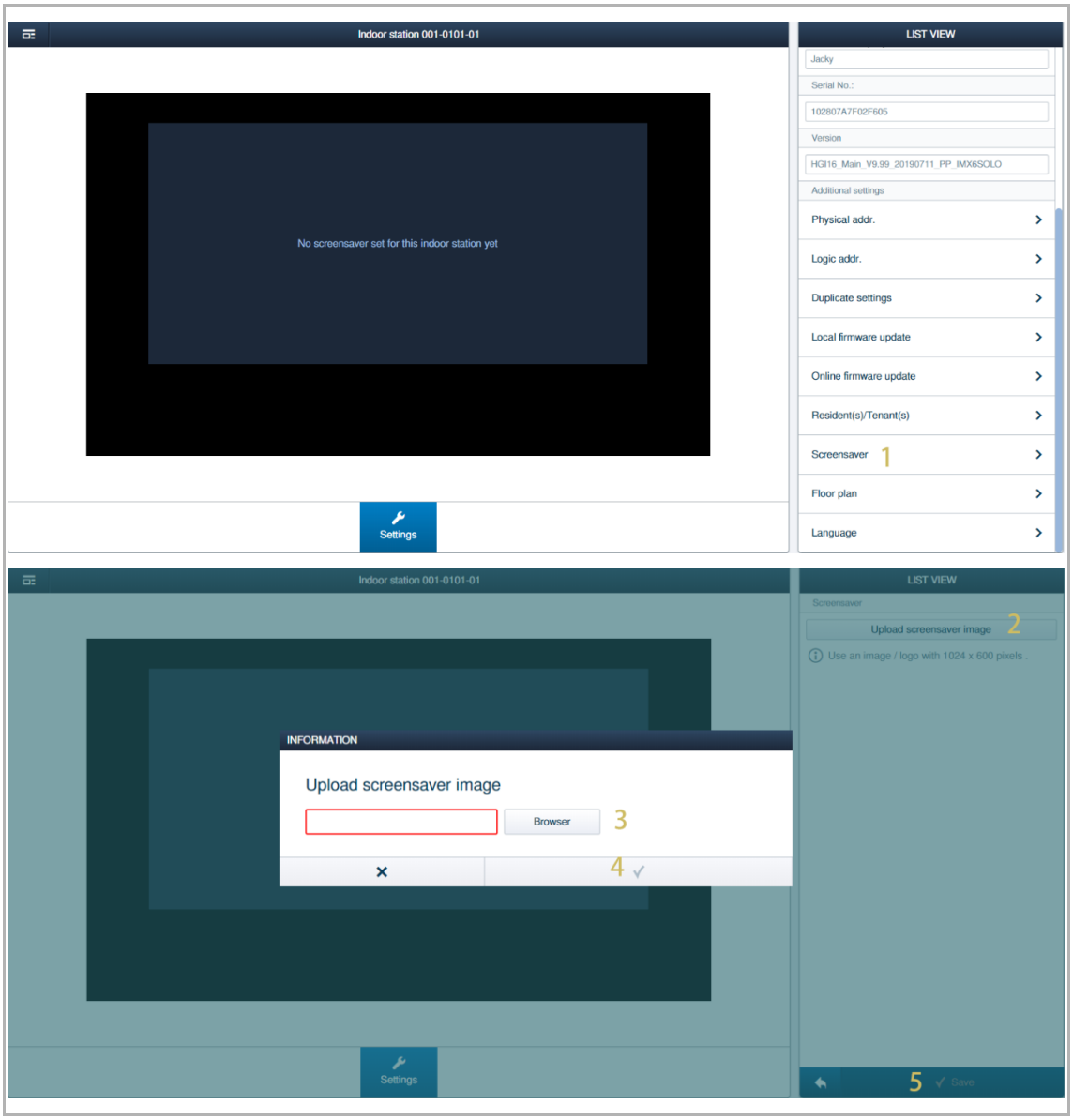
[1] On the master indoor station screen, click "Screensaver".

[2] Click "Upload screensaver image".

[3] Click "Browse" to select the desiganted image (only .jpg is supported, maximum resolution of the image is 1024 x 600 pixels).

[4] Click " √ " to confirm.

[5] Click " √ " to upload.



9.4.7 Managing the floorplan

Please follow the steps below:

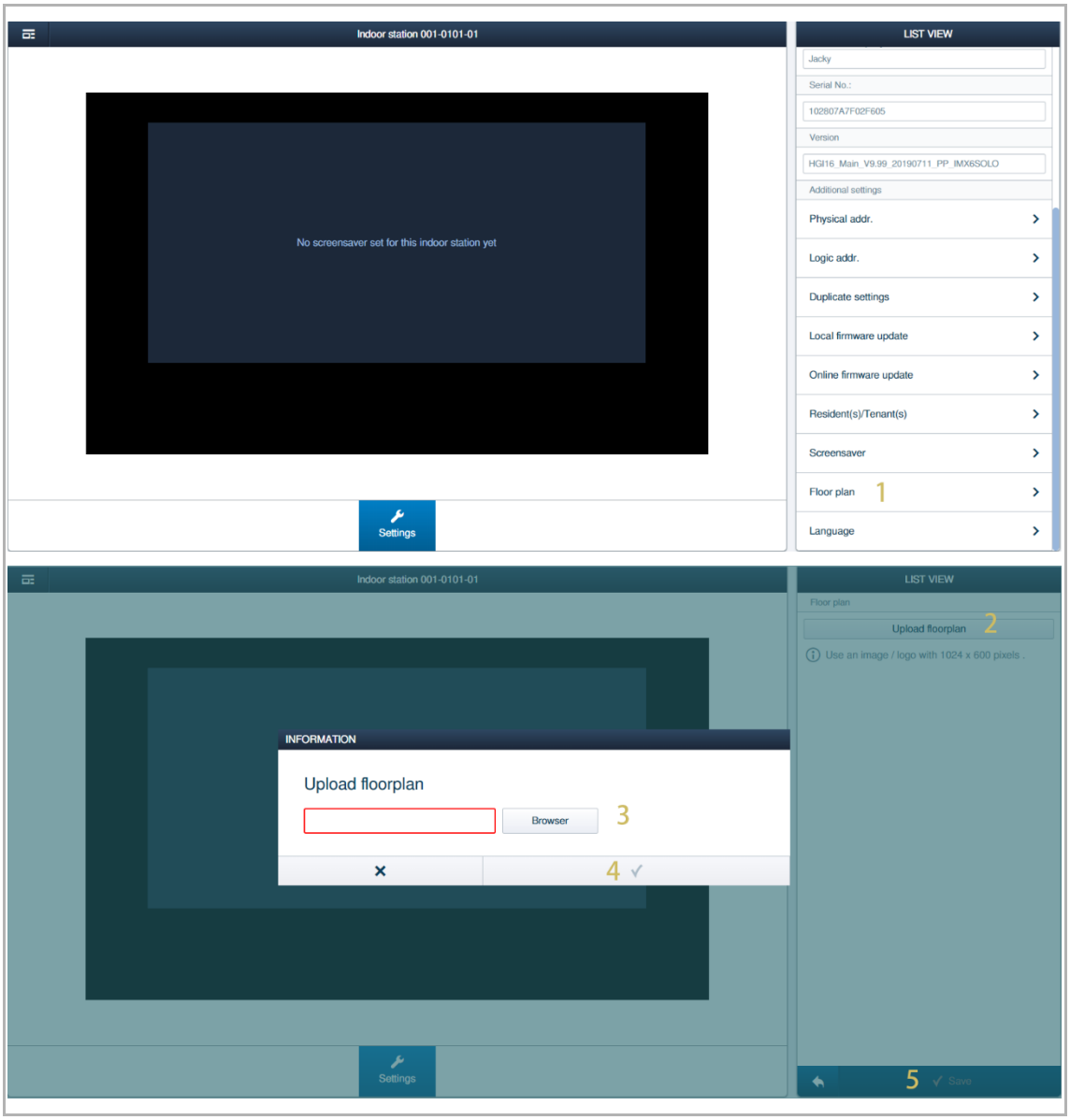
[1] On the master indoor station screen, click "Floor plan".

[2] Click "Upload floorplan".

[3] Click "Browse" to select the desiganted image (only .jpg is supported, maximum resolution of the image is 1024 x 600 pixels).

[4] Click " √ " to confirm.

[5] Click " √ " to upload.



9.4.8 Duplicating the settings

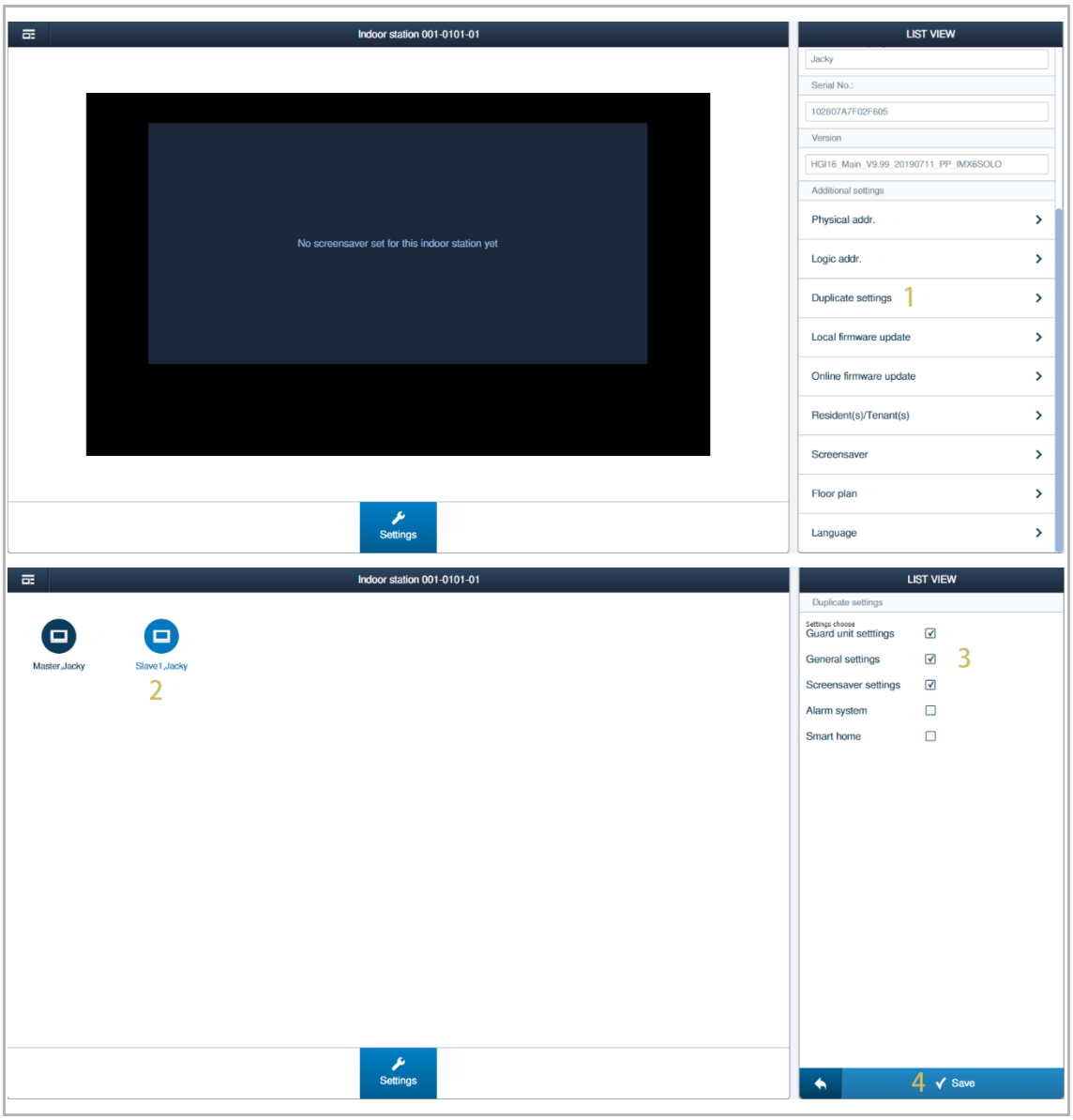
Please follow the steps below:

[1] On the master indoor station screen, click "Duplicate settings".

[2] Click to select the designated indoor station to be dupliacted.

[3] Tick the check boxes to select the settings to be duplicated.

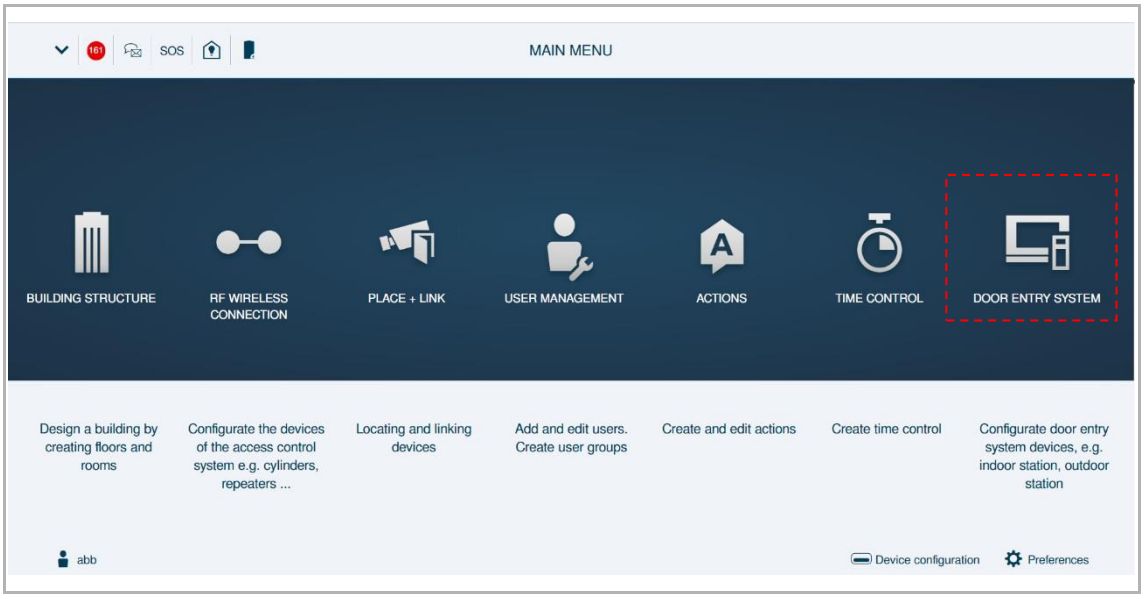
[4] Click "√" to confirm.



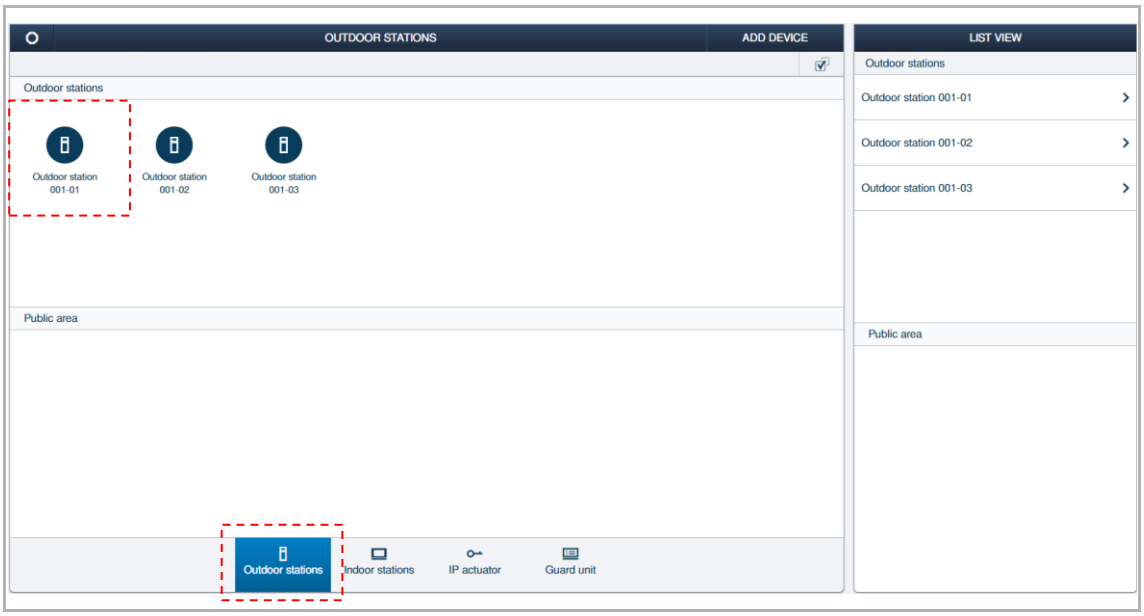
9.5 Configuring the Outdoor Station

Access the designated outdoor station screen

On the configuration screen, click "Door entry system", followed by "Outdoor stations" to access the "Outdoor stations" screen.



On the "Outdoor stations" screen, click the designated outdoor station to access the corresponding screen.



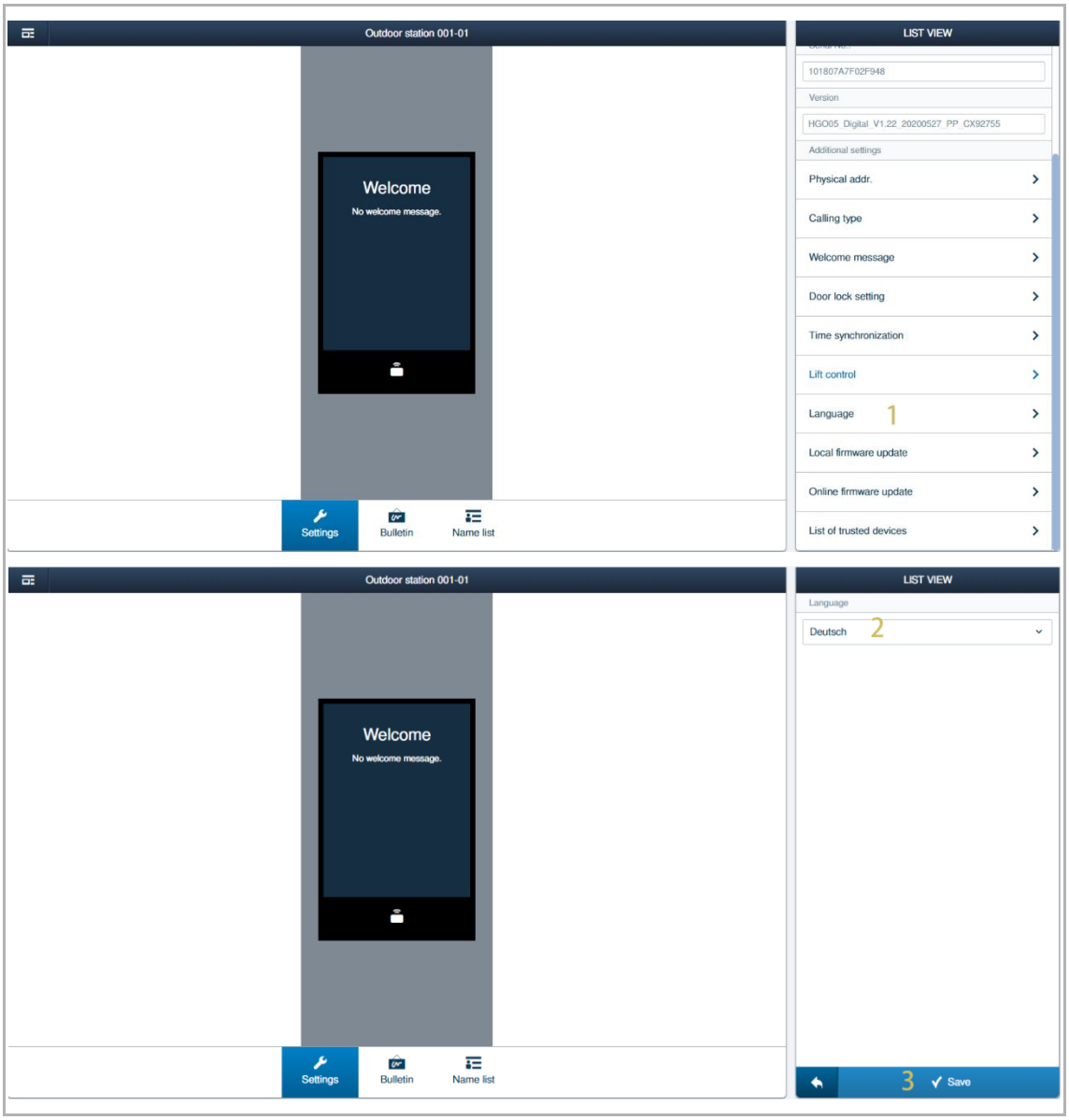
9.5.1 Changing the language

Please follow the steps below:

[1] On the designated outdoor station screen, click "Language".

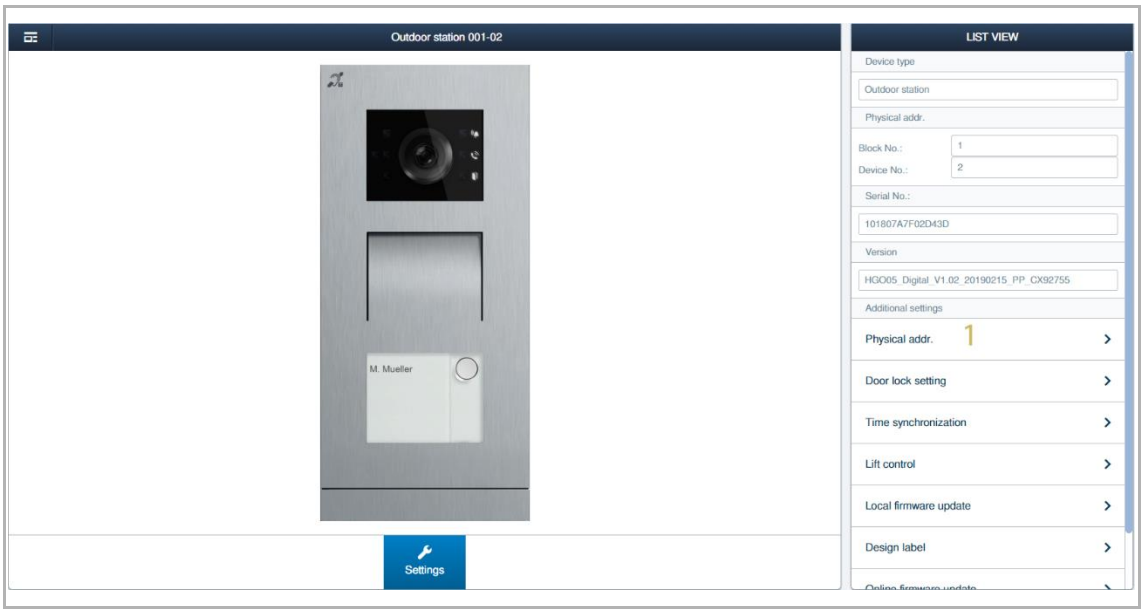
[2] Select the language from the drop-down list.

[3] Click " √ " to save.



9.5.2 Managing the physical address

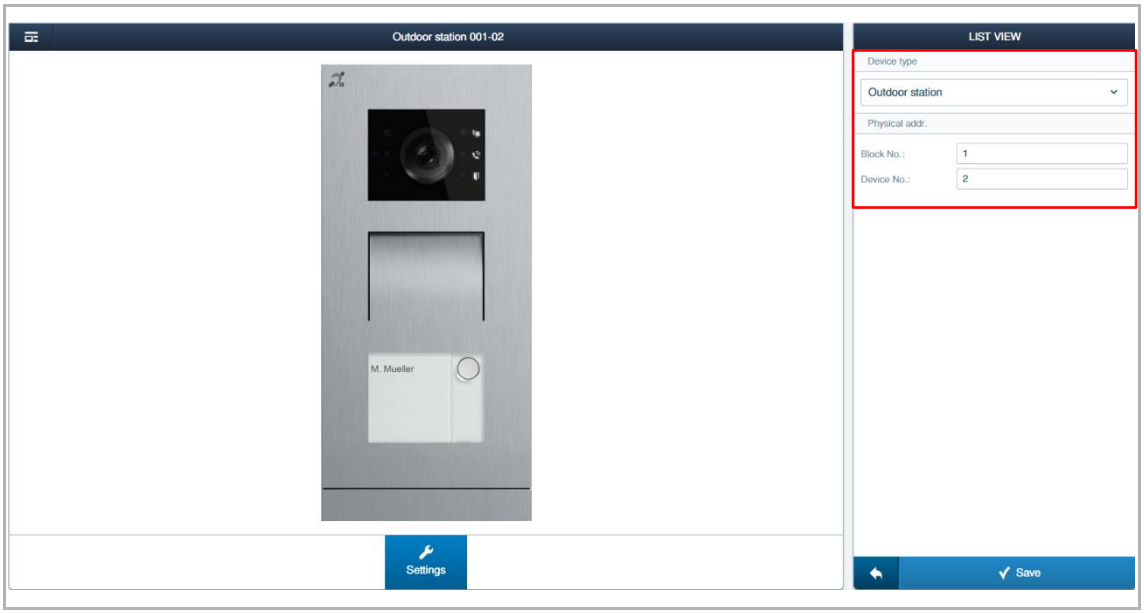
On the designated outdoor station screen, click "Physical address".



There are 3 types devices for selection.

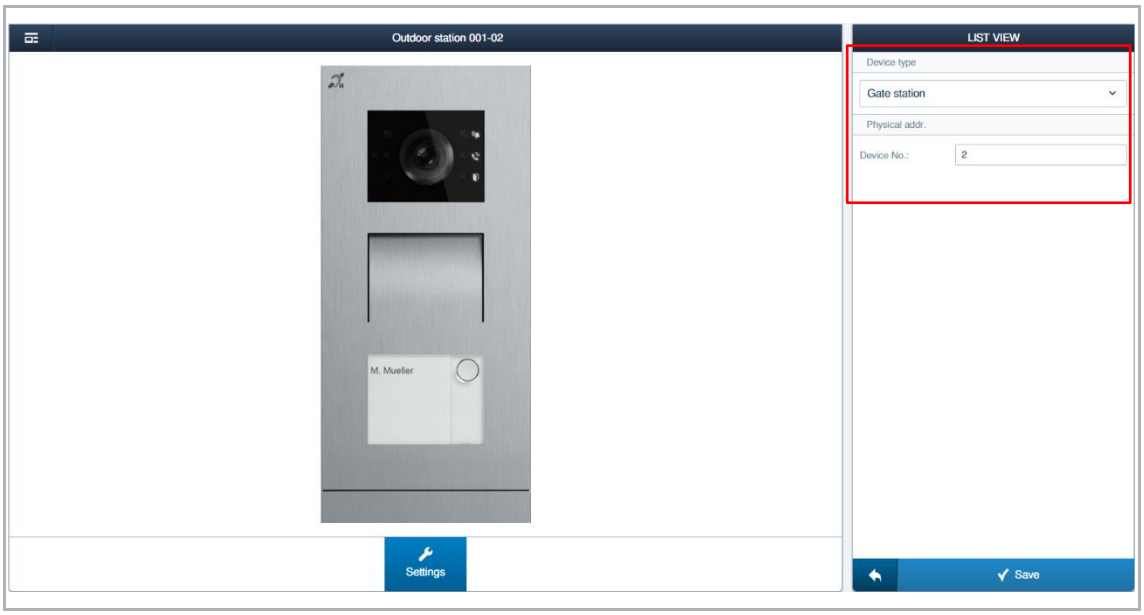
1. Outdoor station

If the "Device type" is set to "Outdoor station", you need to set the block number and the device number.



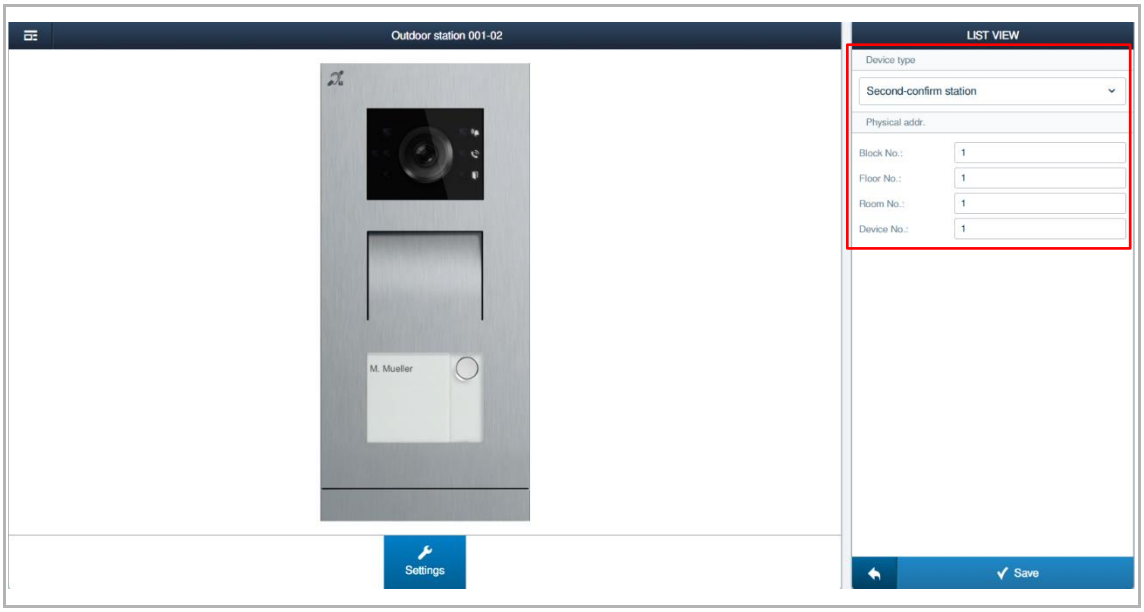
2. Gate station

If the "Device type" is set to "Gate station", you need to set the block number and the device number.



3. Second-confirm station

If the "Device type" is set to "Second-confirm station", you need to set the block number, the floor number, the room number and the device number.



Note

Only IP pushbutton outdoor station can be set to "Second-confirm station".

9.5.3 Surveillance call

If the "Surveillance call" function is disabled, the indoor station & App will not support a surveillance call.

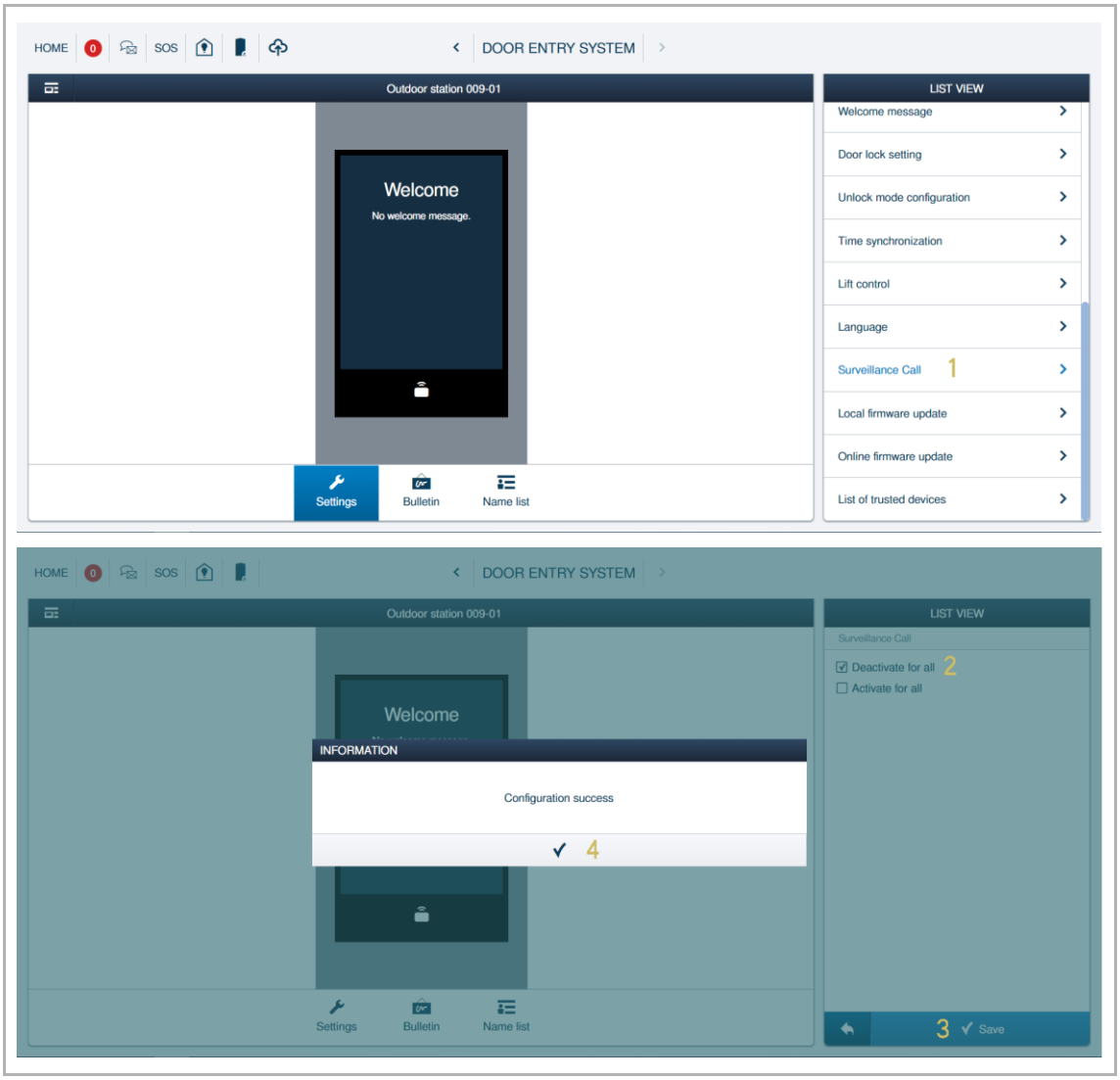
Please follow the steps below to deactivate the function:

[1] On the designated outdoor station screen, click "Surveillance call".

[2] Tick the check box "Deactivate for all".

[3] Click "Save".

[4] Click "√".



9.5.4 Unlock setting

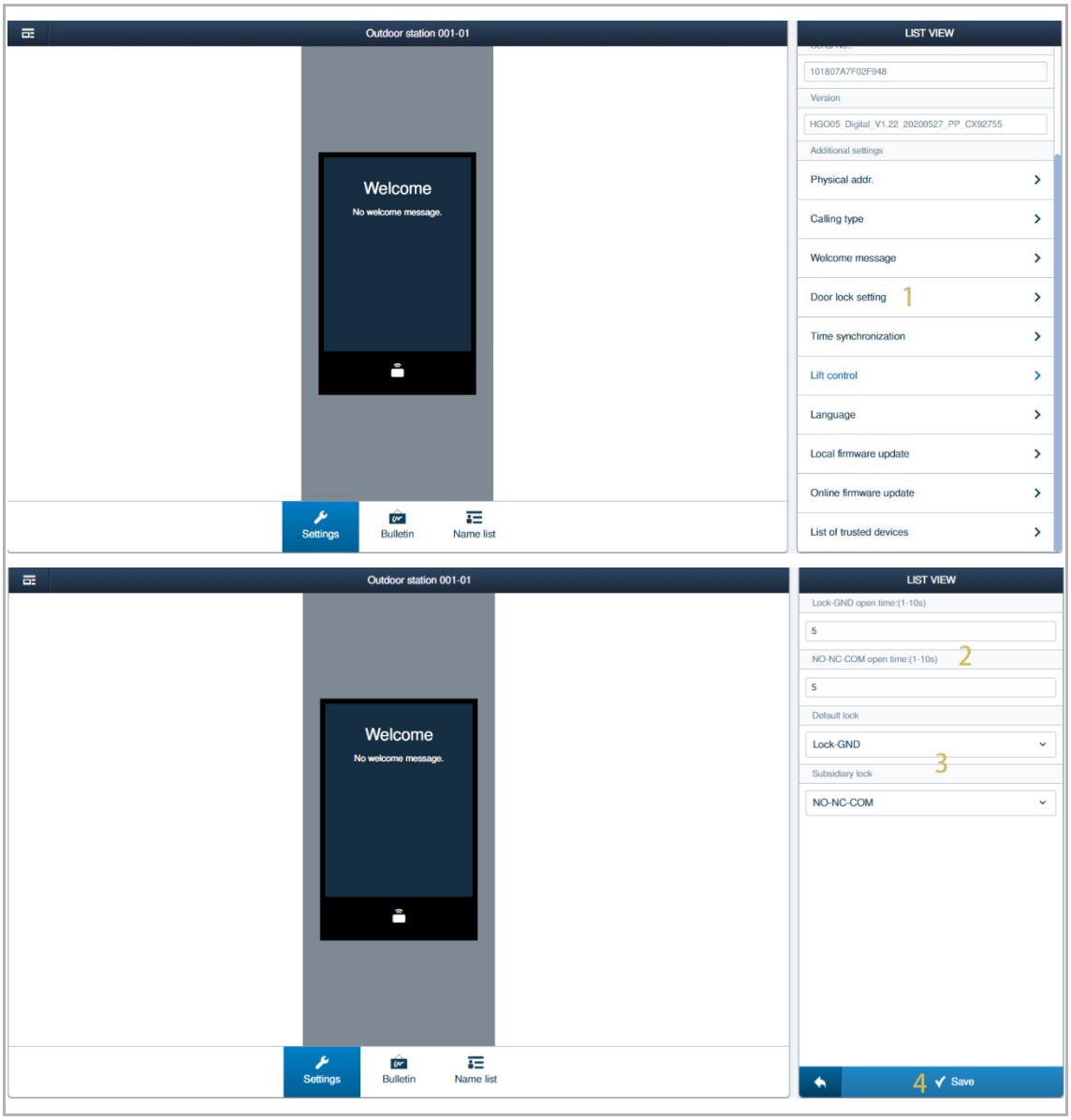
Please follow the steps below:

[1] On the designated outdoor station screen, click "Door lock setting".

[2] Set the unlock time for the locks.

[3] Set the lock type for the locks.

[4] Click "√" to save.



9.5.5 Set outdoor station as SIP client

9.5.6 Configuring IP touch 5 outdoor station

IP touch 5 outdoor station needs to be configured before using SIP function.

1. SIP client settings

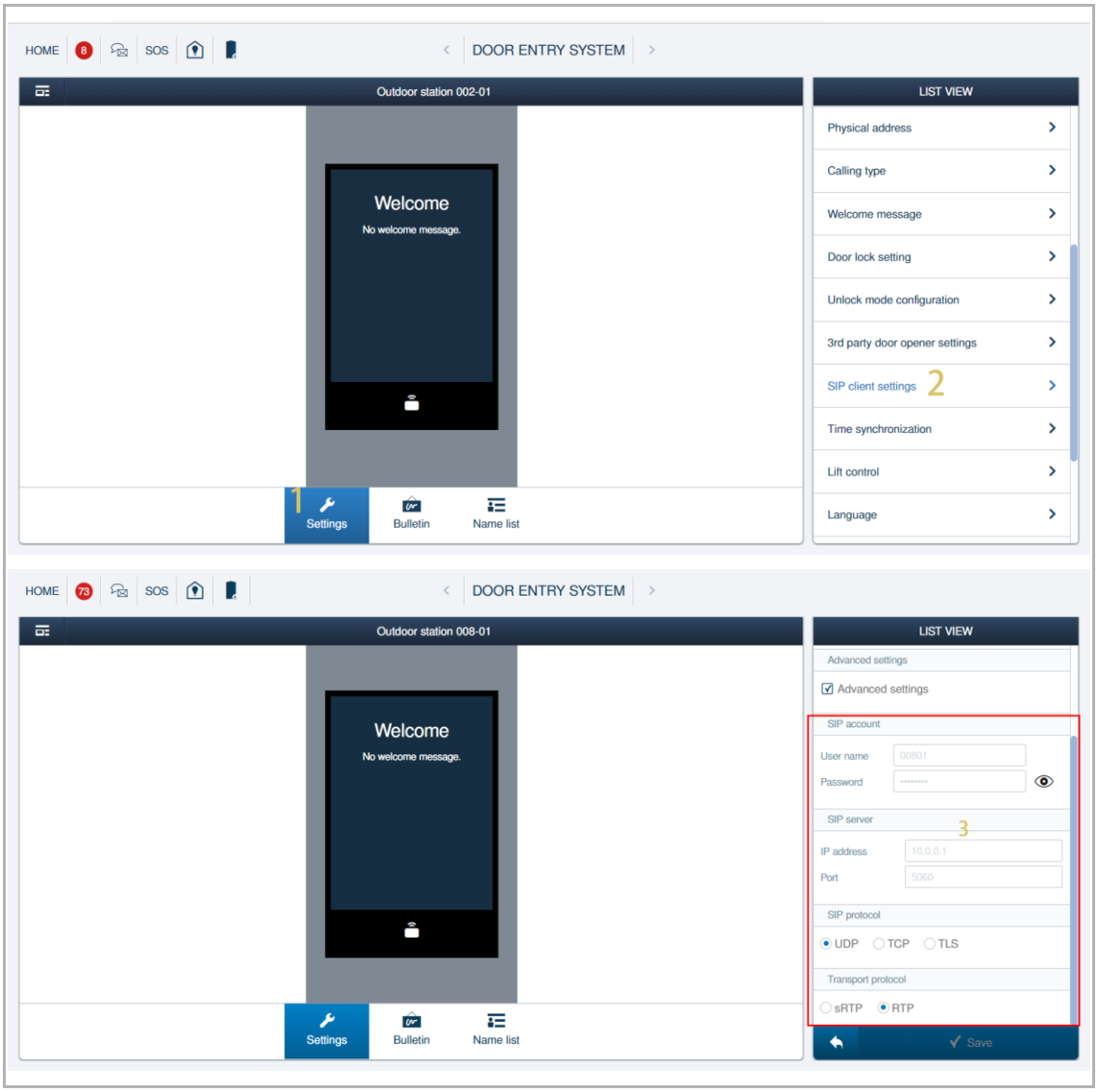
Please follow the steps below:

[1] On the designated IP touch 5 outdoor station screen, click "Settings".

[2] Click "SIP client settings".

[3] The following settings will be filled automatically when "Smart Access Point" is enabled as an SIP server and IP touch 5 has obtained the certification from "Smart Access Point".

- SIP account
- SIP server
- Communication protocol
- Transport protocol



2. 3rd party door opener settings

The 3rd party panel needs to set a command before releasing the lock on IP touch 5 outdoor station.

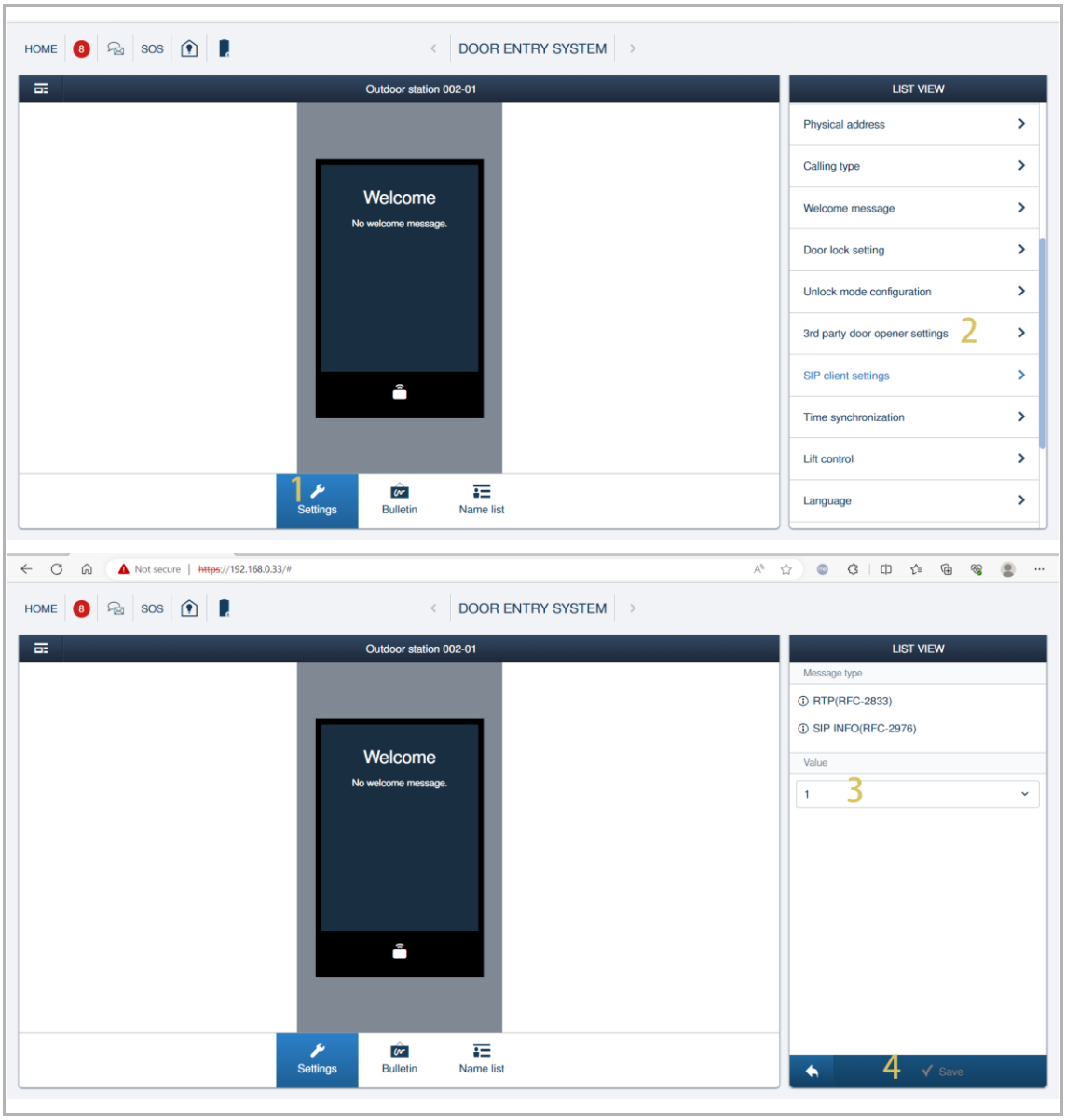
Please follow the steps below:

[1] On the designated IP touch 5 outdoor station screen, click "Settings".

[2] Click "3rd party door opener settings".

[3] Select a value from the drop-list as the command to release the lock. It can be set to "0~9" , "*" or "#".

[4] Click "Save".



3. Adding the 3rd party panels to the name list one by one

It is available for IP touch 5 outdoor station calls the 3rd party panel via keypad directly or name list.

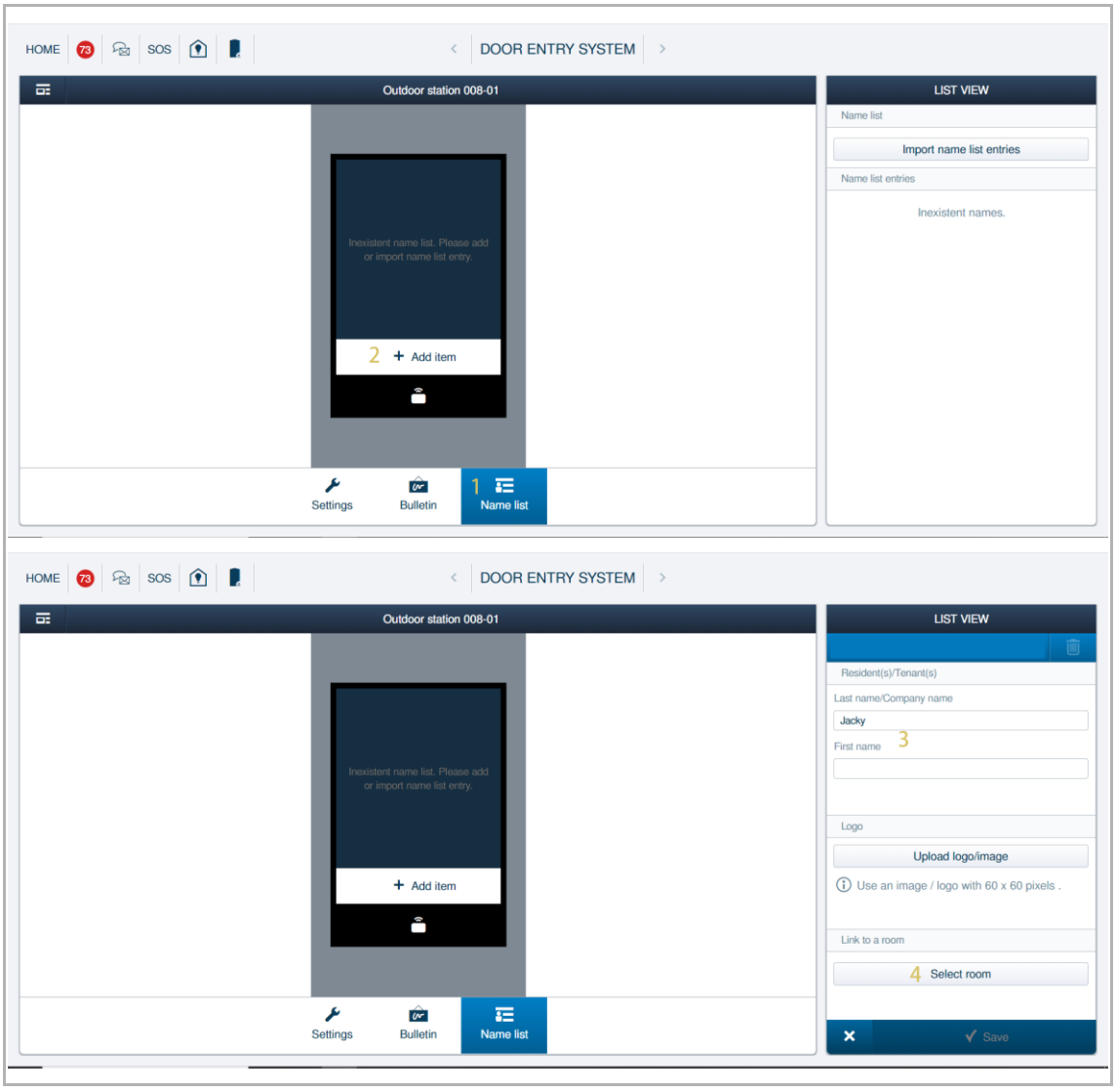
Please follow the steps to add the 3rd party panel to the name list:

[1] On the designated IP touch 5 outdoor station screen, click "Name list".

[2] Click "+ Add item".

[3] Enter the last name and the first name.

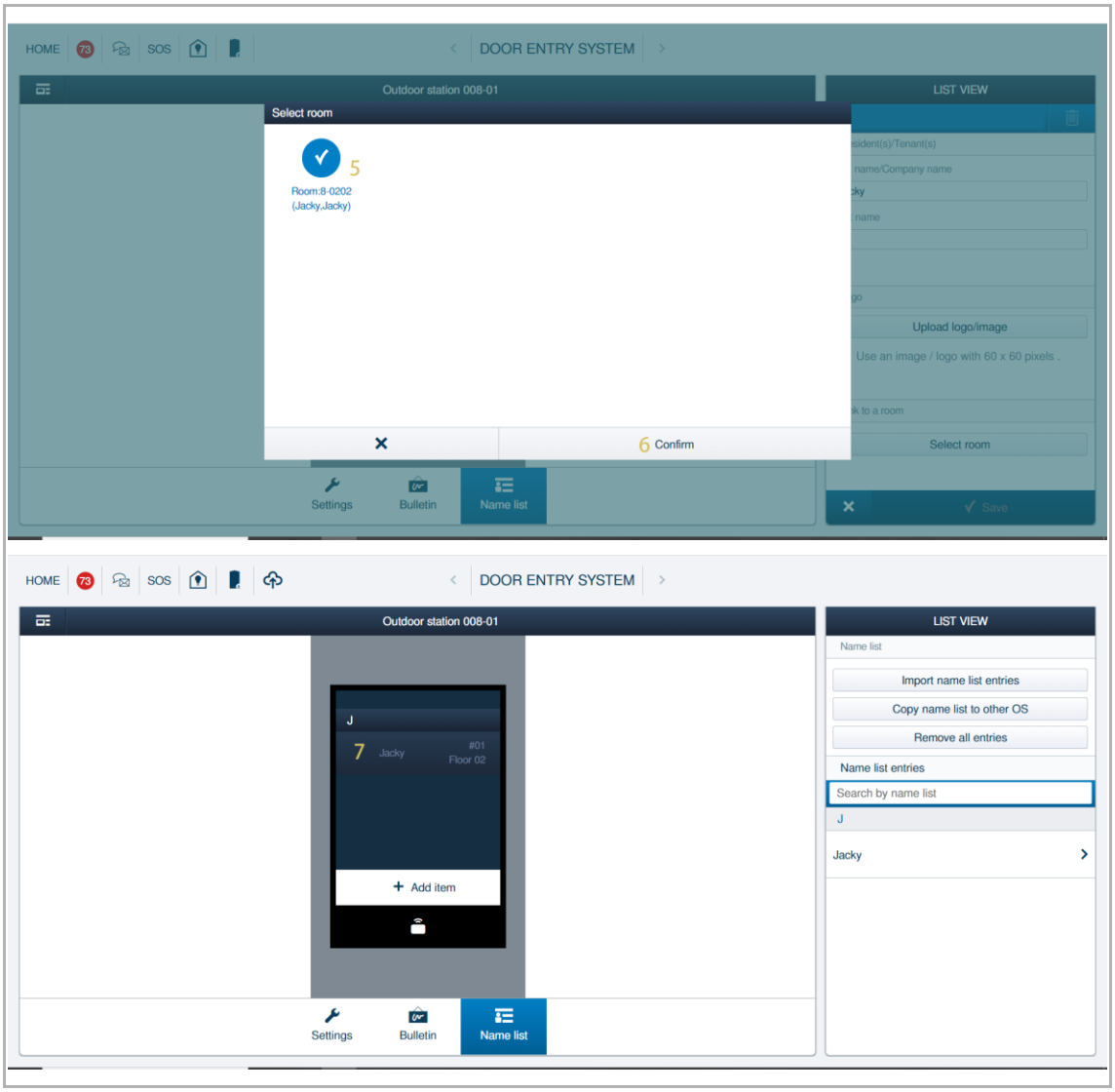
[4] Click "Select room".



[5] Select the designated room where the 3rd party panel is placed.

[6] Click "Confirm".

[7] The alias name has been displayed on the screen of IP touch 5 outdoor station.



4. Adding the 3rd party panels to the name list in batch

If there are many 3rd party panel need to be added to the name list. It is recommended to use importing function.

Please follow the steps to add the 3rd party panels to the name list in batch:

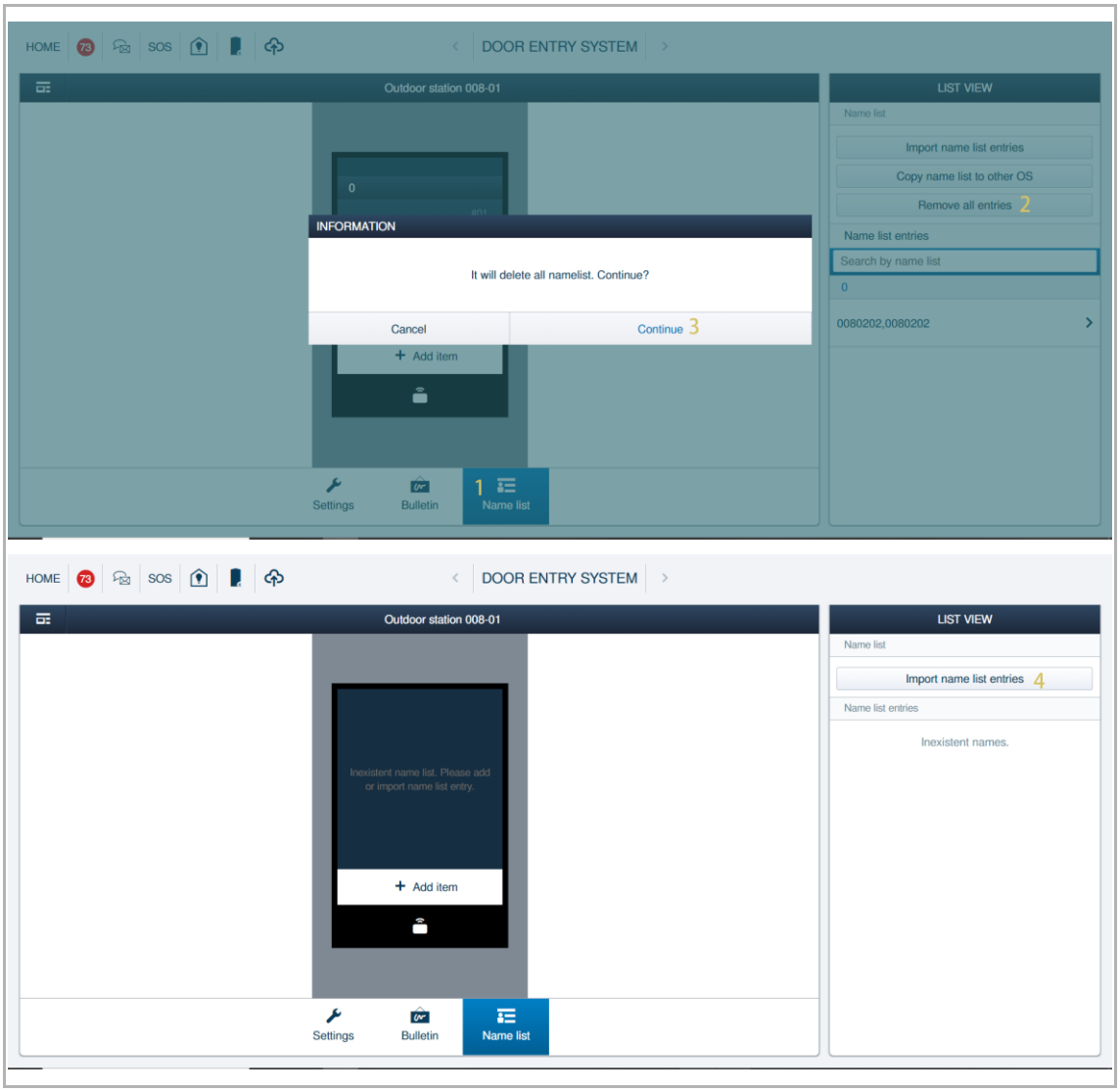
It is recommended remove all entries before importing.

[1] On the designated IP touch 5 outdoor station screen, clcik "Name List".

[2] Click "Remove all entries".

[3] Click "Continue".

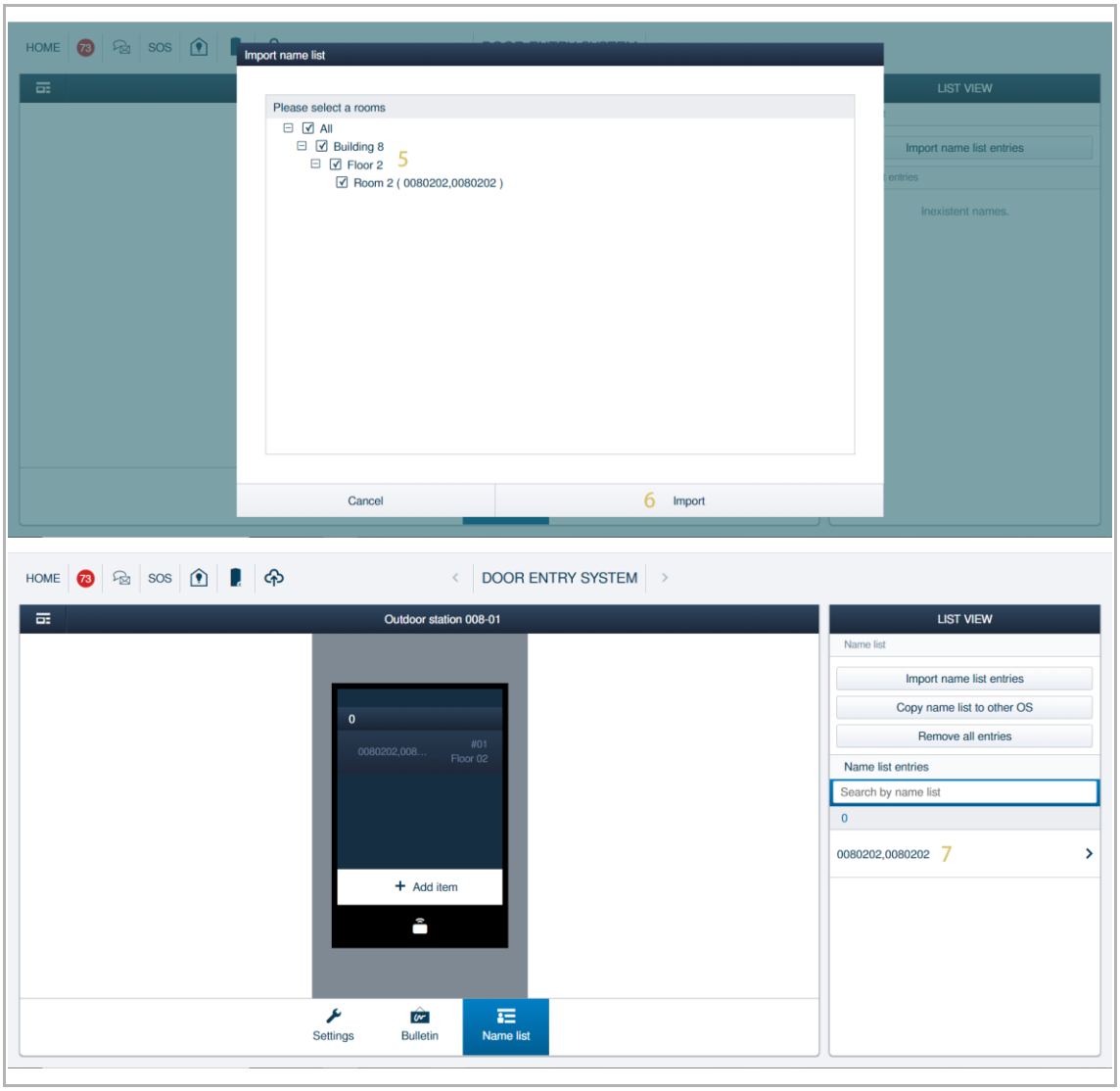
[4] Click "Import name list entries".



[5] Select the designated rooms.

[6] Click "Import".

[7] The alias name has been displayed on the screen. Click the name to set the alias name.



9.5.7 Configuring Audio IP

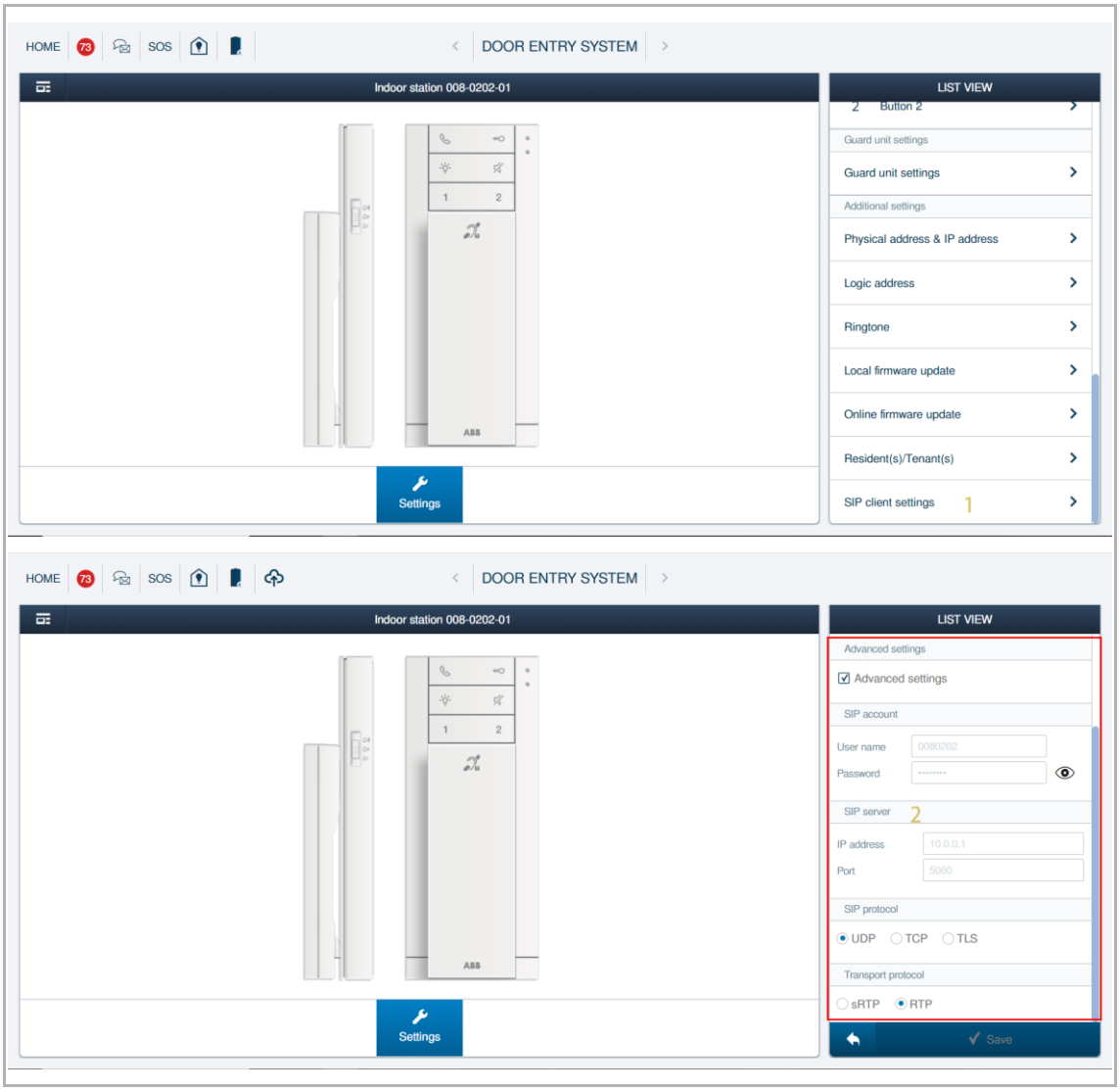
Audio IP needs to be configured before using SIP function.

Please follow the steps below:

[1] On the designated Audio IP "Settings" screen, click "SIP client settings".

[2] The following settings will be filled automatically when "Smart Access Point" is enabled as an SIP server and Audio IP has obtained the certification from "Smart Access Point".

- SIP account
- SIP server
- Communication protocol
- Transport protocol



9.5.8 Time synchronization

Please follow the steps below:

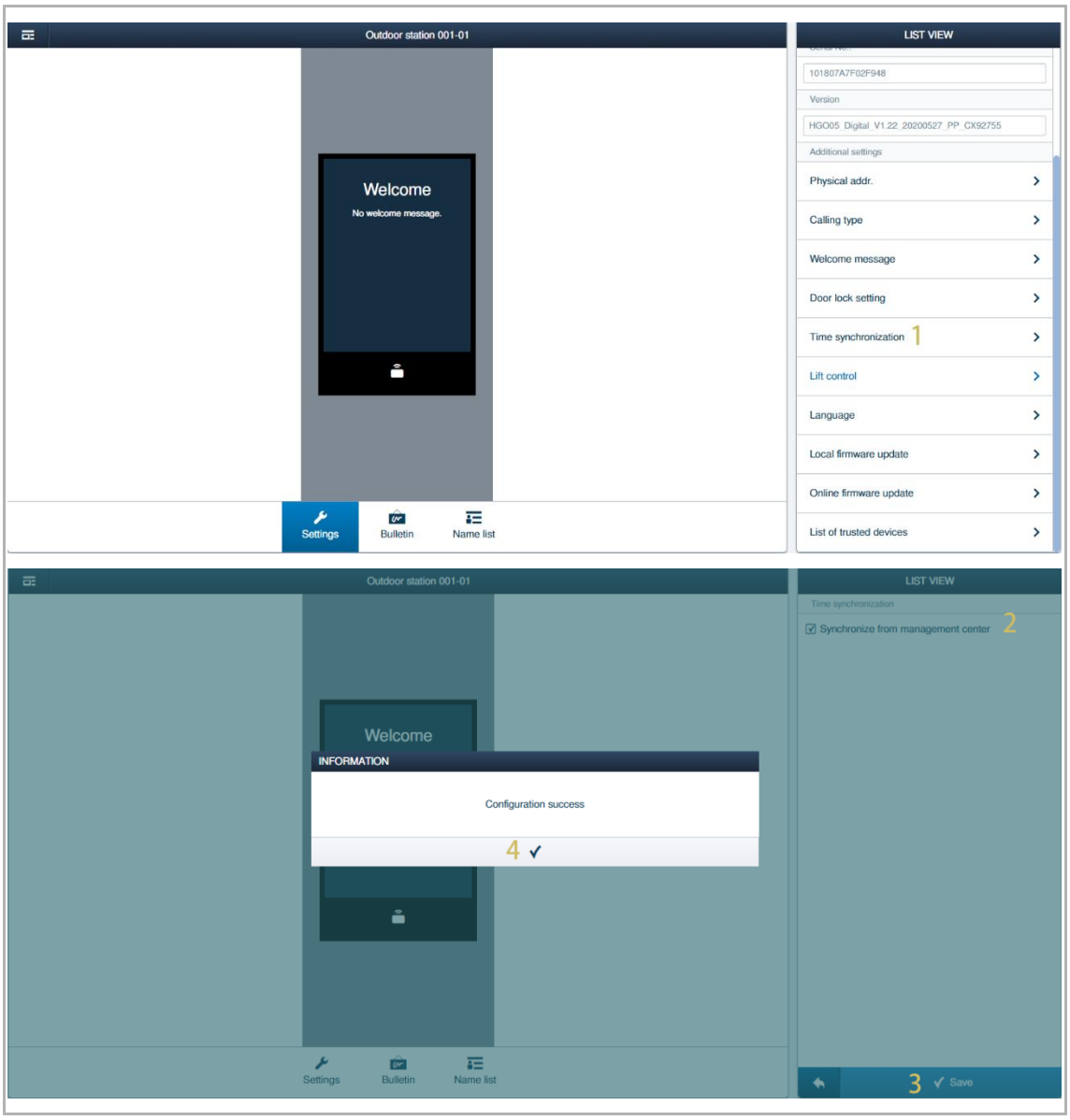
[1] On the designated outdoor station screen, click "Time synchronization".

[2] Tick the check box to enable the function.

[3] Click "√" to save.

[4] Click "√" to confirm.

After the setting, the outdoor station can synchronize its time with "Smart Access Point".



9.5.9 Managing Lift control

Please follow the steps below:

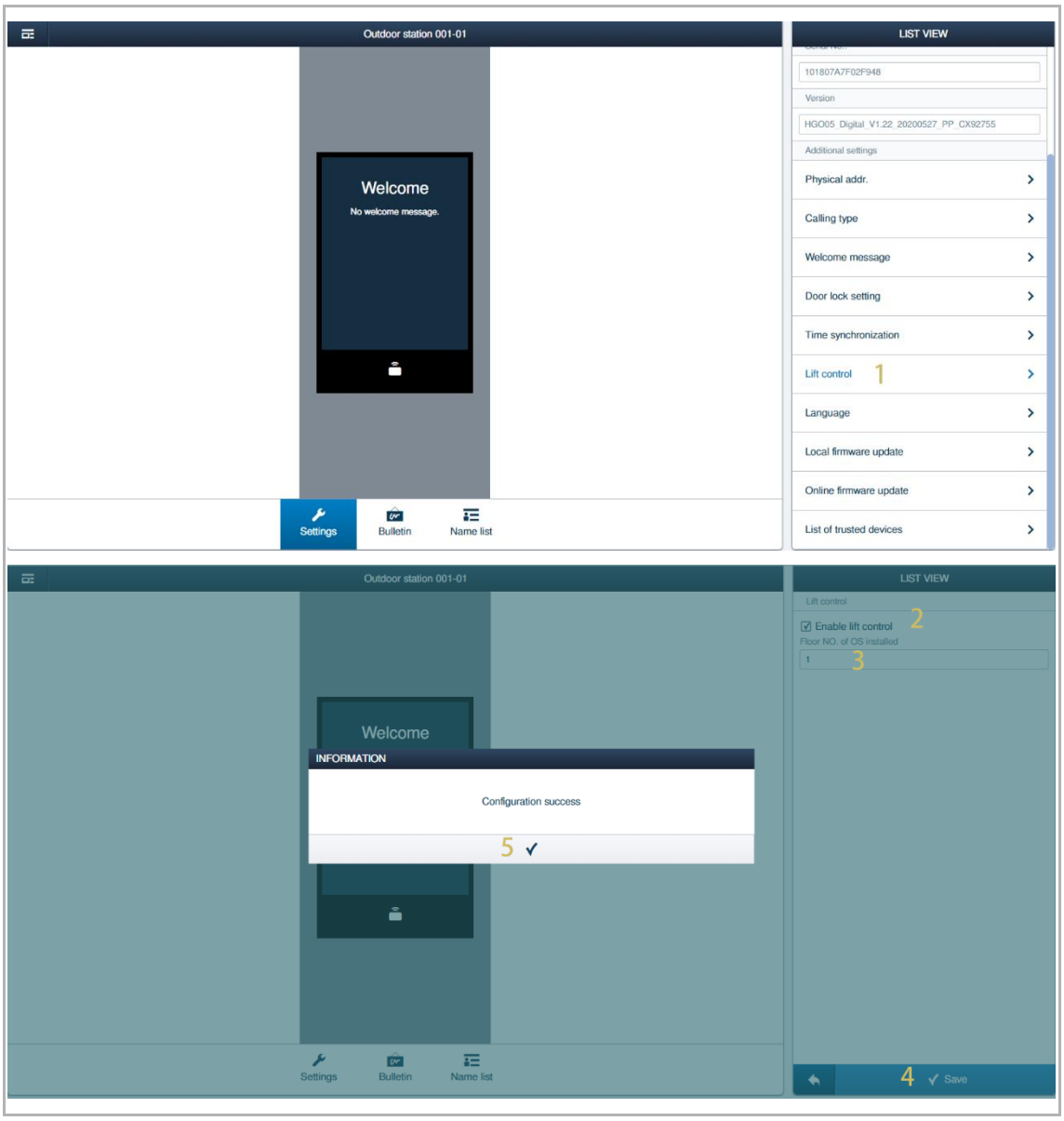
[1] On the designated outdoor station screen, click "Lift control".

[2] Tick the check box to enable the function.

[3] Enter the floor where the outdoor station is located.

[4] Click "√" to save.

[5] Click "√" to confirm.



9.5.10 Initiating a call via the physical address

This chapter applies to the IP touch 5 outdoor station and IP keypad outdoor station.

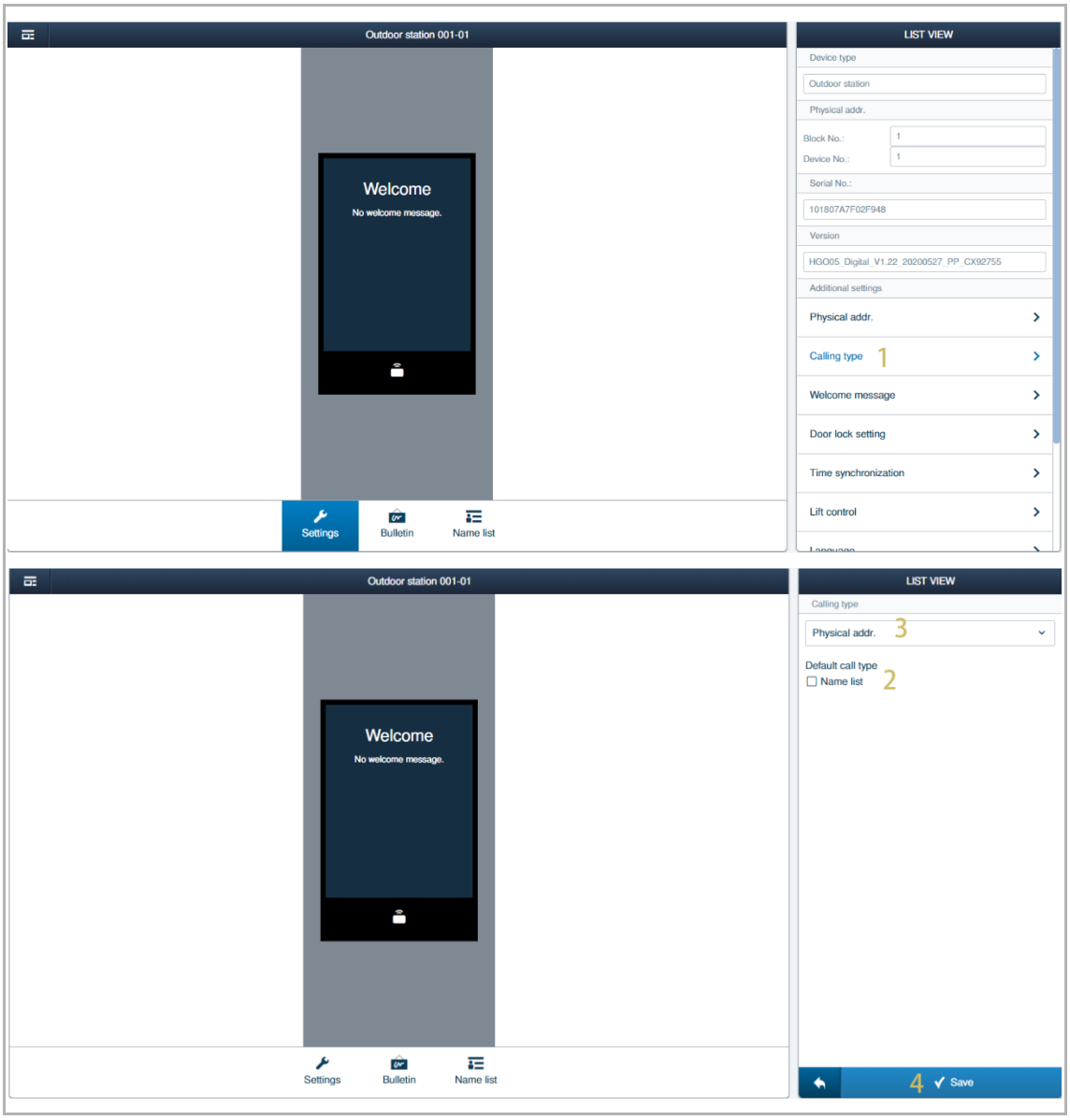
Please follow the steps below:

[1] On the designated outdoor station screen, click "Call type".

[2] Disable the "Name list" (only applied to IP touch 5 outdoor station).

[3] Set "Call type" to "Physical addr."

[4] Click "√" to save.



9.5.11 Initiating a call via the logic address

This chapter applies to the IP touch 5 outdoor station and IP keypad outdoor station.

1. Adding the logic address

Please follow the steps below:

[1] On the designated outdoor station screen, click "Call type".

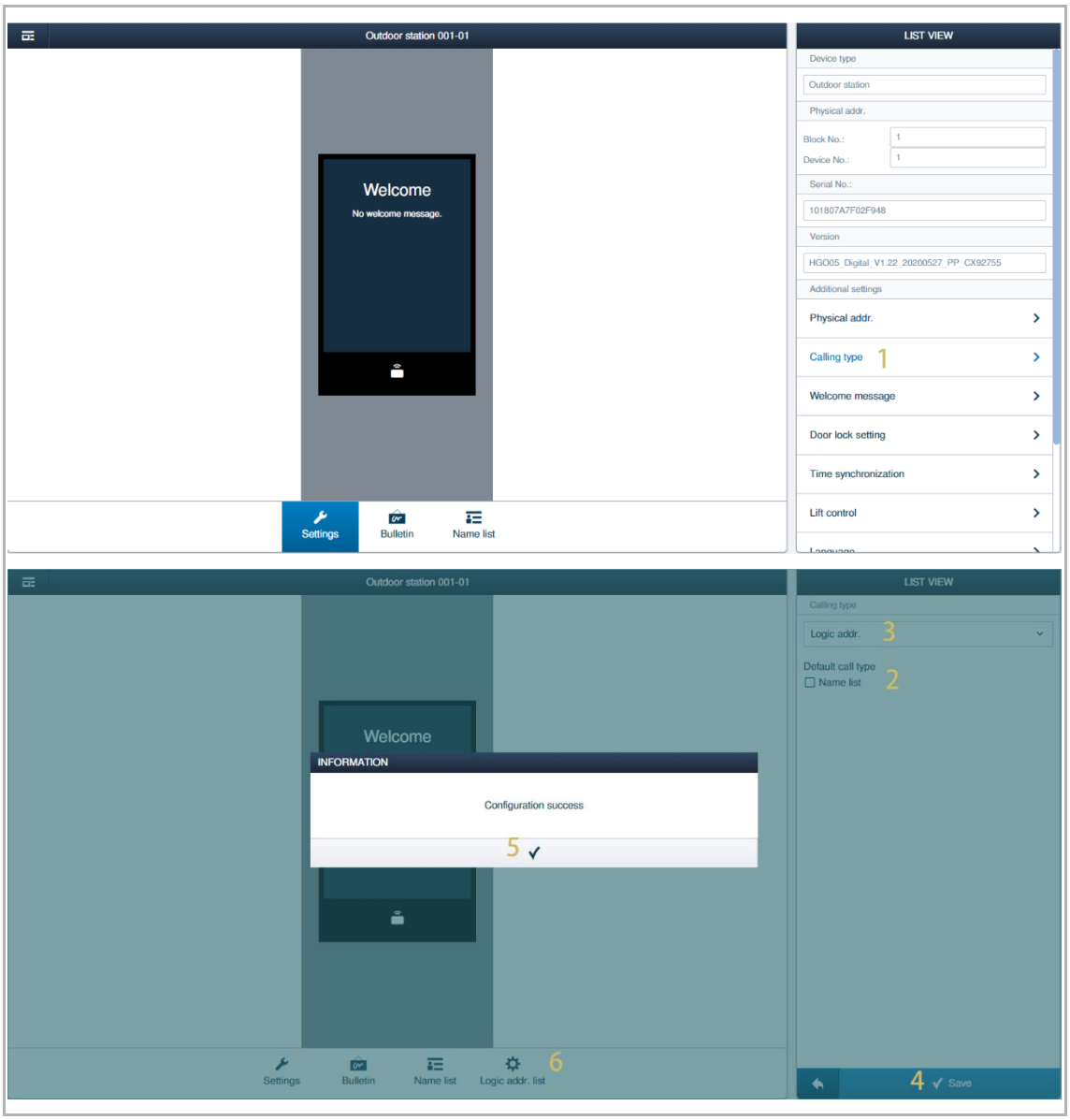
[2] Disable the "Name list" (only applies to the IP touch 5 outdoor station).

[3] Set "Call type" to "Logic addr."

[4] Click "√" to save.

[5] Click "√" to confirm.

[6] "Logic addr. list" is displayed on the screen. Click it to continue.

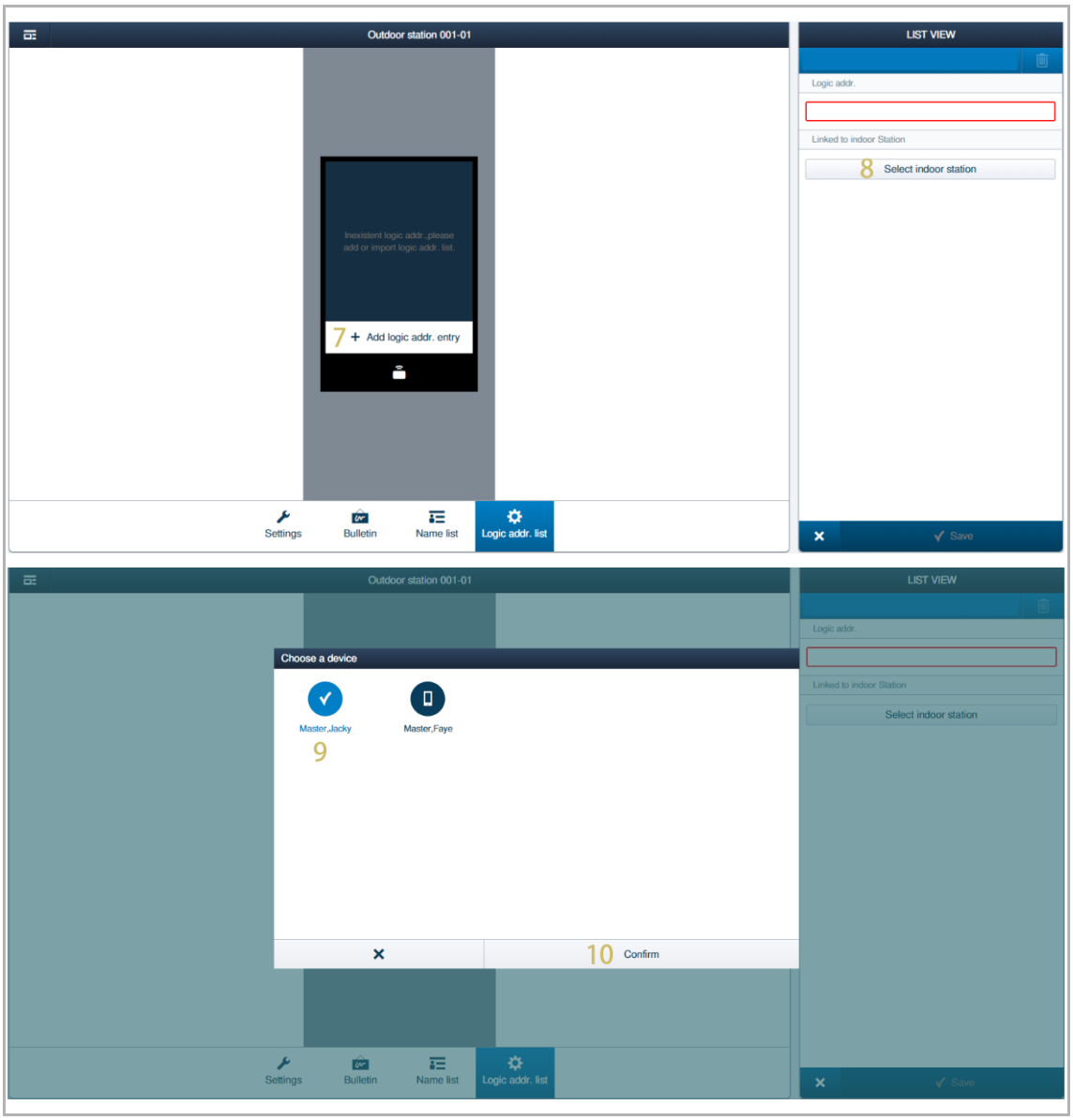


[7] On the "Logic addr. list" screen, click "+".

[8] Click "Select indoor station".

[9] Click to select the designated indoor station.

[10] Click "Confirm".

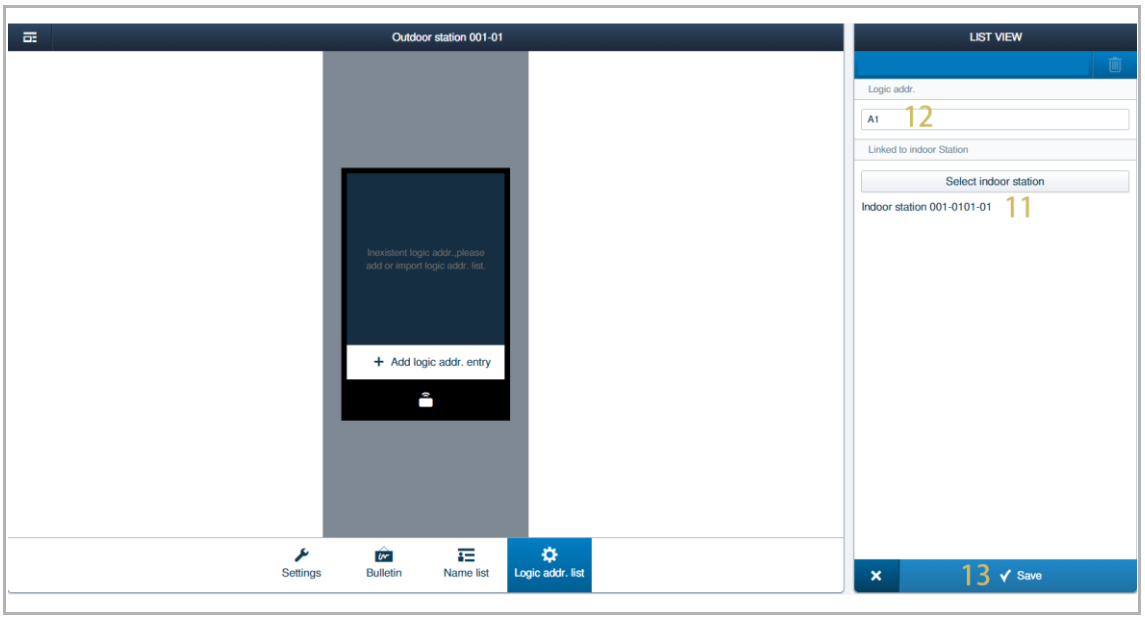


[11]The indoor station is added to the list.

[12]The logic address is imported to the list.

[13]Click " √ " to save, followed by " √ " to confirm.

Repeat steps 7-13 to add the logic address one by one.



2. Importing the logic addresses

Please follow the steps below:

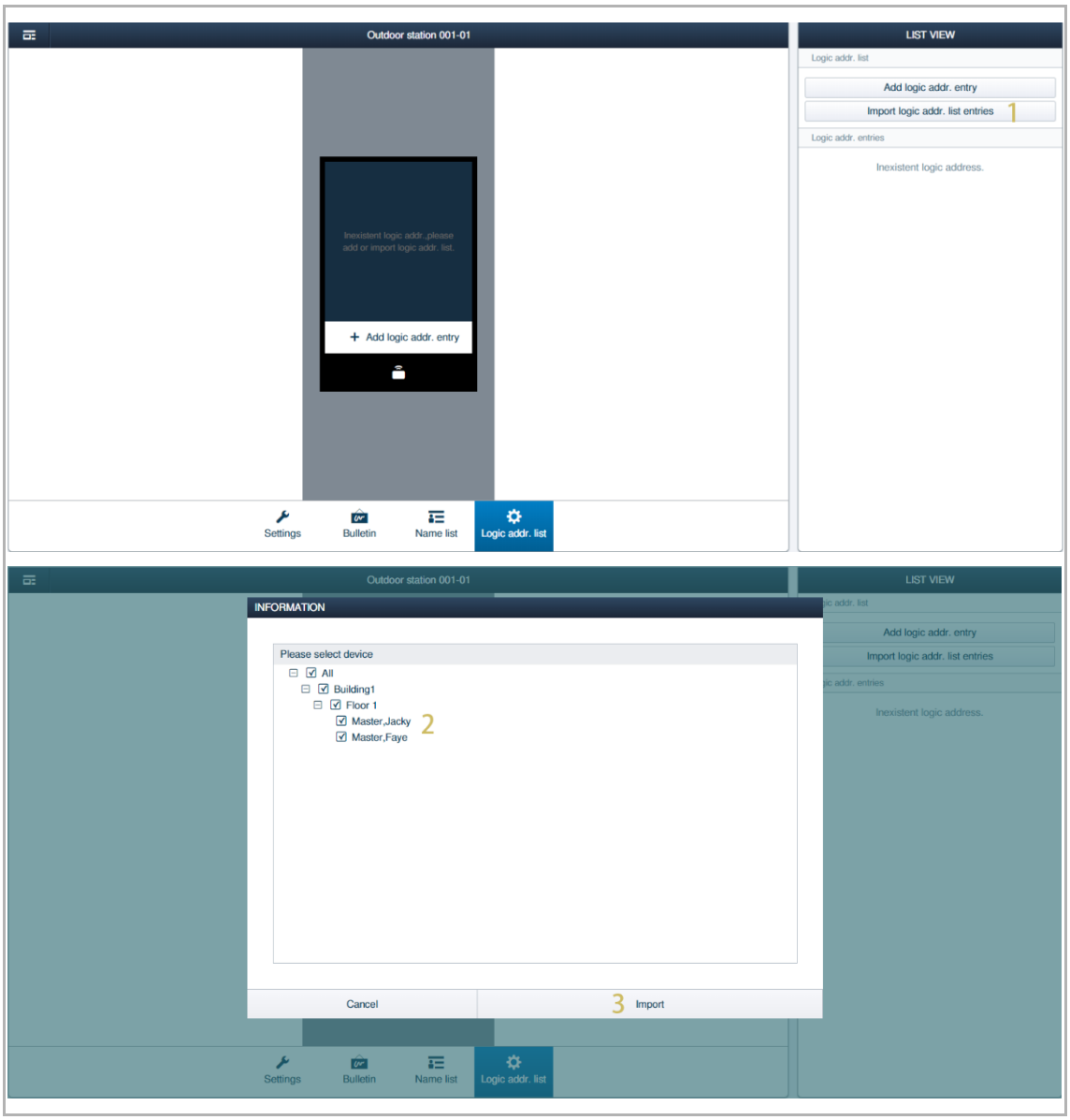
[1] On the "Logic addr. list" screen, click "Import logic addr. list entries".

Note

It is recommended to set the logic address for the indoor station before importing.

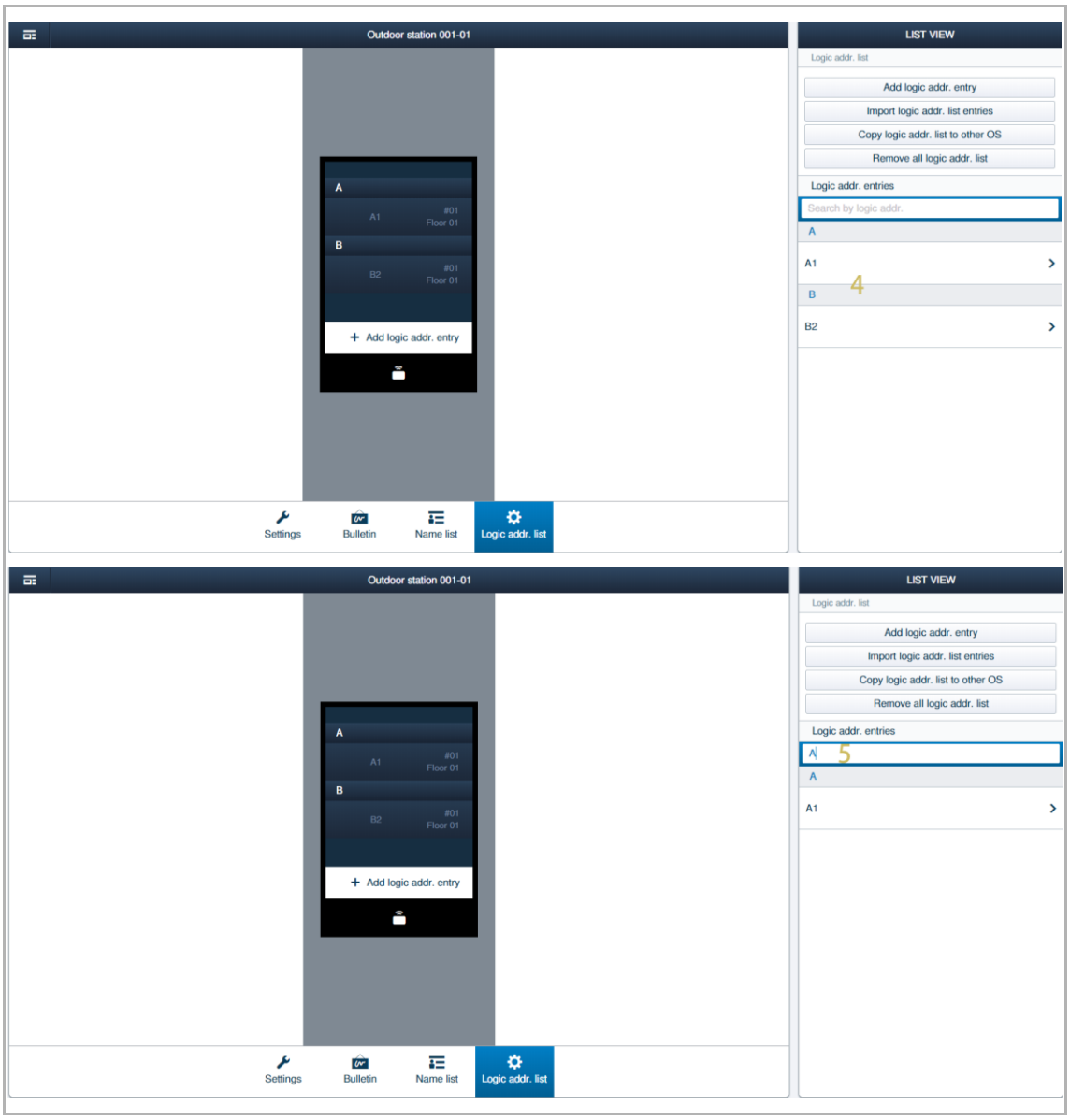
[2] Click to select the designated indoor stations.

[3] Click "Import", followed by " √ ".



[4] The logic addresses are imported to the list.

[5] Enter the key word to filter the search results.



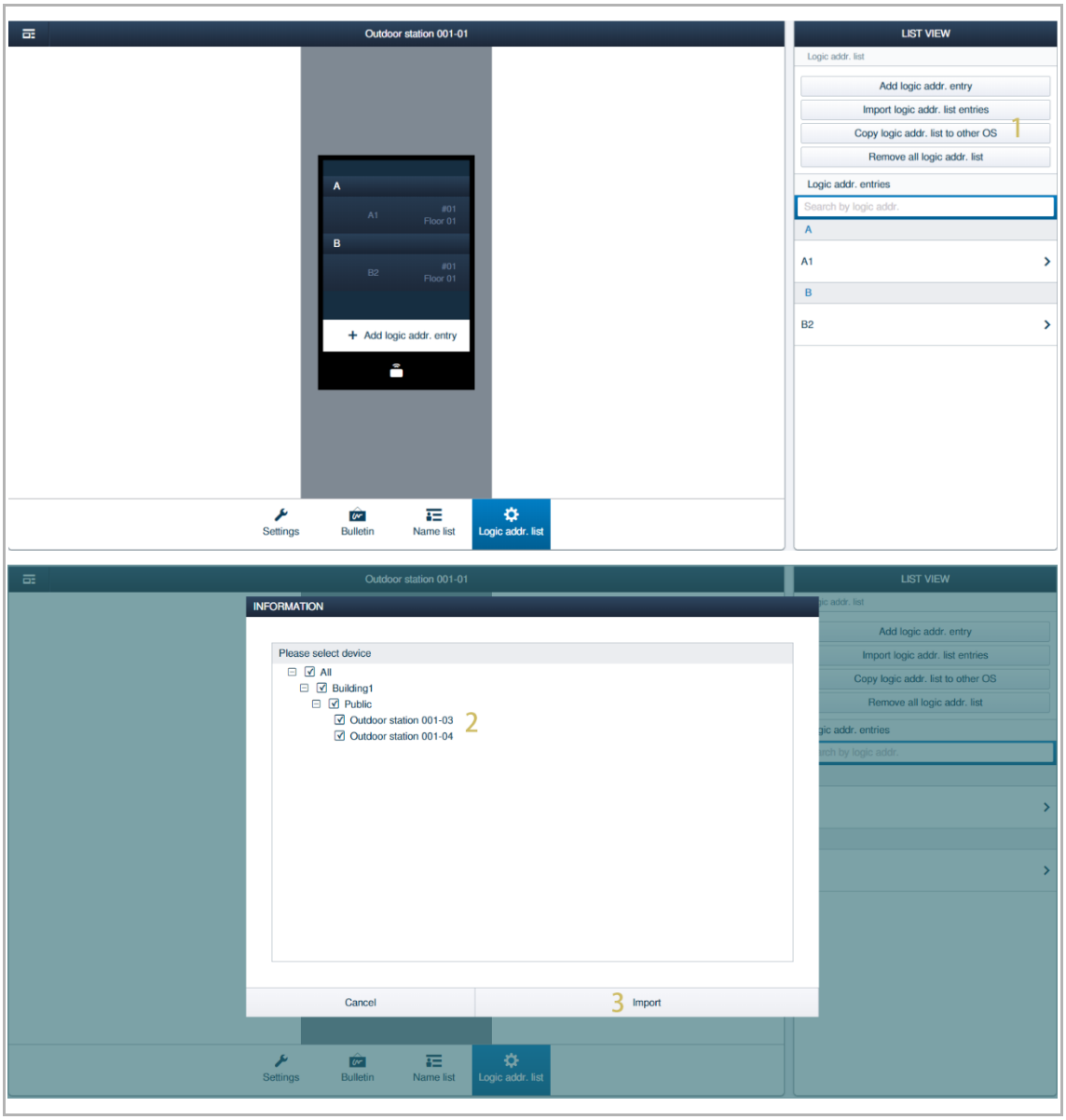
3. Copying the logic address list to another outdoor station

Please follow the steps below:

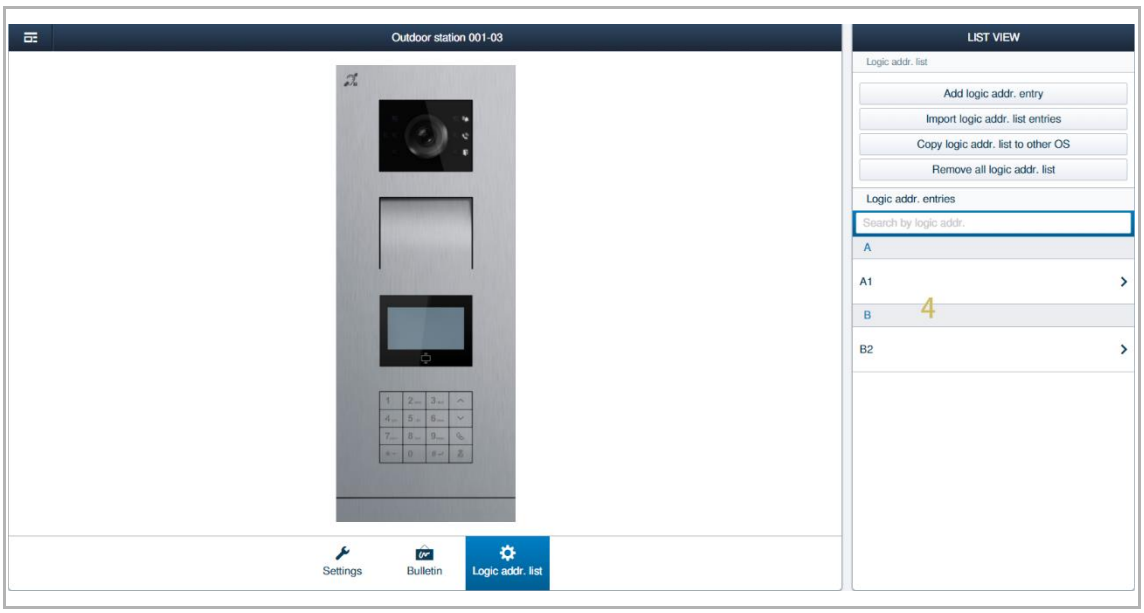
[1] On the "Logic addr. list" screen, click "Copy logic addr. list to other OS".

[2] Click to select the designated outdoor stations.

[3] Click "Import", followed by " √ ".



[4] The logic address list is copied to the other outdoor station.

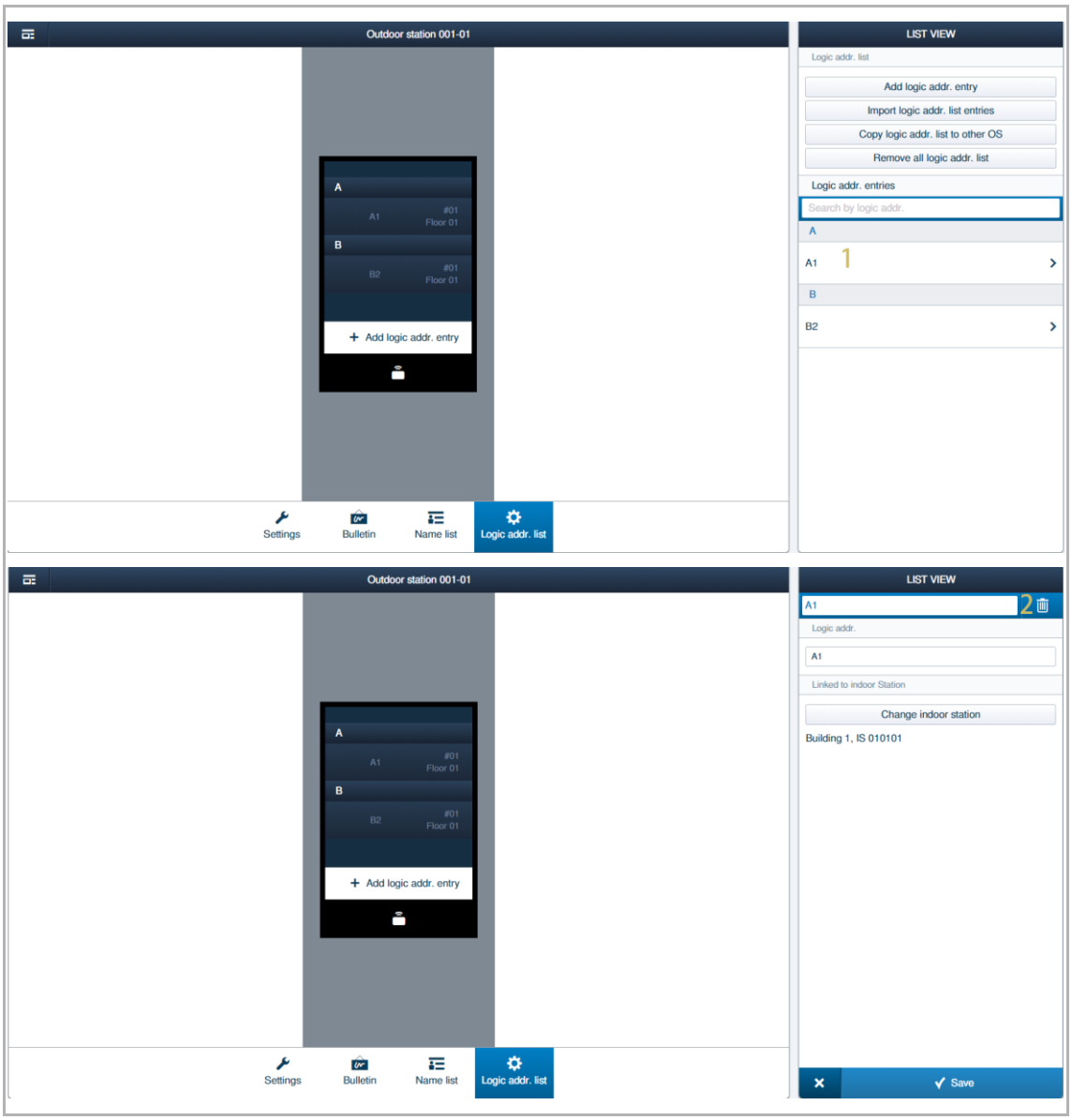


4. Removing the logic address

Please follow the steps below:

[1] On the "Logic addr. list" screen, click the designated logic address.

[2] Click "  ", followed by " √ " to confirm.



Note

You can also click "Remove all logic addr. list" to clear all logic addresses.

9.5.12 Initiating a call via the name list

This chapter only applies to the IP touch 5 outdoor station.

1. Importing the name list

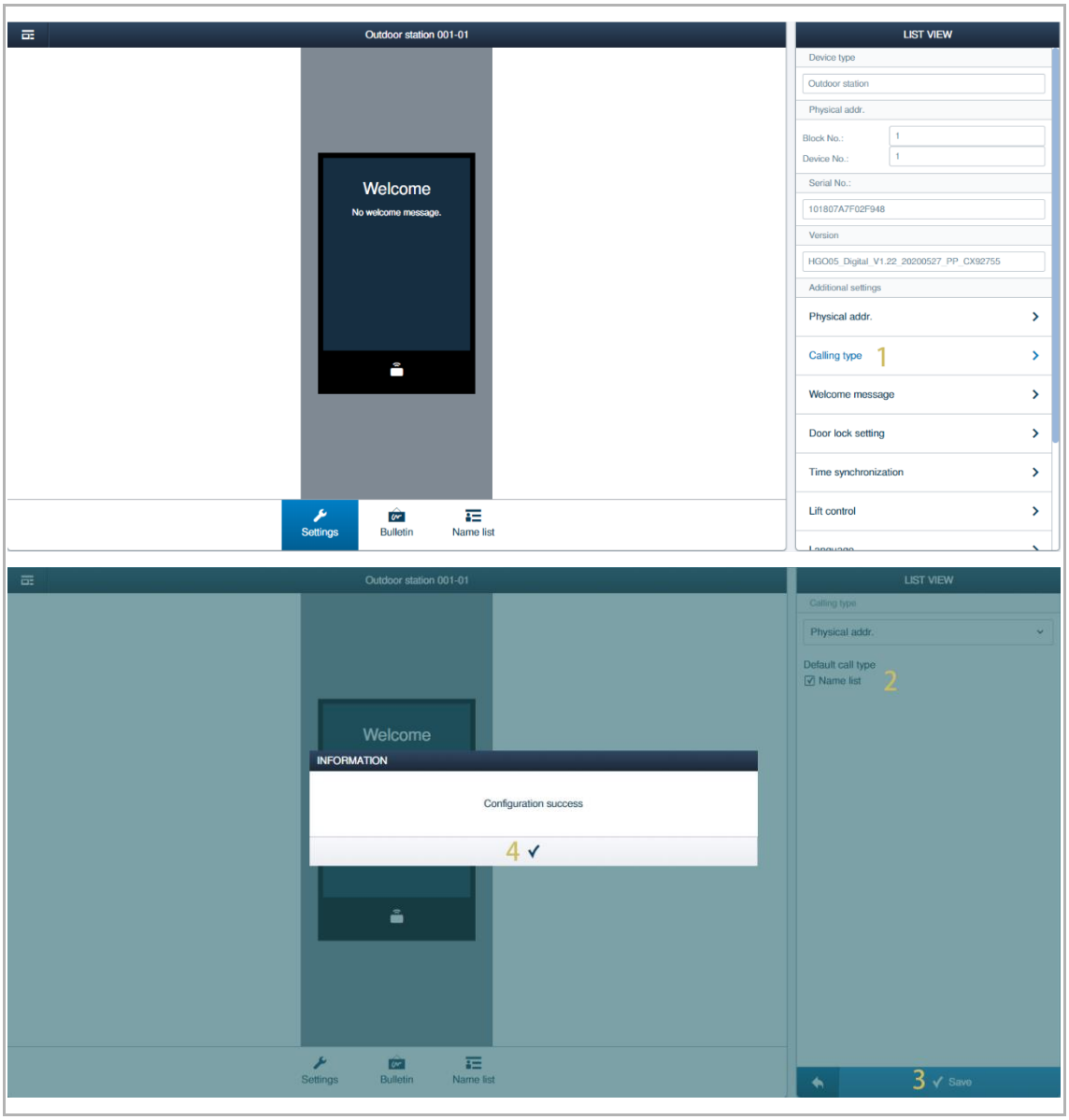
Please follow the steps below:

[1] On the designated outdoor station screen, click "Call type".

[2] Enable the "Name list".

[3] Click "√" to save.

[4] Click "√" to confirm.



[5] On the designated outdoor station screen, click "Name list".

Note
It is recommended to set the name for the indoor stations before importing.

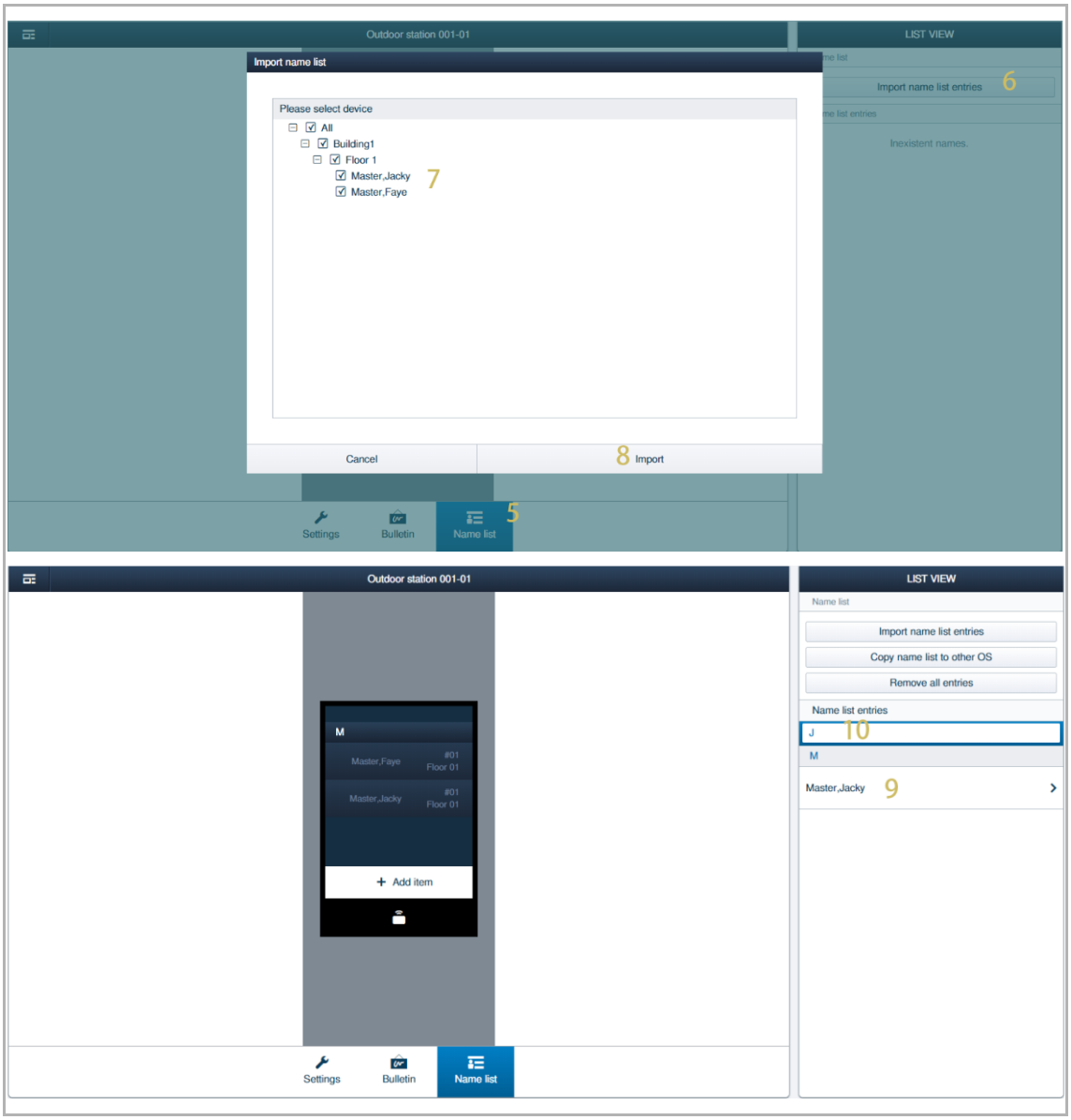
[6] Click "Import name list entries".

[7] Click to select the designated indoor stations.

[8] Click "Import", followed by " √ " to confirm.

[9] The names are imported to the list.

[10]Enter the key word to filter the search result.

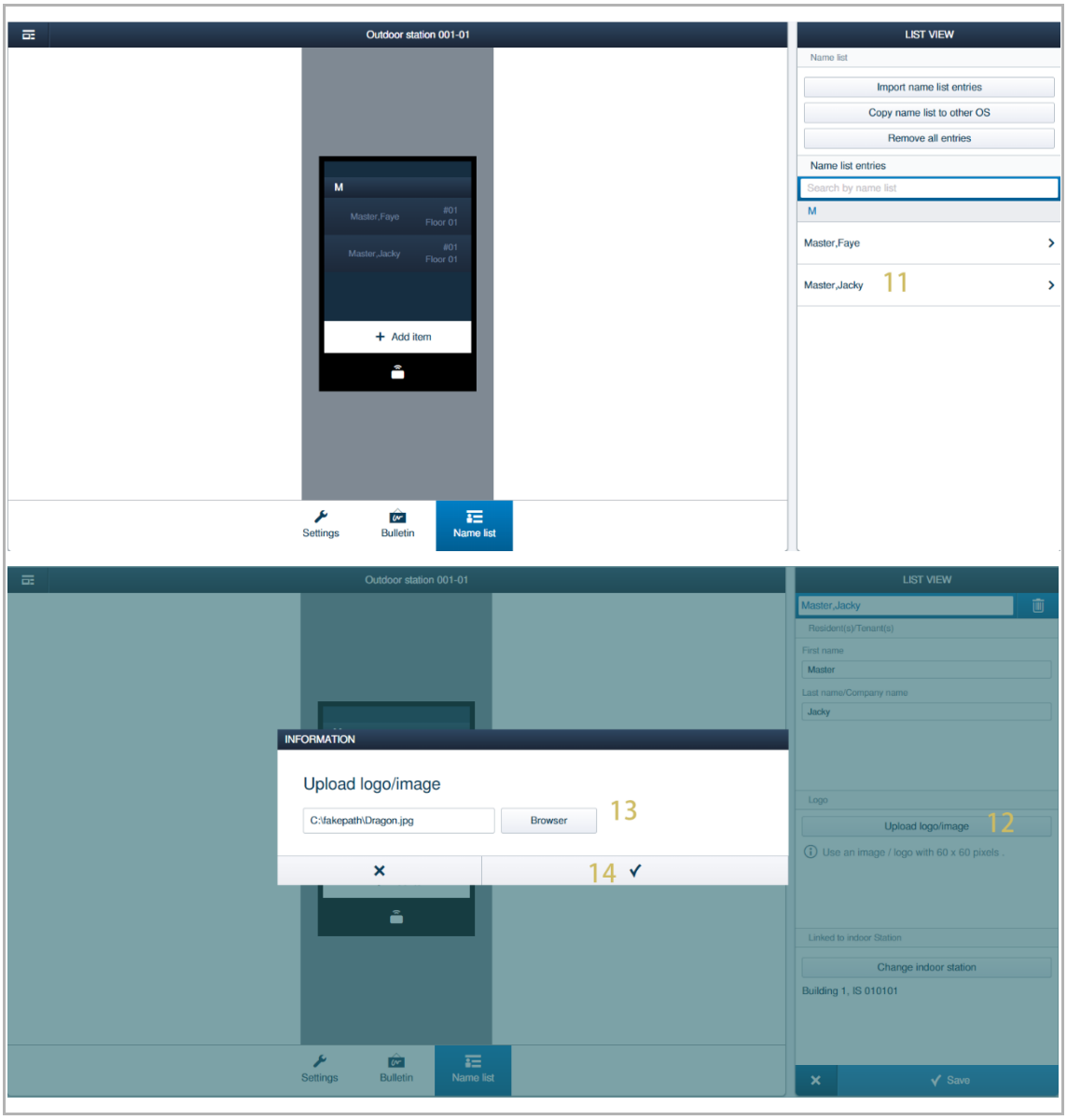


[11]Click the designated name.

[12]Click "Upload logo image".

[13]Click "Browser" to select a logo image (only .jpg is supported. Maximum resolution is 60 x 60 pixels).

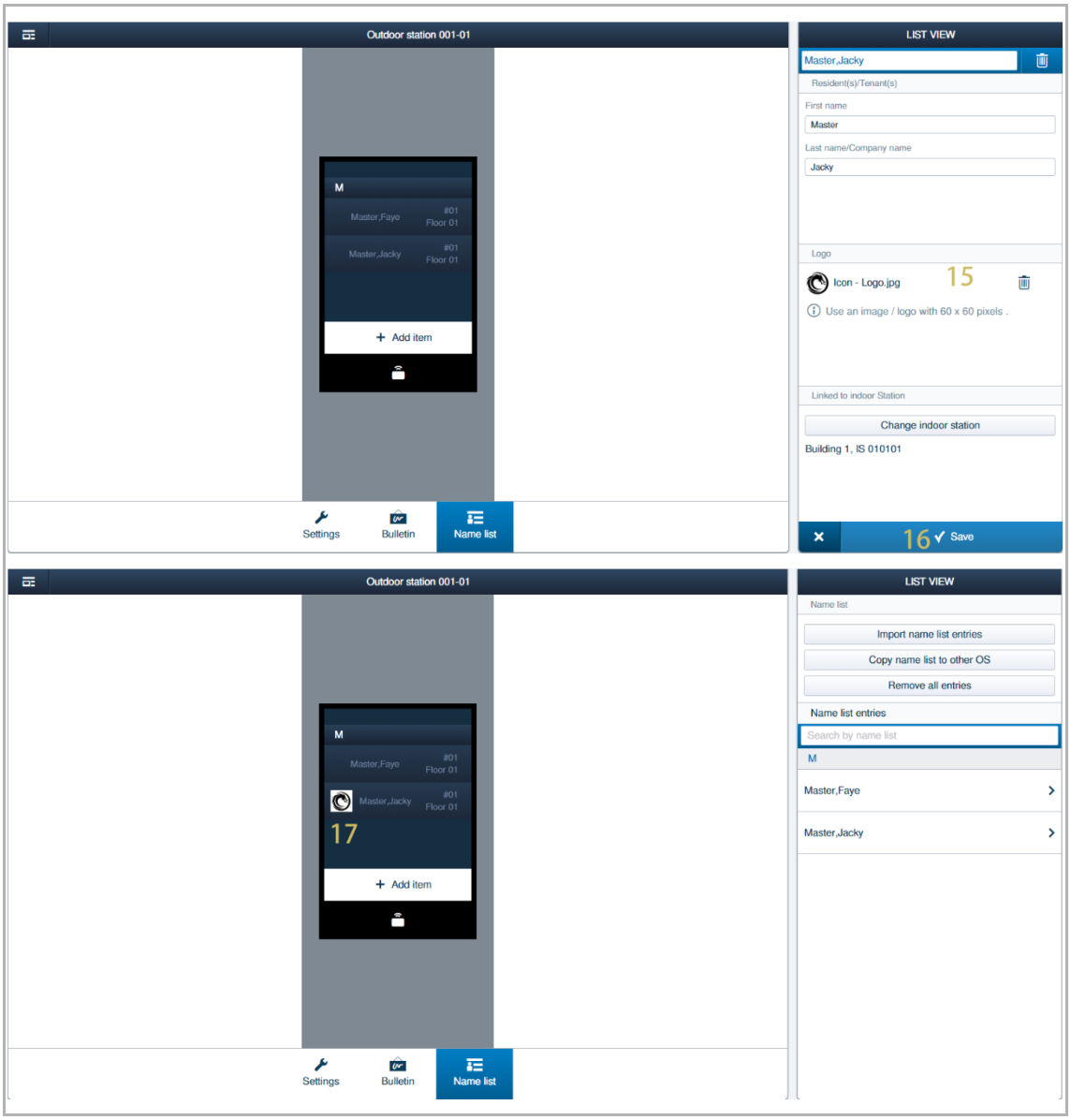
[14]Click " √ " to confirm.



[15]The logo is displayed in the list.

[16]Click " √ " to save.

[17]The logo is displayed on the outdoor station screen.



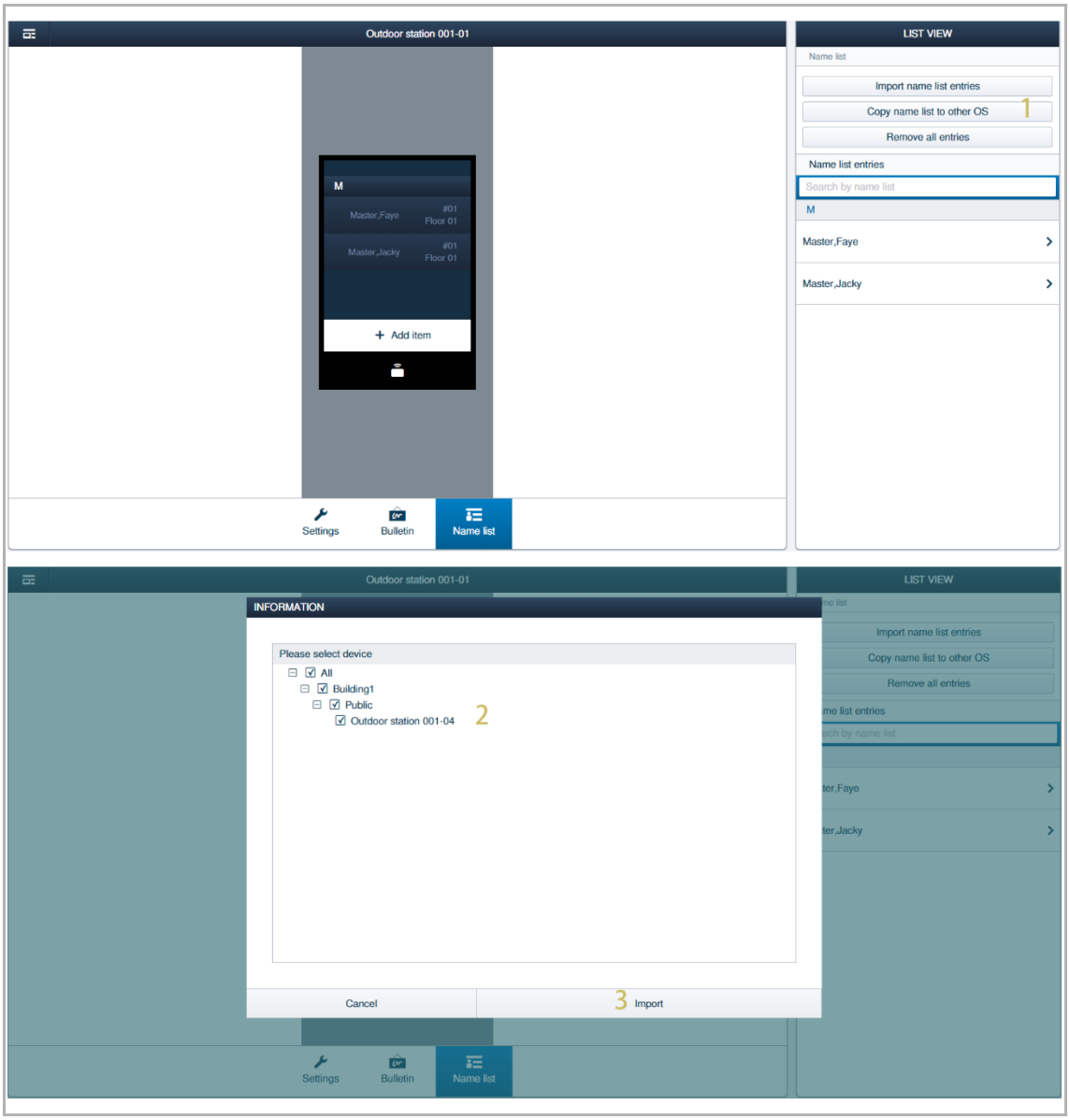
2. Copying the name list to other outdoor station

Please follow the steps below:

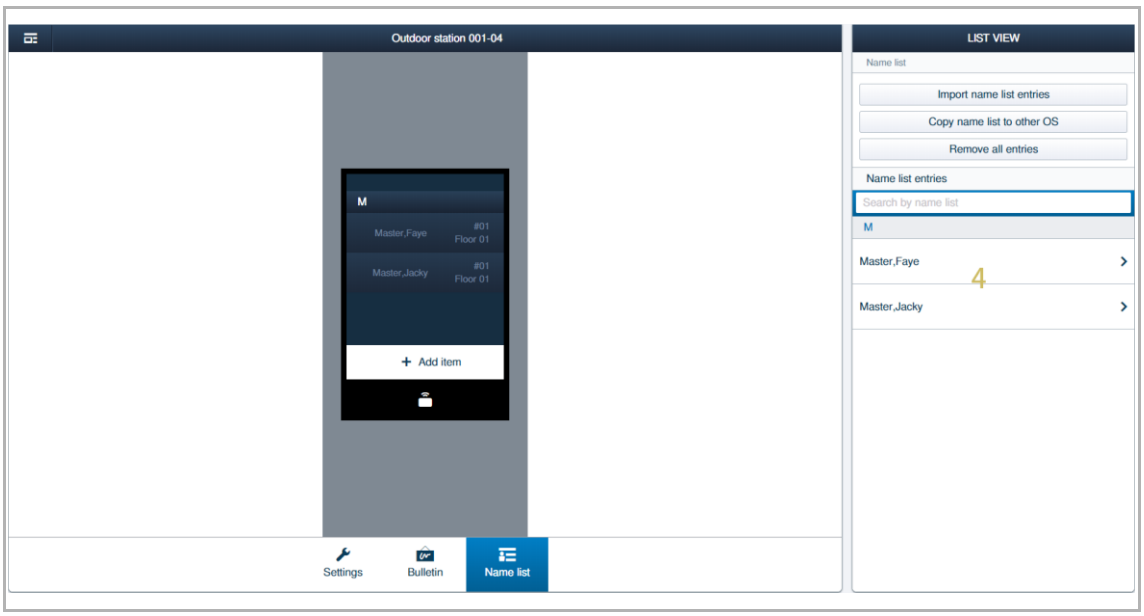
[1] On the "Name list" screen, click "Copy name list to other OS".

[2] Click to select the designated outdoor stations (only supports the IP touch 5 outdoor station).

[3] Click "Import", followed by " √ ".



[4] The name list is copied to the other outdoor station.

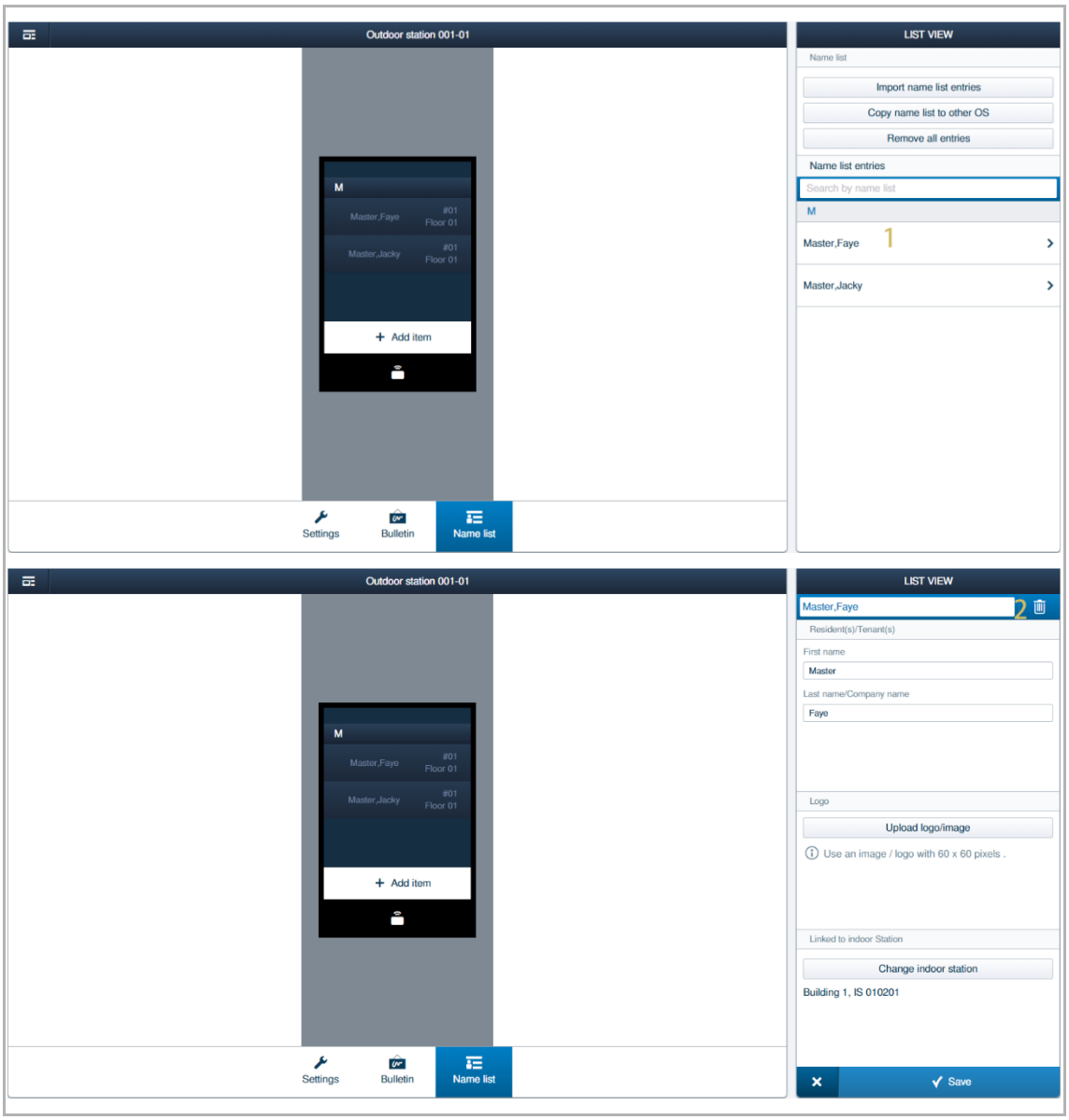


3. Removing the logic address

Please follow the steps below:

[1] On the "Logic addr. list" screen, click the designated logic address.

[2] Click "  ", followed by " √ " to confirm.



Note

You can also click "Remove all entries" to clear the name list.

9.5.13 Managing the welcome message

This chapter only applies to the IP touch 5 outdoor station.

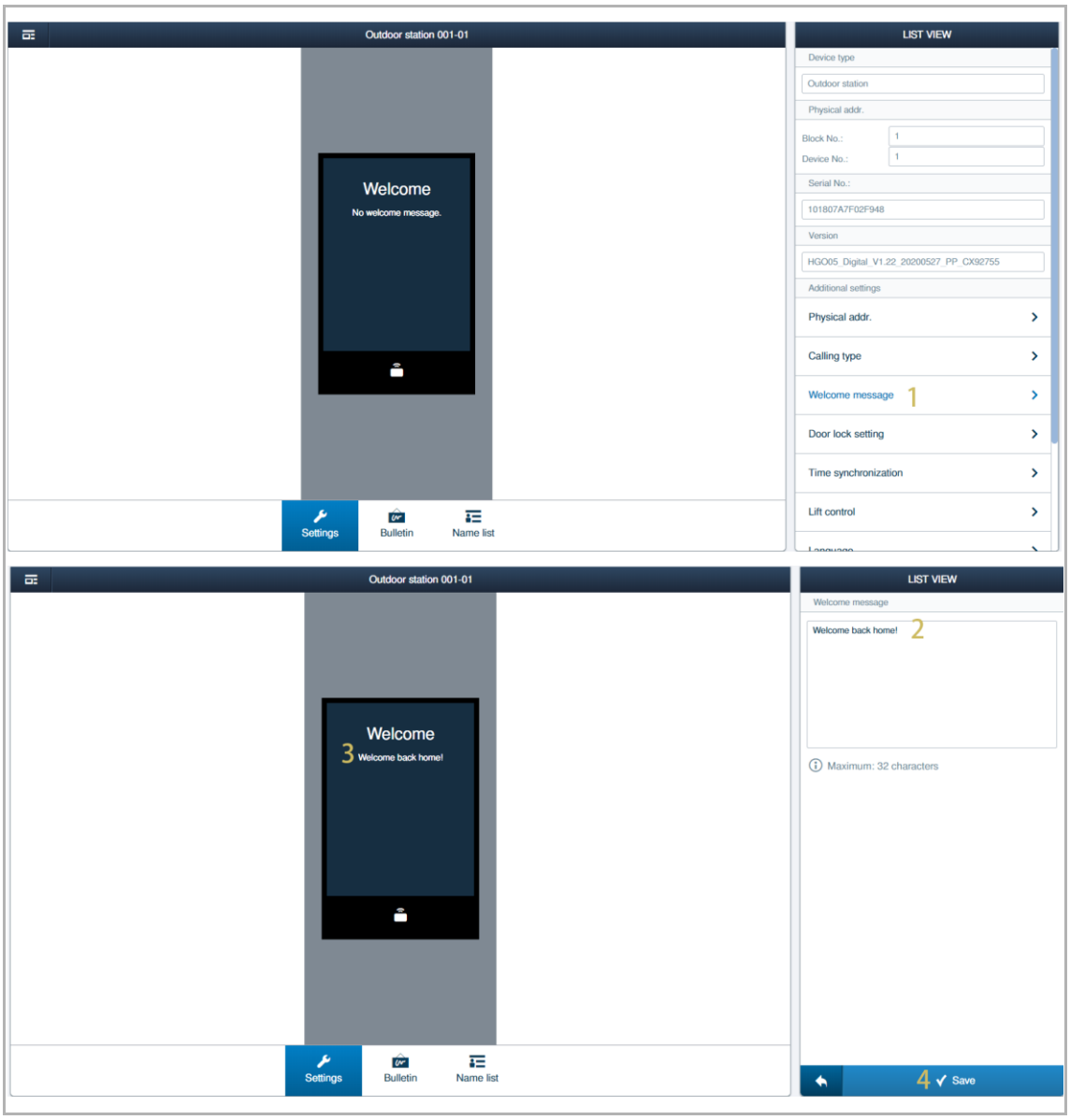
Please follow the steps below:

[1] On the designated outdoor station screen, click "Welcome message".

[2] Enter the message (not more than 32 characters).

[3] The result is displayed on the outdoor station screen.

[4] Click " √ " to save.



9.5.14 Managing the developer information

This chapter is only applied to IP touch 5 outdoor station.

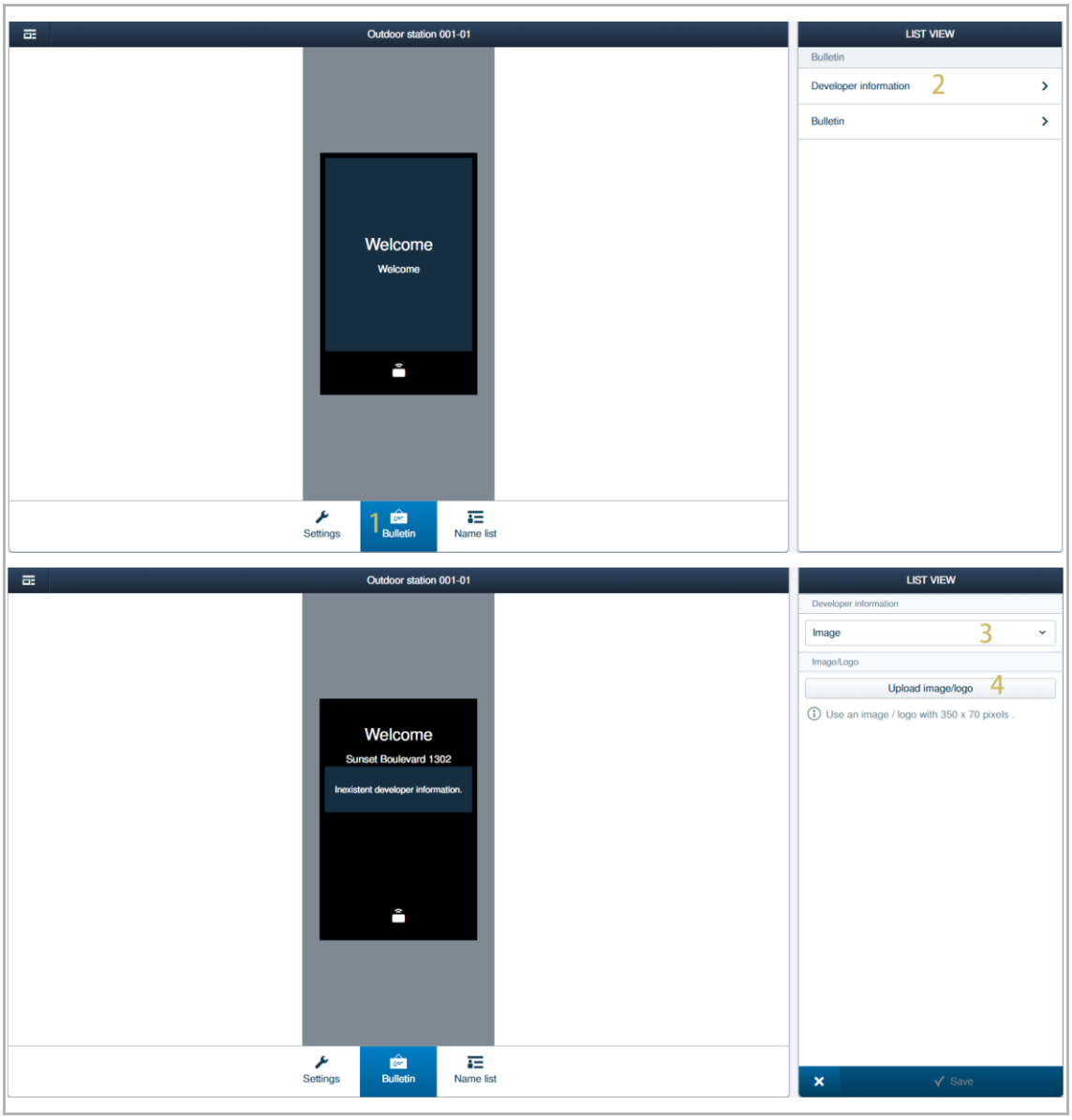
Please follow the steps below:

[1] On the designated outdoor station screen, click "Bulletin".

[2] Click "Developer information".

[3] Selet "Image" from the drop-down list.

[4] Click "Upload image/logo" to select the image (e.g company logo).



9.5.15 Managing the bulletin

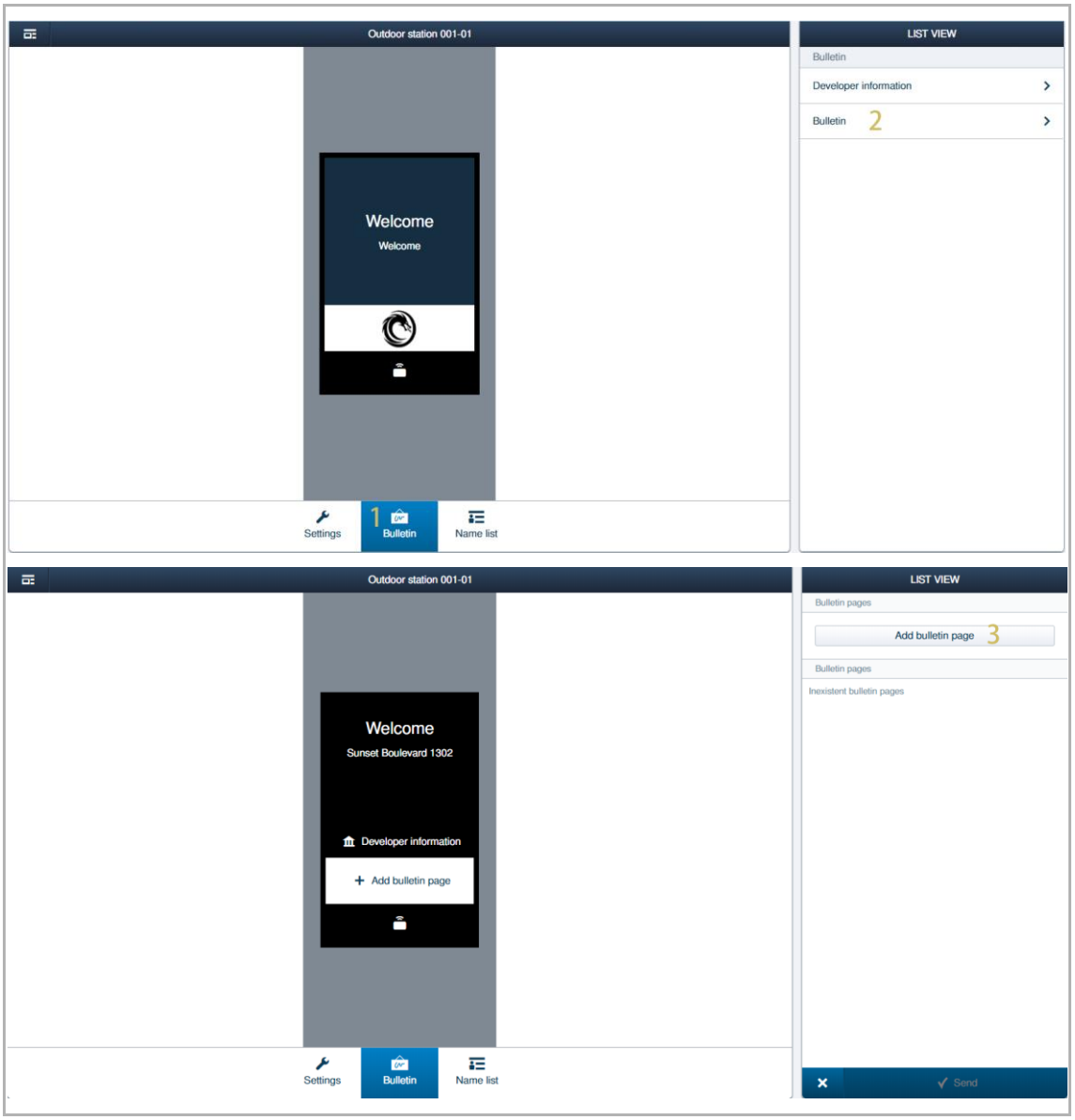
This chapter only applies to the IP touch 5 outdoor station.

Please follow the steps below:

[1] On the designated outdoor station screen, click "Bulletin".

[2] Click "Bulletin".

[3] Click "Add bulletin page" to select the image.



9.5.16 Managing the unlock QR code

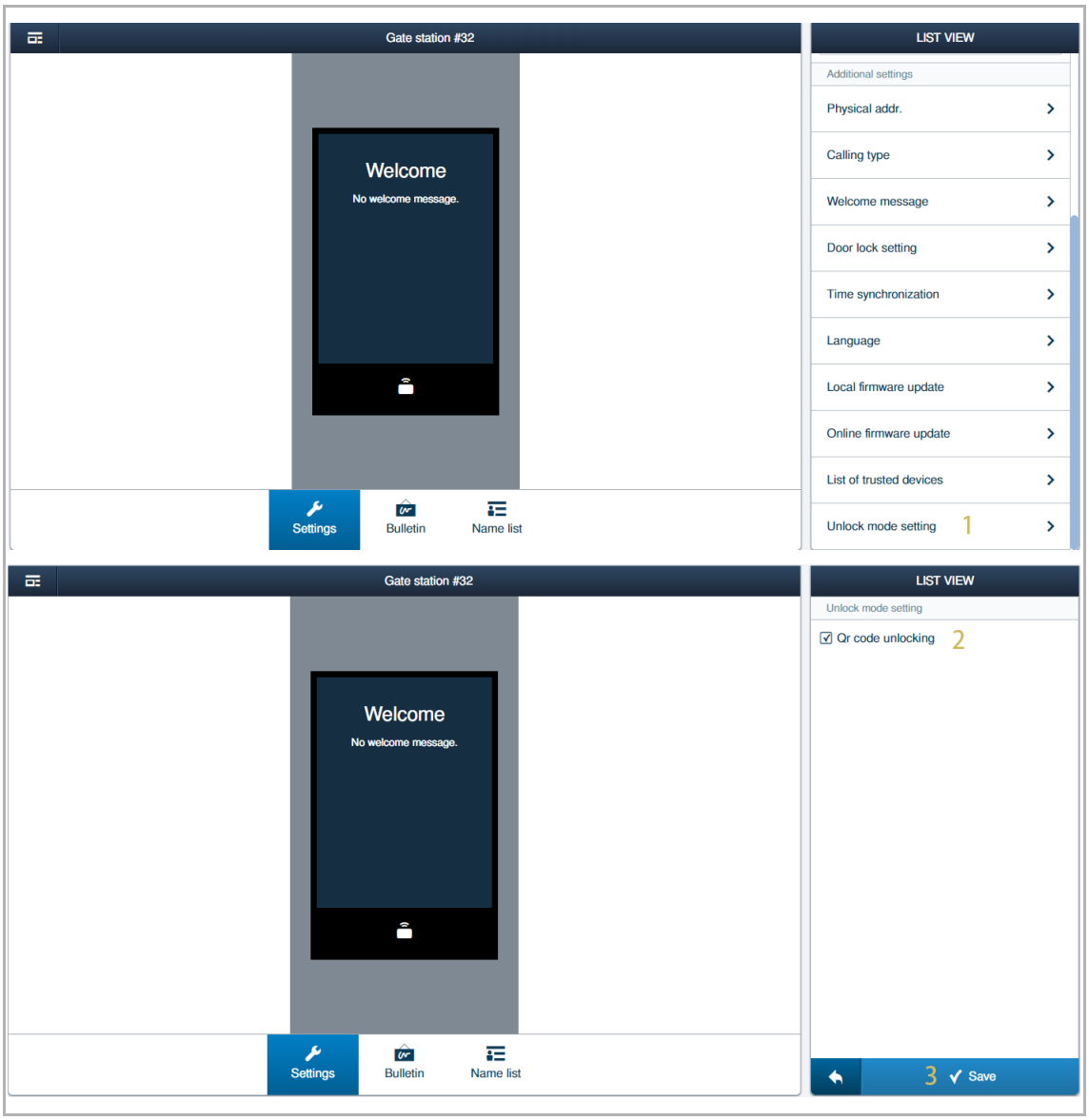
This chapter only applies to the IP touch 5 outdoor station.

Please follow the steps below:

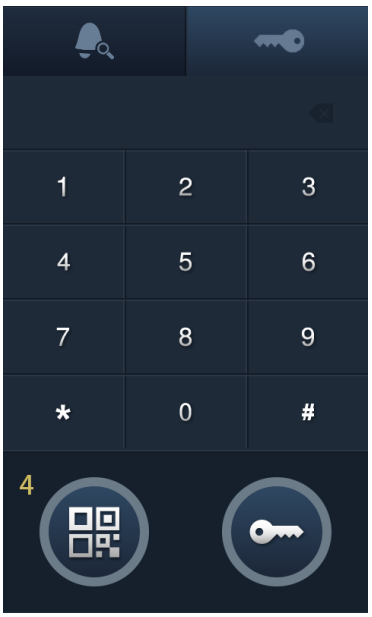
[1] On the designated outdoor station screen, click "Unlock mode setting".

[2] Tick the check box "QR code unlocking" to enable the function.

[3] Click " √ " to save.



[4] The QR code will be displayed on the unlock screen of the IP touch 5 outdoor station.



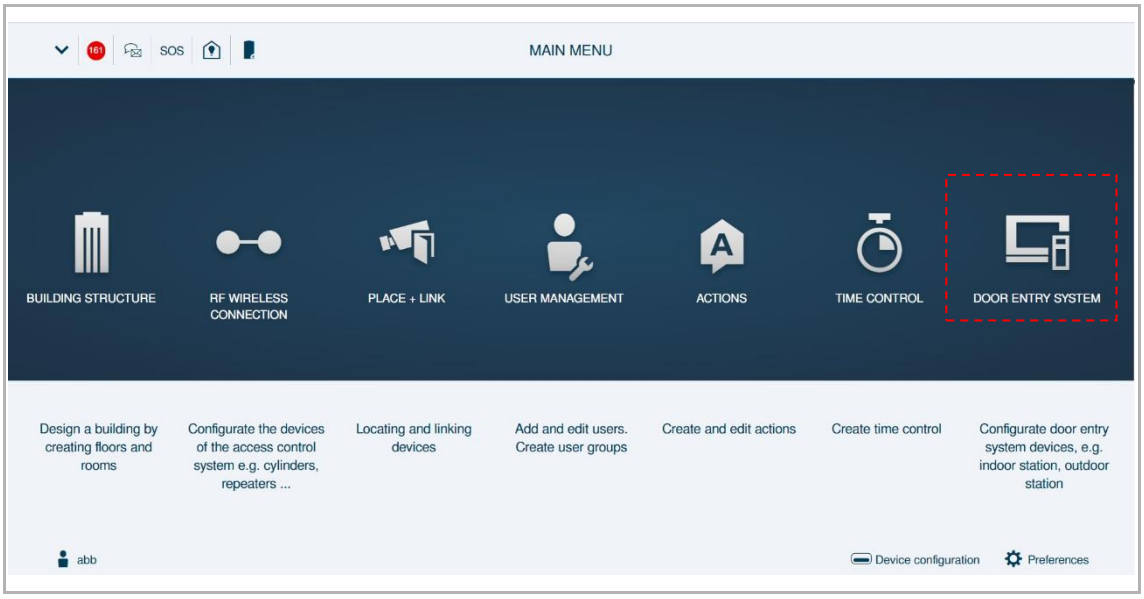
9.5.17 Updating the firmware

see chapter 13.4 “Updating the firmware“ on page 318.

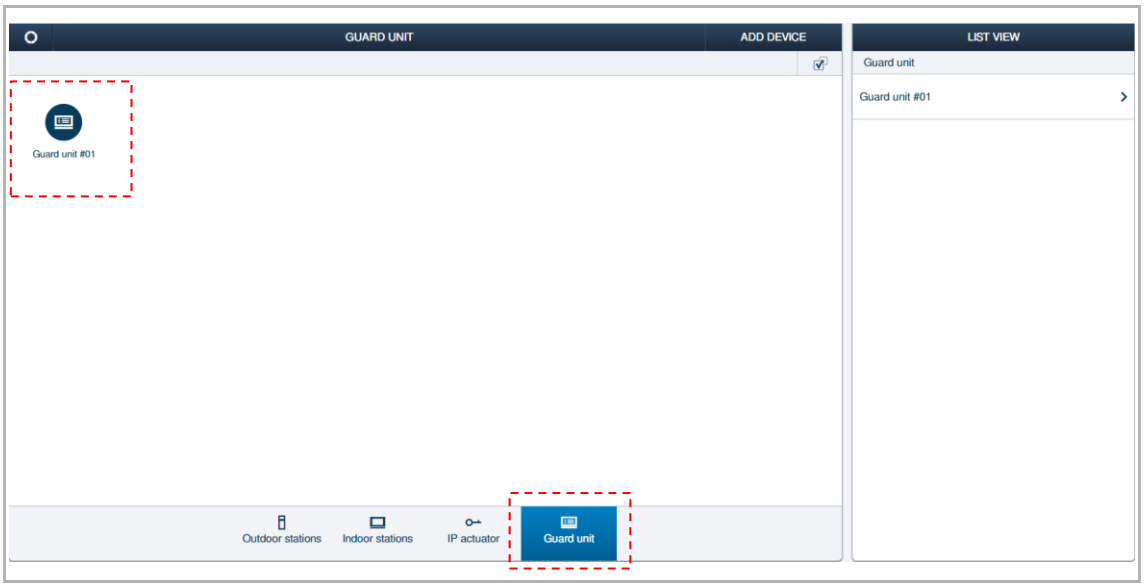
9.6 Configuring the guard unit

Access the designated guard unit screen

On the configuration screen, click "Door entry system", followed by "Guard unit" to access the "Guard unit" screen.



On the "Outdoor station" screen, click the designated guard unit to access the corresponing screen.



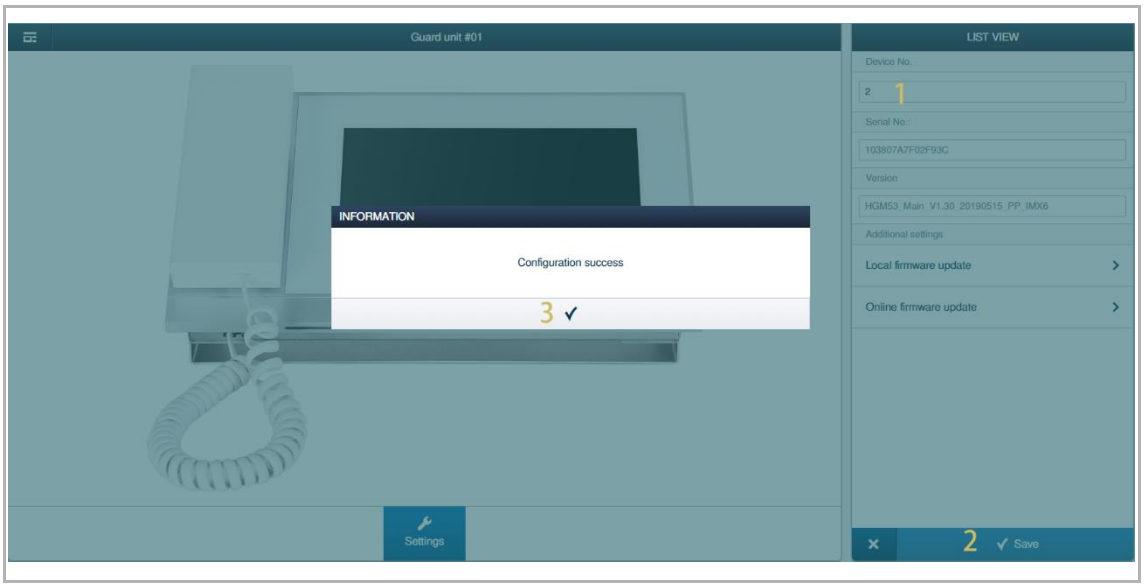
9.6.1 Setting the device number

Please follow the steps below:

[1] On the designated guard unit screen, enter a new device number.

[2] Click " √ " to save.

[3] Click " √ " to confirm.



9.6.2 Viewing the serial number

Please follow the steps below:

[1] On the designated guard unit screen, the serial number is displayed on the screen. It is recommended to write down the serial number for further use.

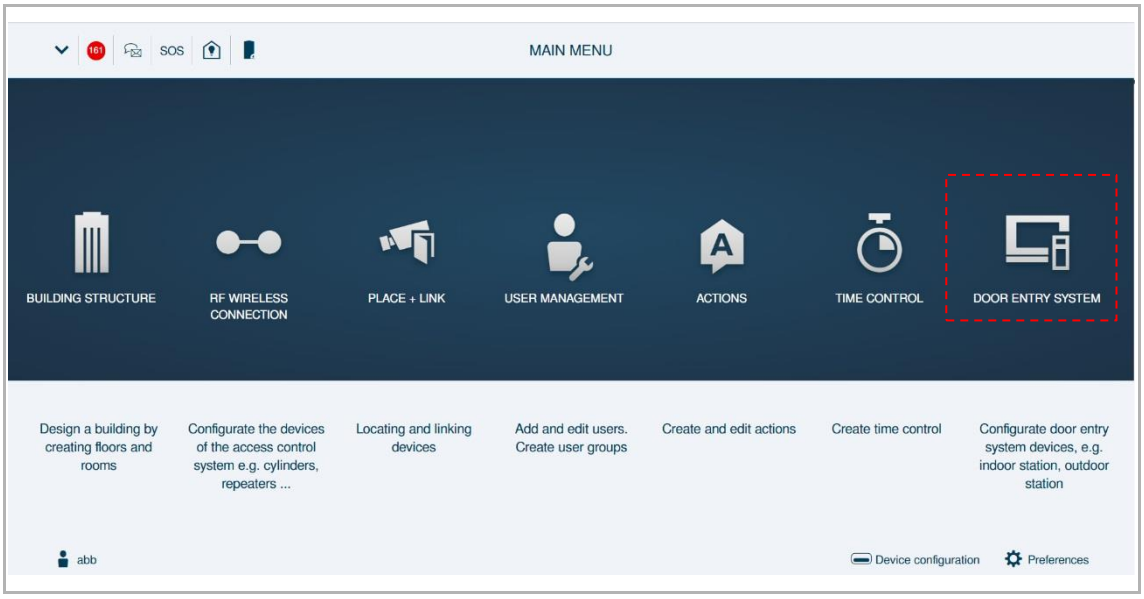
9.6.3 Updating the firmware

see chapter 13.4 “Updating the firmware“ on page 318.

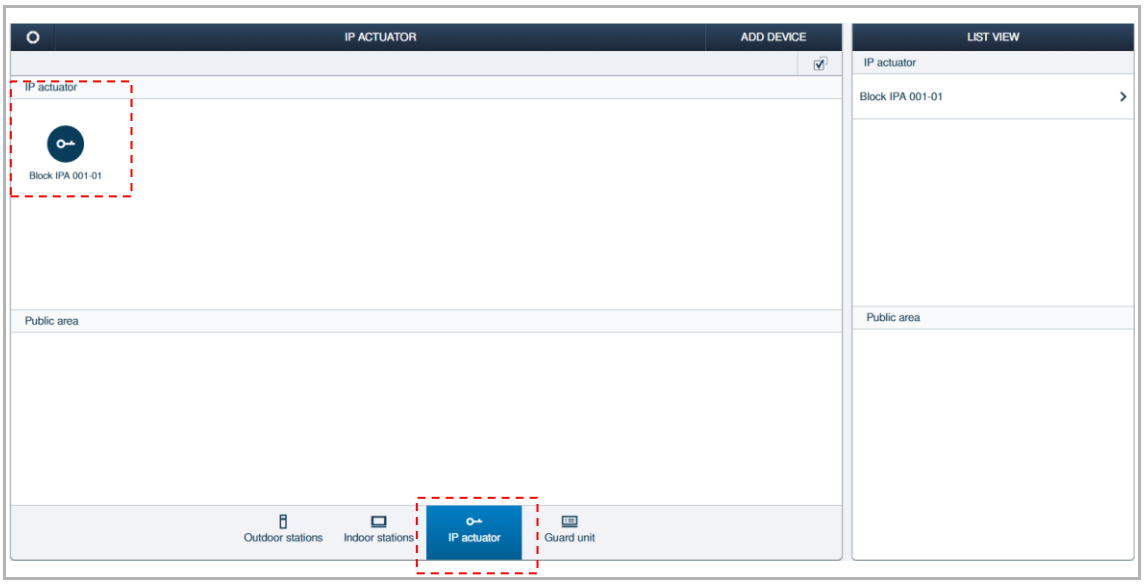
9.7 Configuring the IP Actuator

Accessing the designated IP actuator screen

On the configuration screen, click "Door entry system", followed by "IP actuator" to access the "IP actuator" screen.



On the "IP actuator" screen, click the designated IP actuator to access the corresponding screen.



9.7.1 Viewing the serial number

Please follow the steps below:

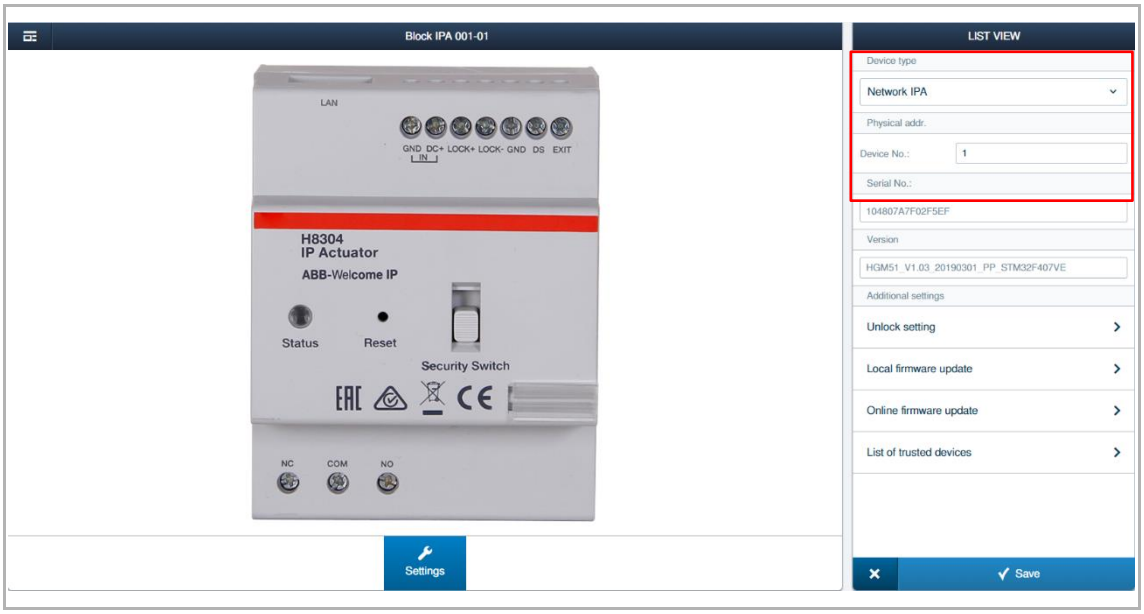
[1] On the designated IP actuator screen, the serial number is displayed on the screen. It is recommended to write down the serial number for further use.

9.7.2 Managing the physical address

There are 3 types devices for selection.

1. Network IPA

If the "Device type" is set to "Network IPA", you need to set the device number (1-32).



2. Building IPA

If the "Device type" is set to "Building IPA", you need to set the block number (1-999) and the device number (1-32).

3. Private IPA

If the "Device type" is set to "Private IPA", you need to set the block number (1-999), floor number (1-63), room number (1-32), and the device number (1-32).

9.7.3 Unlock setting

Please follow the steps below:

[1] On the designated IP actuator screen, click "Unlock setting".

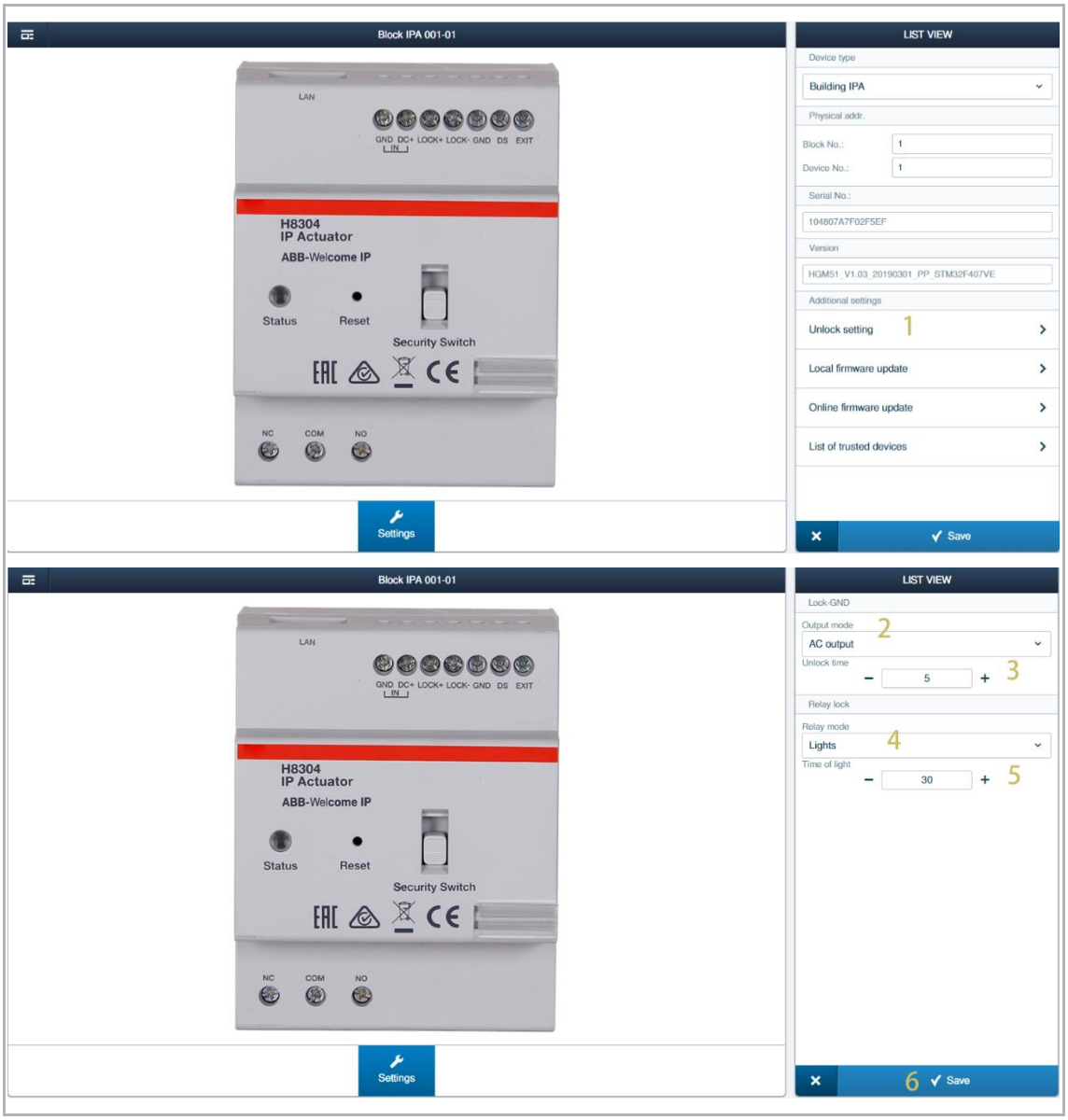
[2] Set the output mode for "Lock-GND" among "AC output", "DC output (NC)" and ", "DC output (NO)".

[3] Set the unlock time for "Lock-GND".

[4] Set the output mode for "Relay lock" between "Unlock" and "Light".

[5] Set the unlock time for "Relay lock".

[6] Click "√" to save.



9.7.4 Managing the trusted devices

see chapter 9.3.2 “Managing the trusted devices for IP actuator“ on page 107.

9.7.5 Releasing the IP actuator related to the outdoor station

Please follow the steps below:

[1] On the designated outdoor station screen, click "Door lock setting".

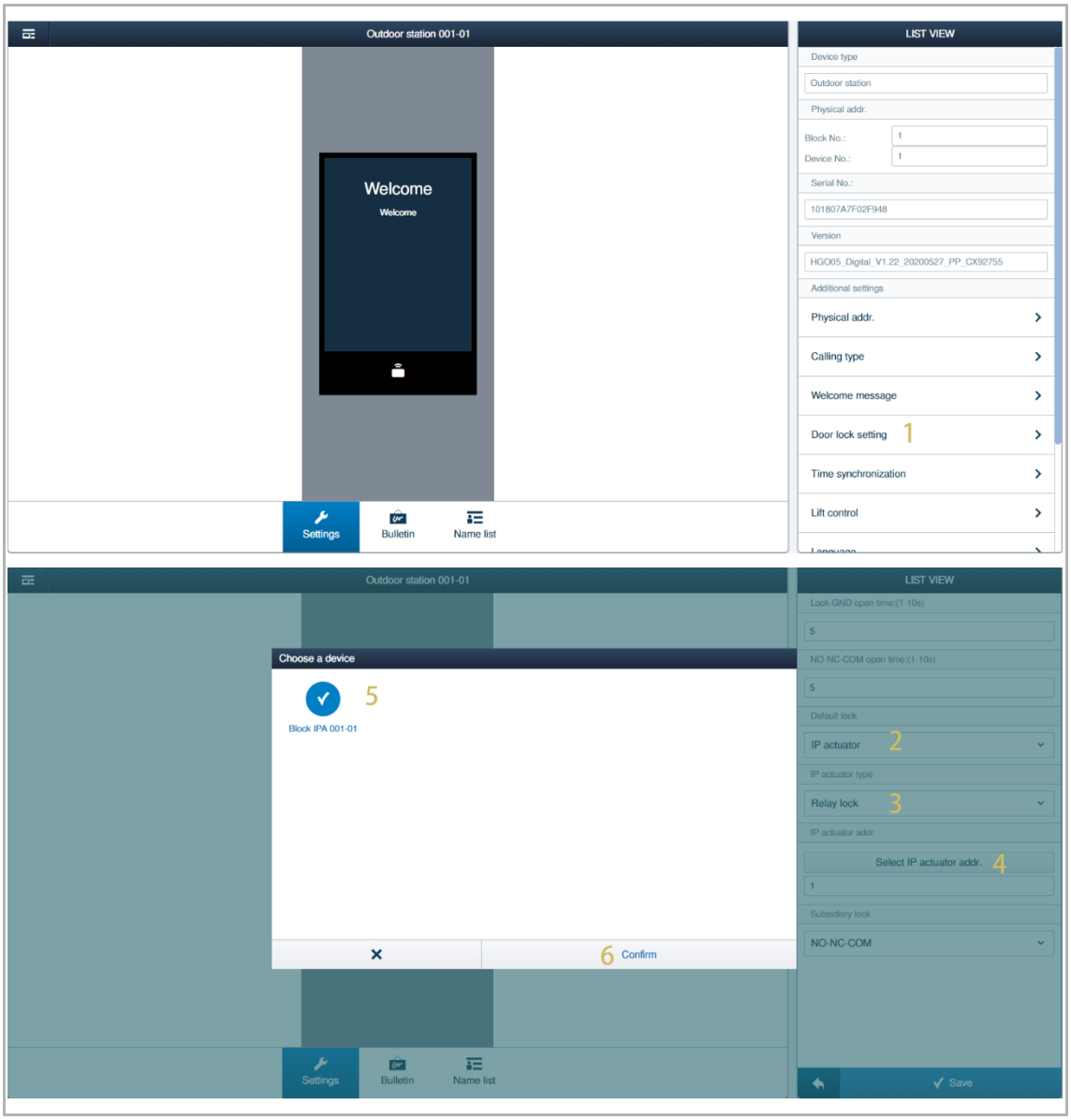
[2] Set door type to "IP actuator".

[3] Select IP actuator type between "Power lock" and "Relay lock".

[4] Click "Select IP actuator addr.".

[5] Click to select the designated IP actuator.

[6] Click "Confirm".

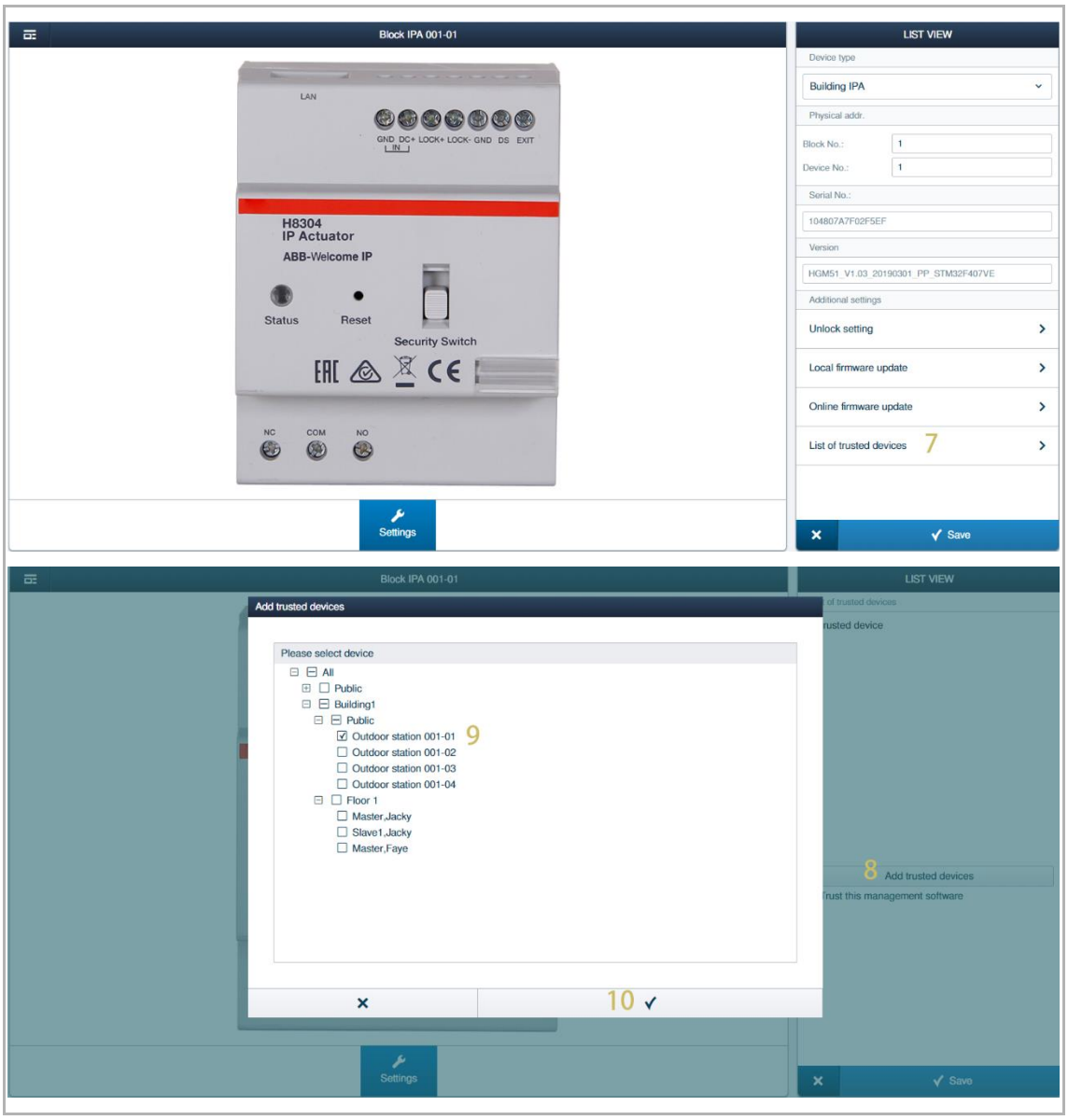


[7] On the designated IP actuator screen, click "List of trusted devices".

[8] Click "Add trusted devices".

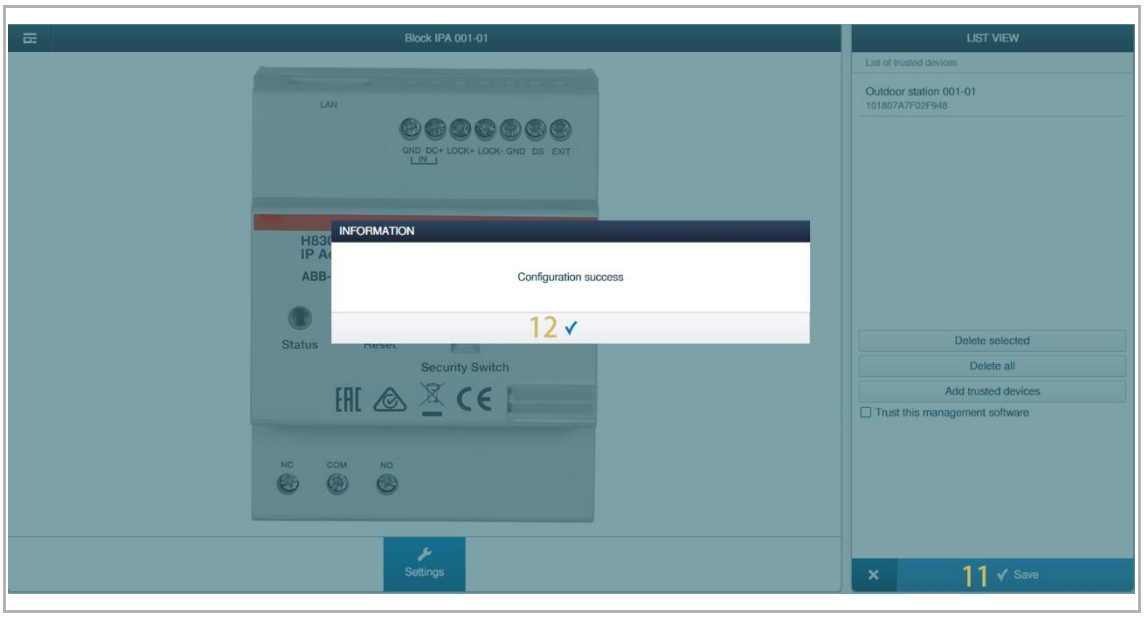
[9] Click the designated outdoor station.

[10] Click " √ " to save.



[11]Click " √ " to save.

[12]Click " √ " to confirm.



9.8 Removing the devices

9.8.1 Removing the devices one by one

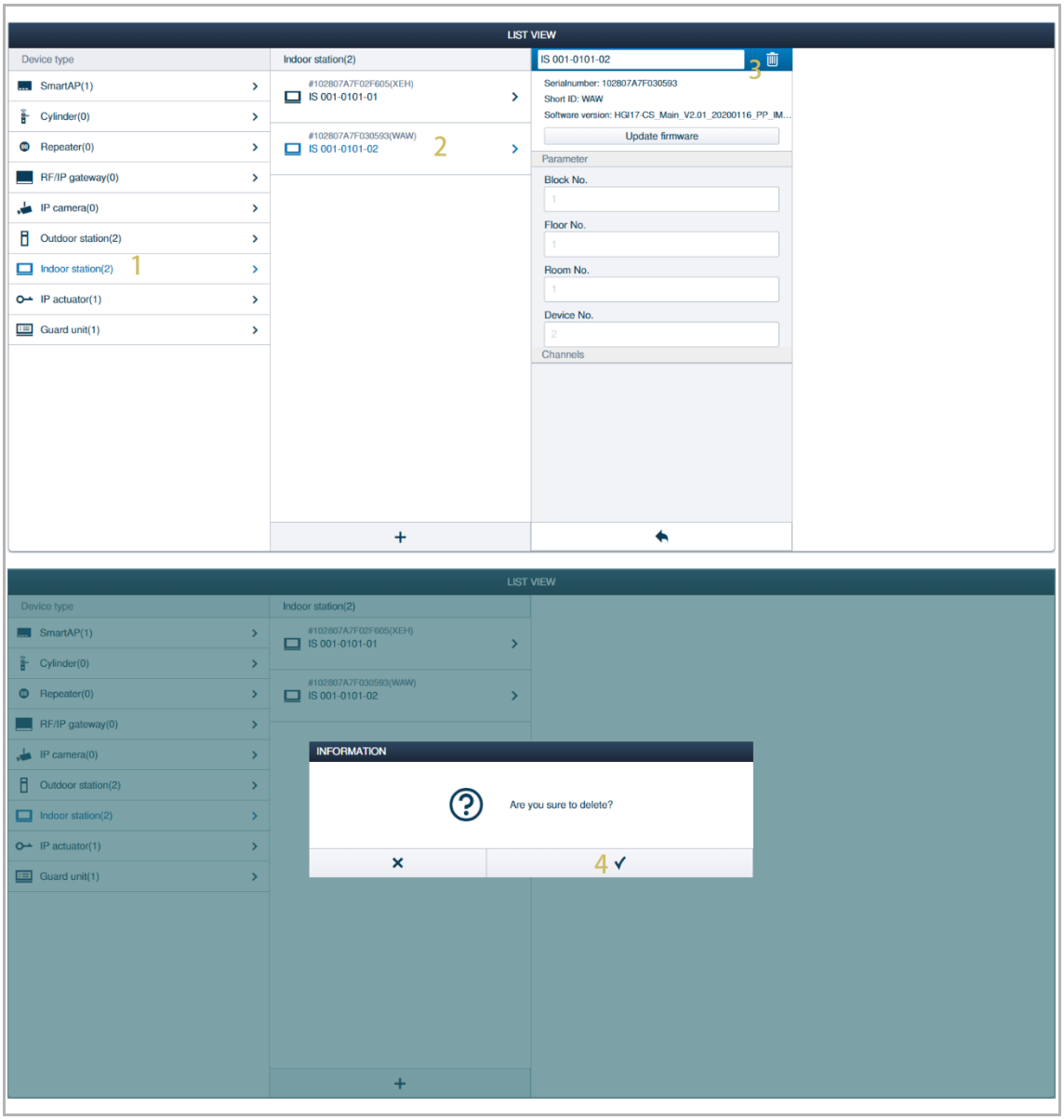
Please follow the steps below:

[1] On the "Device configuration" screen, click a device (e.g. "Indoor station").

[2] Click the designated device (e.g. "Indoor station 2").

[3] Click "  ".

[4] Click " √ " to confirm.



9.8.2 Removing the devices in batch

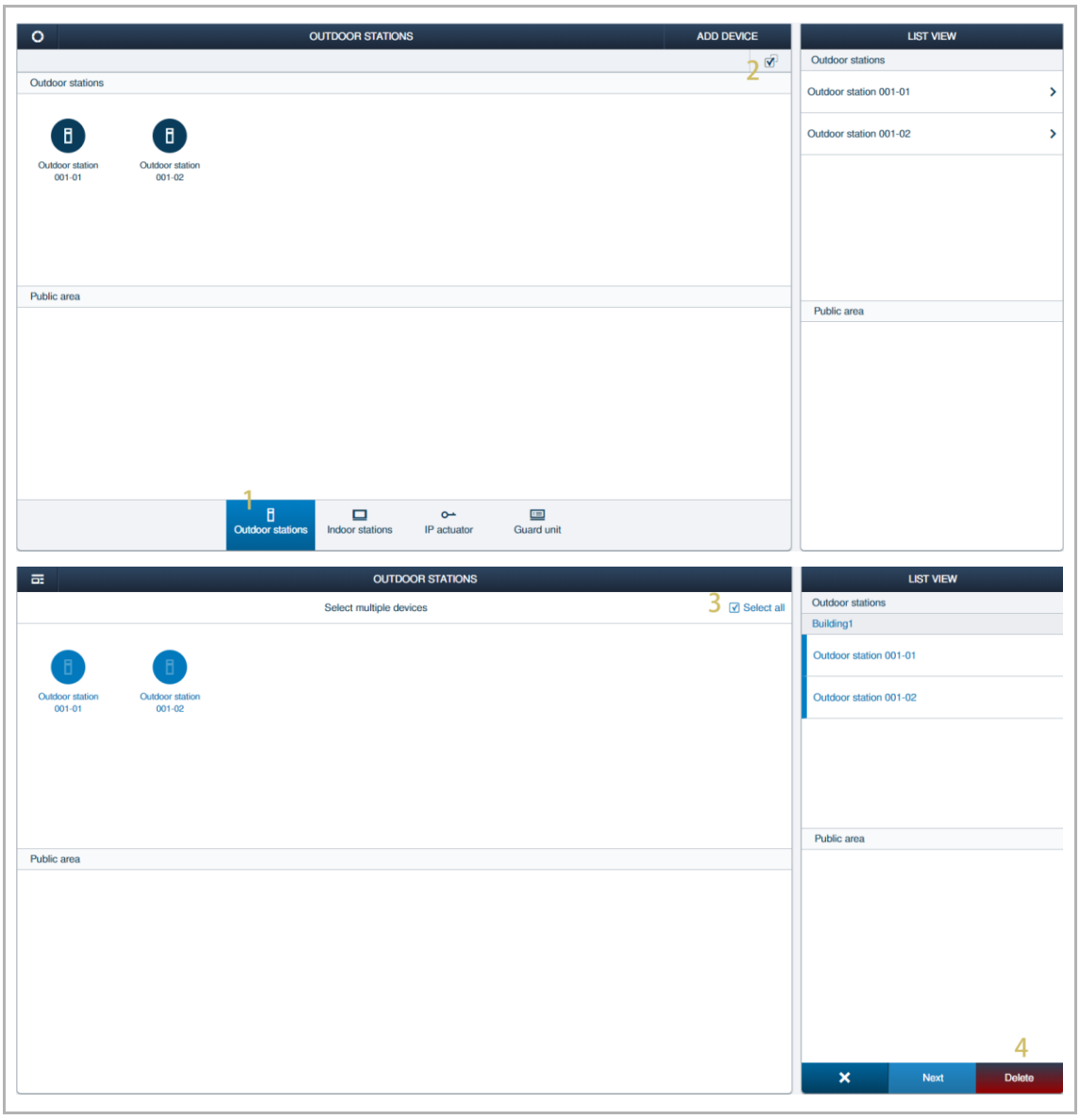
Please follow the steps below:

[1] On the "Device configuration" screen, click a Door Entry System device (e.g. "Outdoor station").

[2] Click " ".

[3] Click "Select all" to select all devices or click the designated device one by one to select multiple devices.

[4] Click "Delete".



10 Operating the AccessControl devices

10.1 AccessControl topology

Scenario 1: A small number of the "Electronic locking cylinders" used and short distance between devices

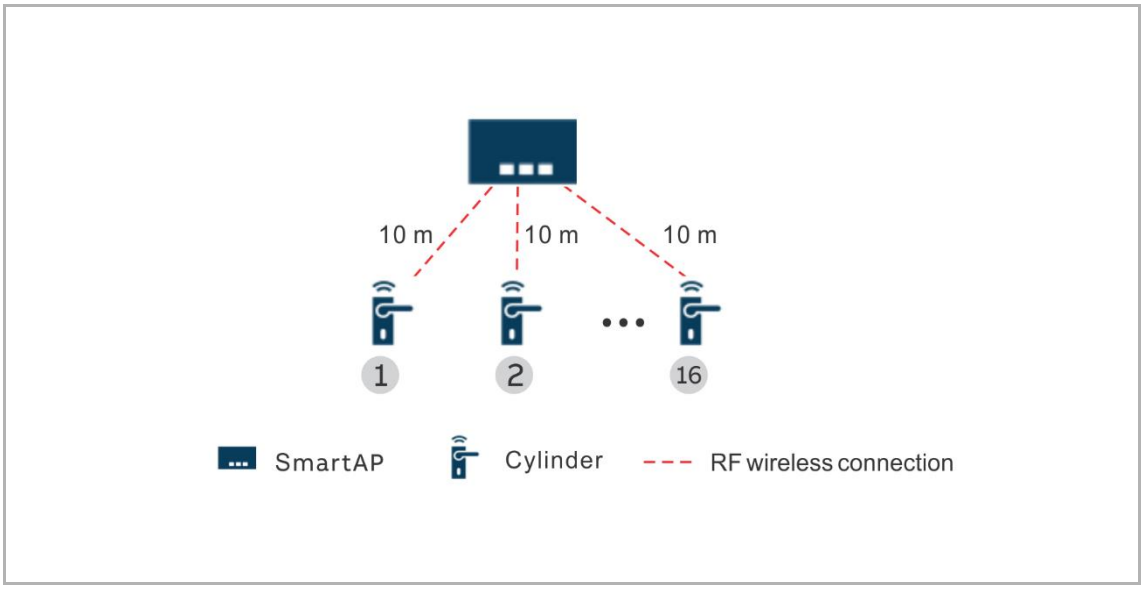
1. Preconditions

- The number of "Electronic locking cylinders" operated by "Smart Access Point" is ⩽ 16 units.
- The distance from the furthest "Electronic locking cylinder" to "Smart Access Point" is ⩽ 10 metres.

2. Capacity

- The radio range between each RF device is ⩽ 10 metres.
- Up to 16 "Electronic locking cylinders" can be operated via a "Smart Access Point".

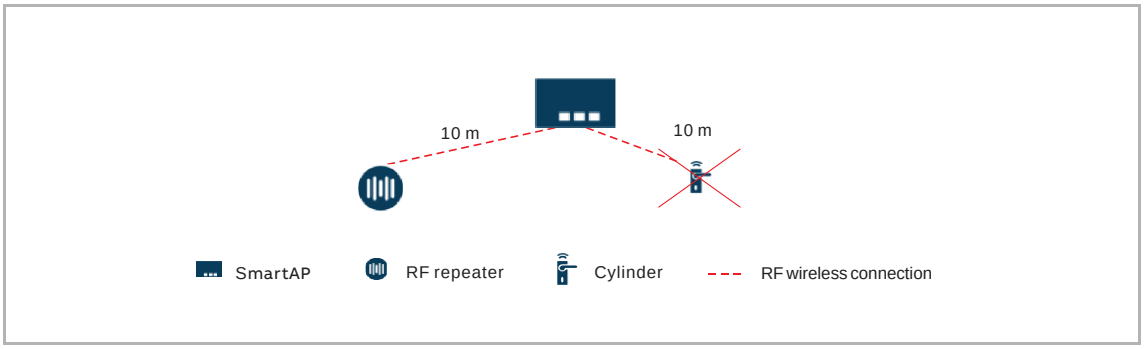
3. Topology



Scenario 2: A small number of the "Electronic locking cylinders" used and moderate distance between devices

1. Preconditions

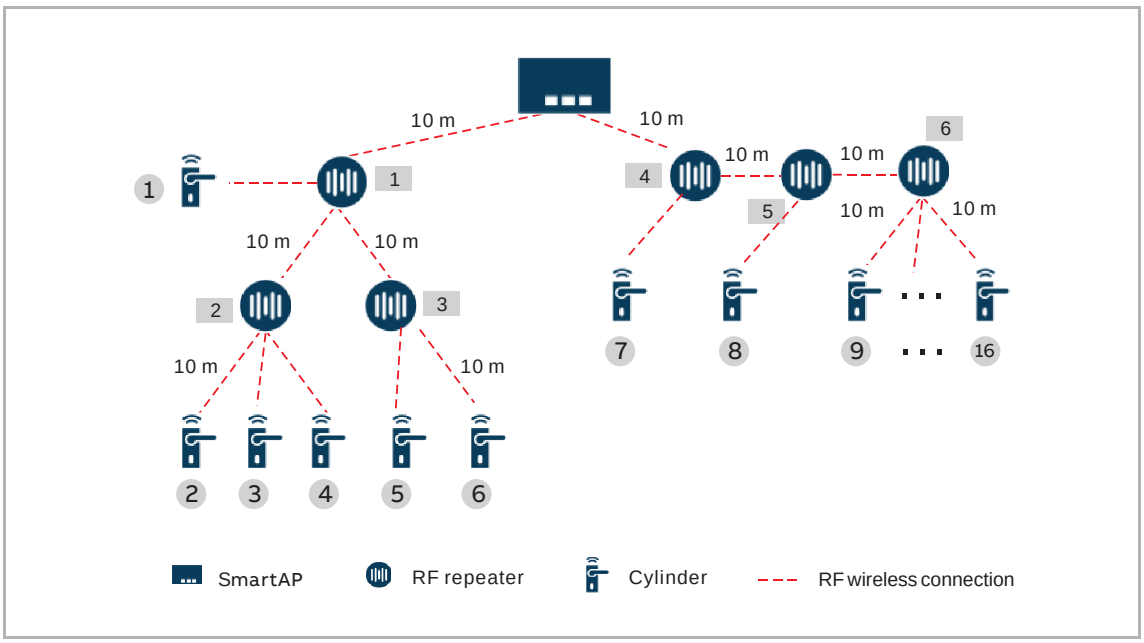
- The number of "Electronic locking cylinders" operated by "Smart Access Point" is ⩽ 16 units.
- The distance from the furthest "Electronic locking cylinder" to "Smart Access Point" is ⩽ 40 metres.
- "RF Repeater" is necessary to extend the radio range, each "RF Repeater" extends the radio range by 10 metres.
- An "Electronic locking cylinder" and a "RF Repeater" cannot be the slave devices of one "Smart Access Point" at the same time.



2. Capacity

- The radio range between each RF device is ⩽ 10 metres.
- Up to 16 "Electronic locking cylinders" can be operated via one "Smart Access Point".
- Up to 6 "RF Repeaters" can be operated via one "Smart Access Point".
- Up to 3 "RF Repeaters" can be connected to one "Smart Access Point" in series in a radio line.
- Each "RF Repeater" can have up to 2 slave "RF Repeaters".
- The "Electronic locking cylinder" can be freely assigned to the "RF Repeater" in the radio line.
- The maximum radio range between an "Electronic locking cylinder" and "Smart Access Point" is 40 metres.

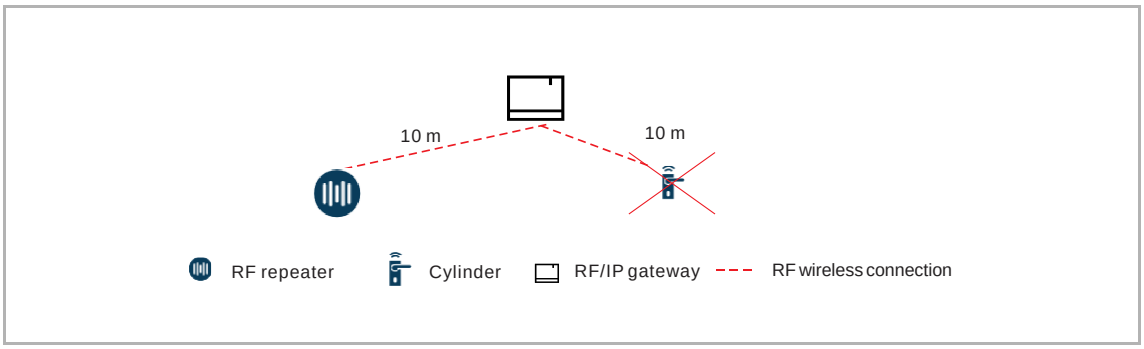
3. Topology


10 m
10 m
10 m
10 m
10 m
10 m
10 m
10 m
10 m
10 m
1
2
3
4
5
6
7
8
9
16
SmartAP
RF repeater
Cylinder
RF wireless connection

Scenario 3: A large number of "Electronic locking cylinders" used and long distance between devices

1. Preconditions

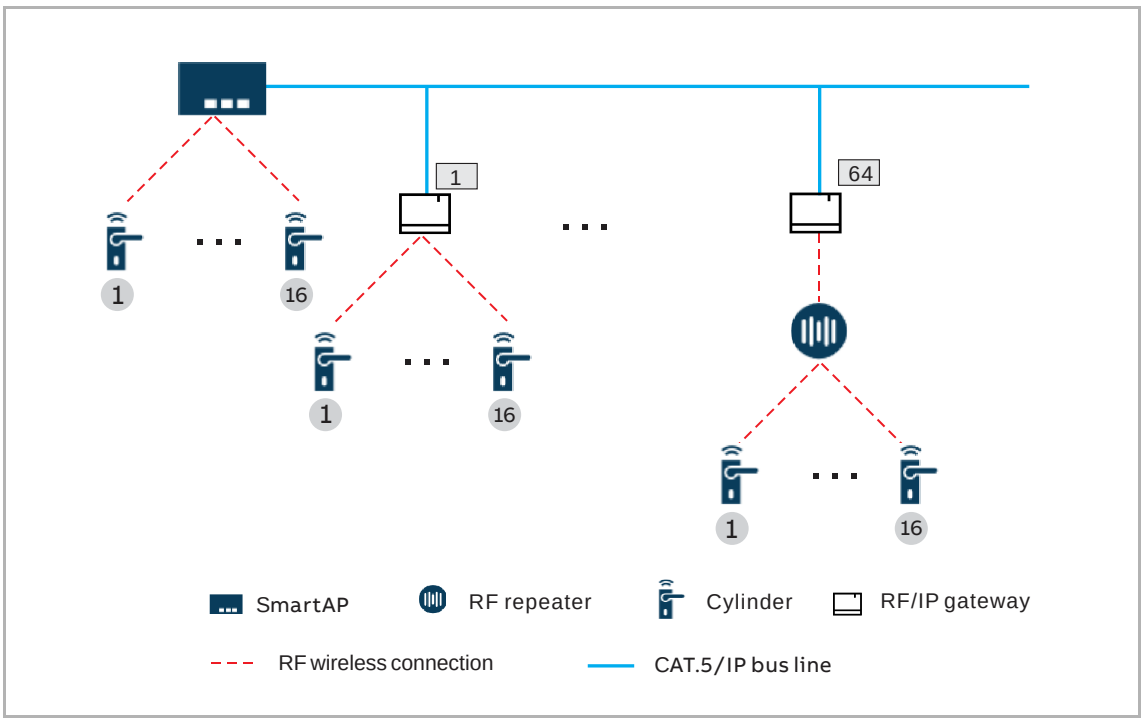
- The number of "Electronic locking cylinders" operated by "Smart Access Point" is ⩽ 600 units.
- "RF/IP Gateway" is necessary to extend the radio range, each "RF/IP Gateway" can be seen as "Smart Access Point" in a radio line.
- An "Electronic locking cylinder" and a "RF Repeater" cannot be the slave devices of one "RF/IP Gateway" at the same time.



2. Capacity

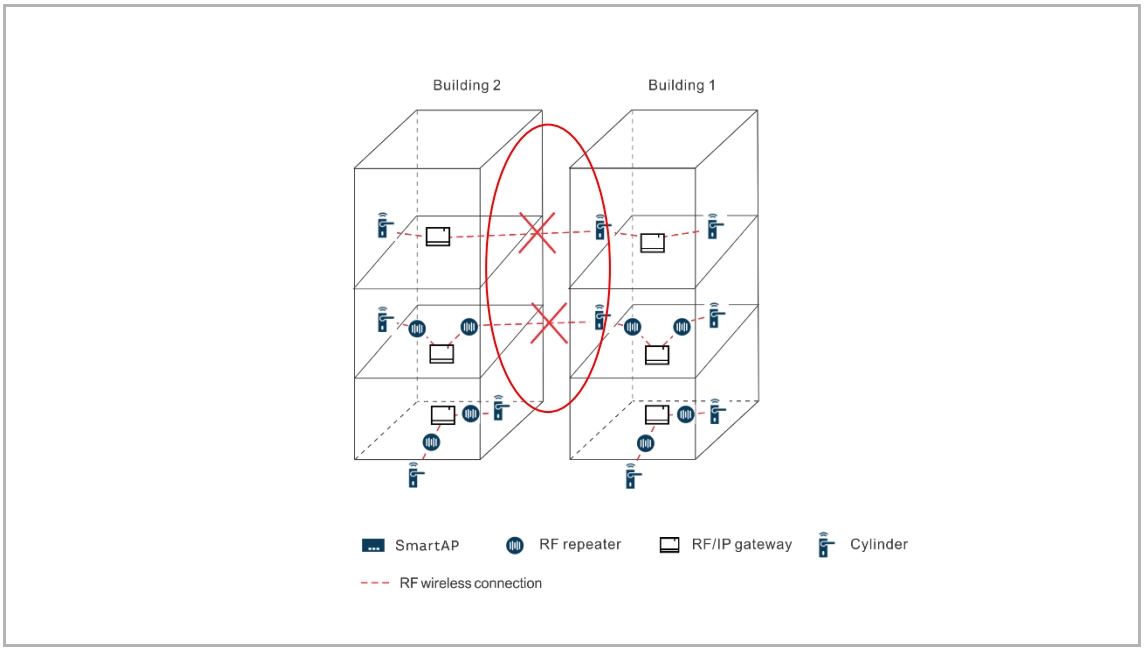
- The radio range between each RF device is ⩽ 10 metres.
- Up to 64 RF/IP Gateways can be operated via one "Smart Access Point".
- Up to 500 "Electronic locking cylinders" can be operated via a "Smart Access Point" due to limited system performance.
- Up to 16 "Electronic locking cylinders" can be operated via one "RF/IP Gateway".
- Up to 6 "RF Repeaters" can be operated via one "RF/IP Gateway".
- Up to 3 "RF Repeaters" can be connected to one "RF/IP Gateway" in series in a radio line.
- Each "RF Repeater" can have up to 2 slave "RF Repeaters".
- The "Electronic locking cylinder" can be freely assigned to the "RF Repeaters" in the radio line.

3. Topology



Note

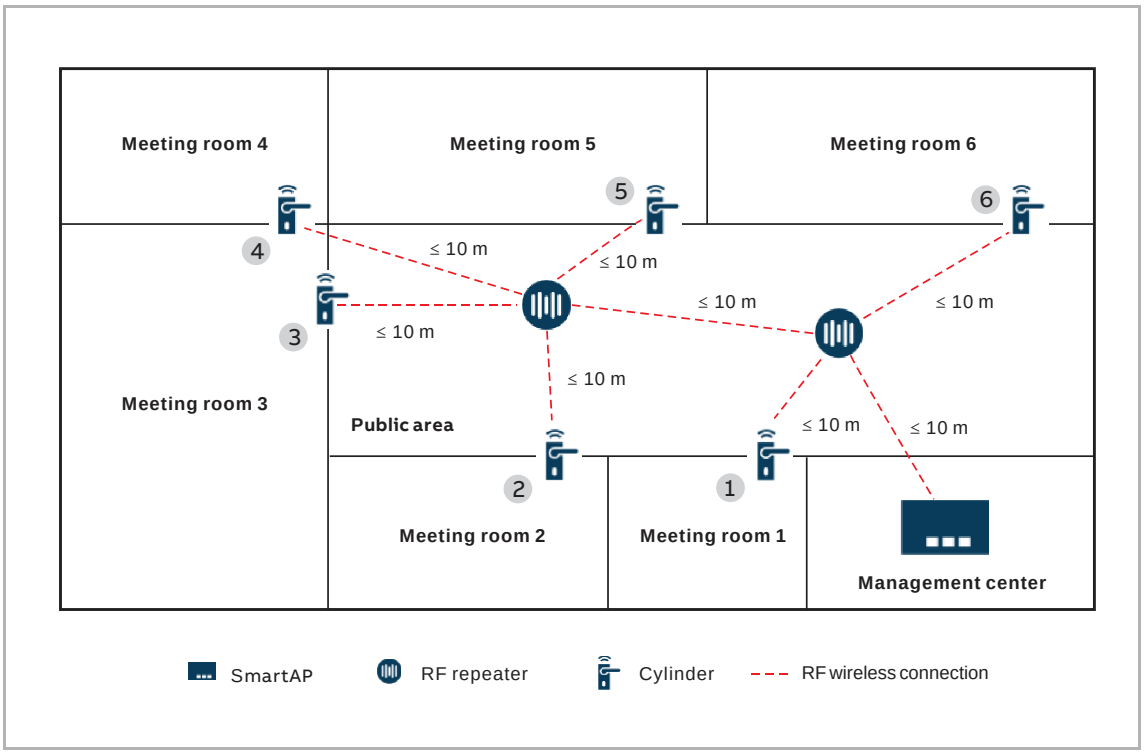
The "Electronic locking cylinder" can’t be connected across the buildings (see the diagram below).



Demo case

This demo case is used to familiarize yourself with the operations of AccessControl devices.

You need to adjust your operations when you operate an actual project.



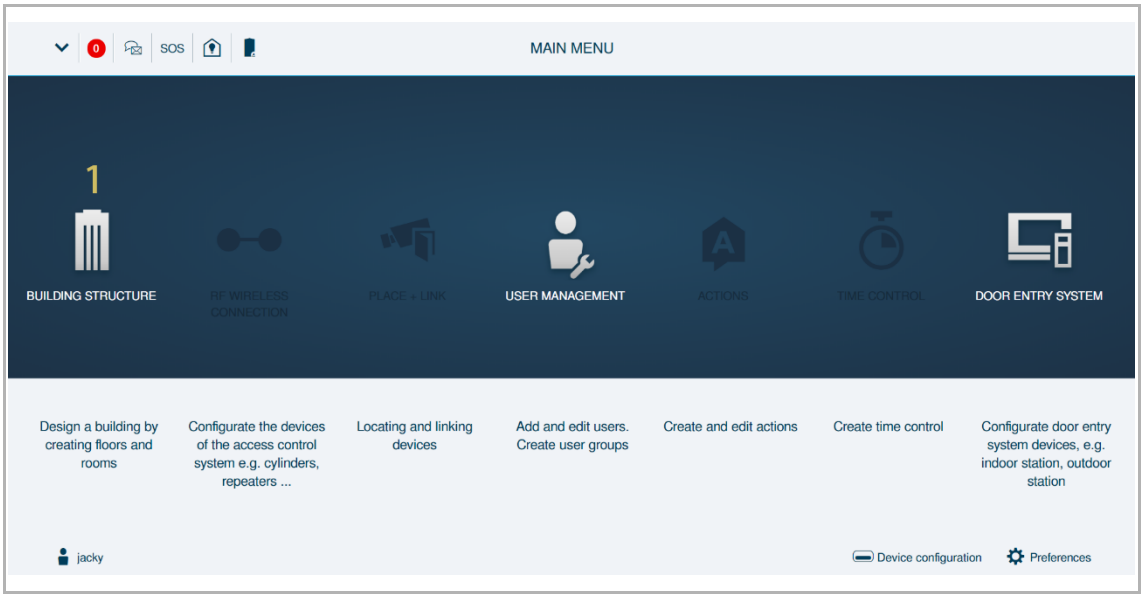
10.2 Creating a building

10.2.1 Creating a building via "Smart Access Point"

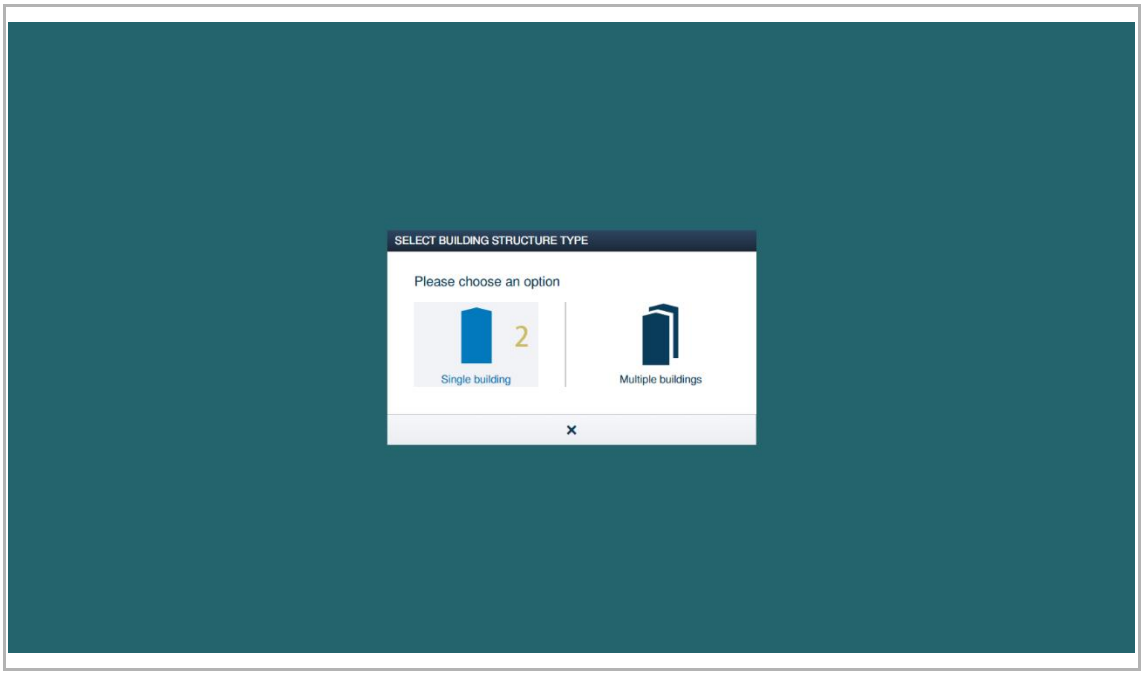
The following operations are all based on the demo case.

Please follow the steps below:

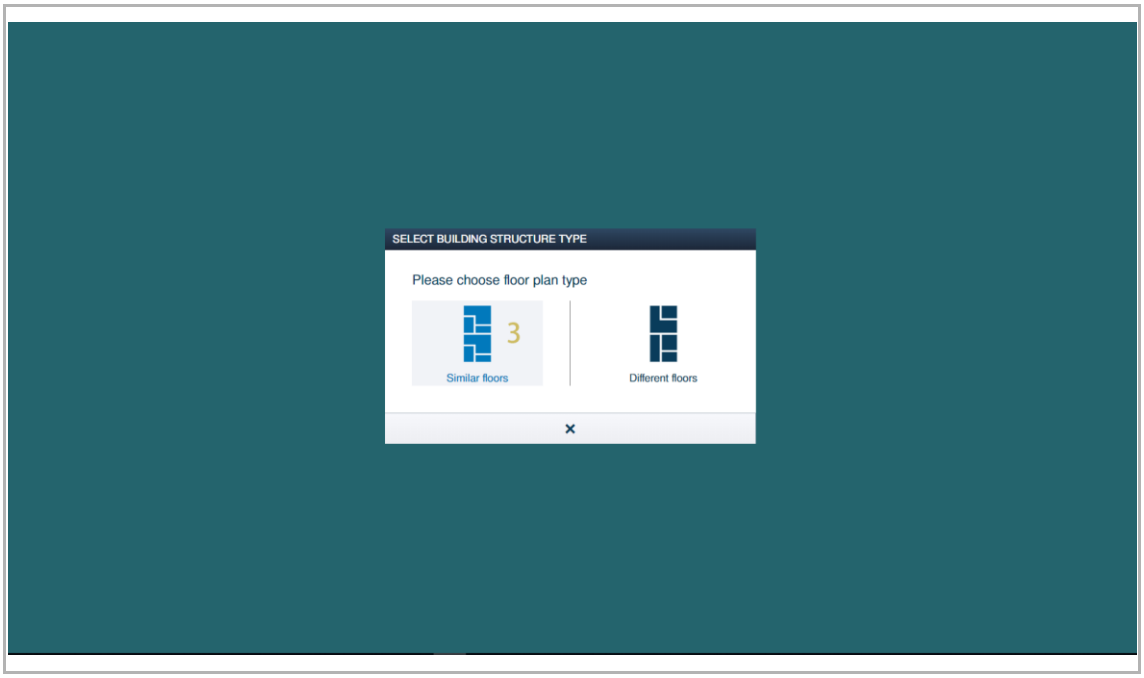
[1] On the configuration screen, click "Building structure".



[2] Click "Single building".



[3] Click "Similar floors".



[4] Drag the "Building" icon onto the floor plan.

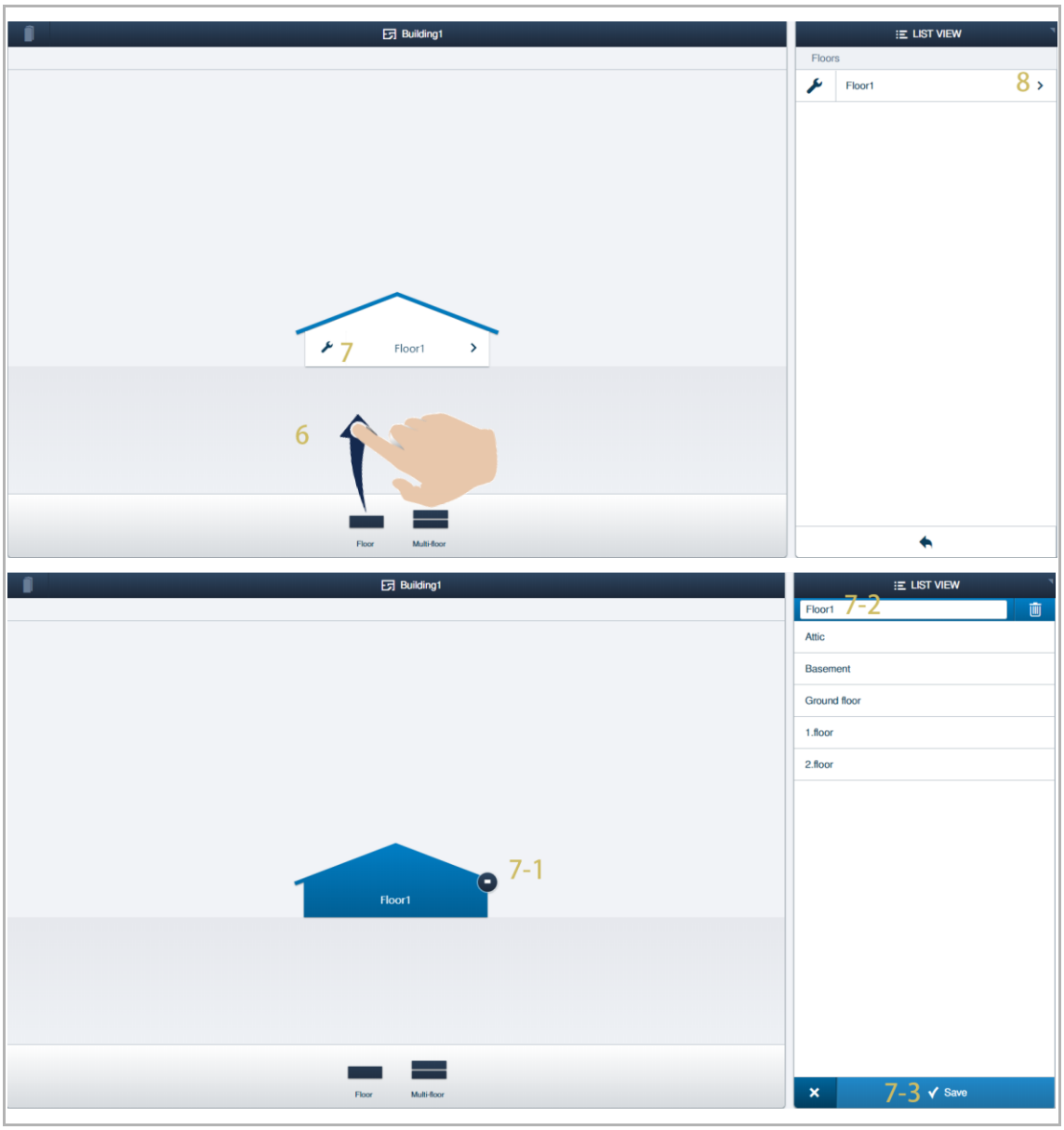
[5] Click ">" to continue.

[6] Drag the "Floor" icon onto the floor plan.

[7] Click " " to edit the floor (optional).

- 7-1, click the icon to change the floor shape.
- 7-2, change the floor name.
- 7-3, save the change.

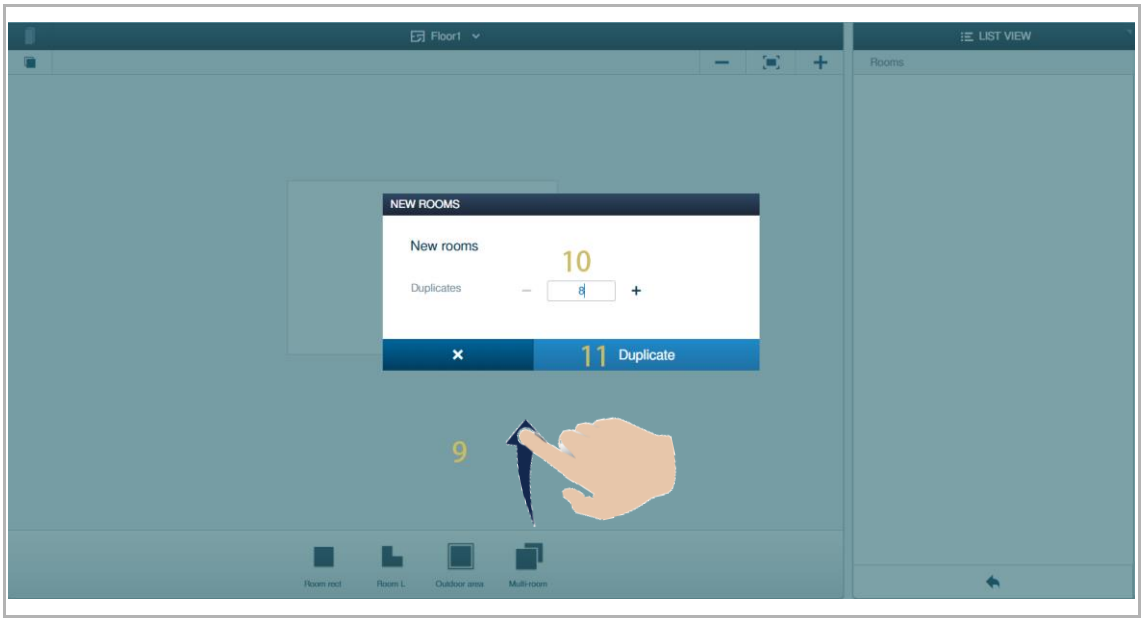
[8] Click ">" to continue.



[9] Drag the "Multi-room" icon into the floor plan.

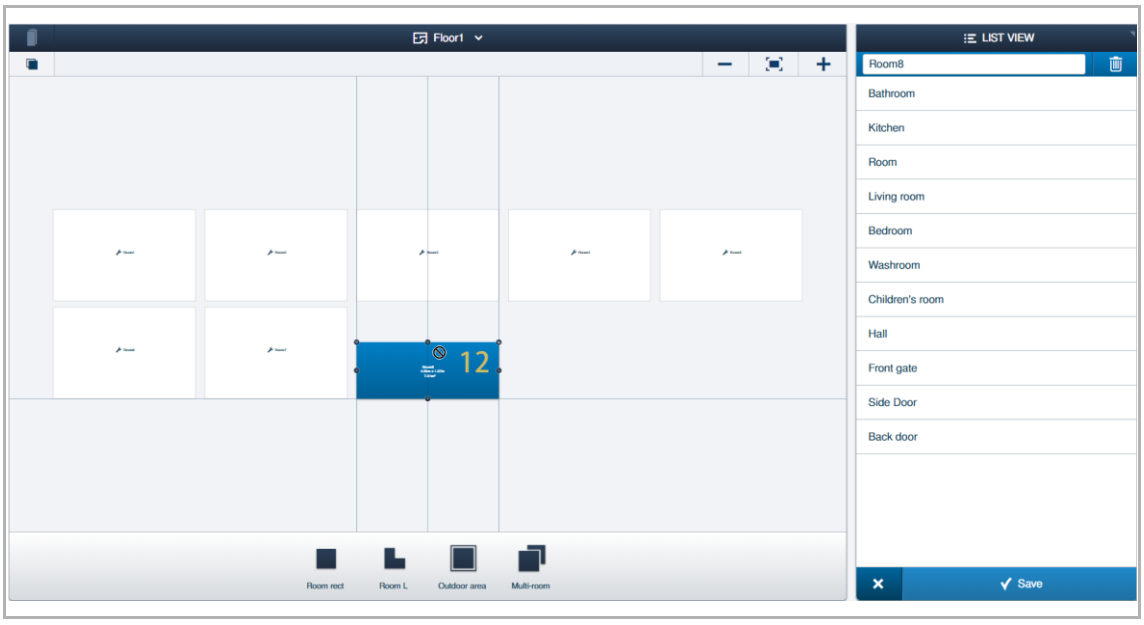
[10]Enter the room number (e.g. "8" for demo case 1).

[11]Click "Duplicate".



[12]Click on the designated room to edit the room shape.

- Click the icon " " to change the height or the width of the room shape.
- Click the icon " " to restore the room shape.
- Click the icon " " to change the room shape from "Rectangle" shape to "L" shape.
- Click the icon " " to change the room shape from "L" shape to "Rectangle" shape.



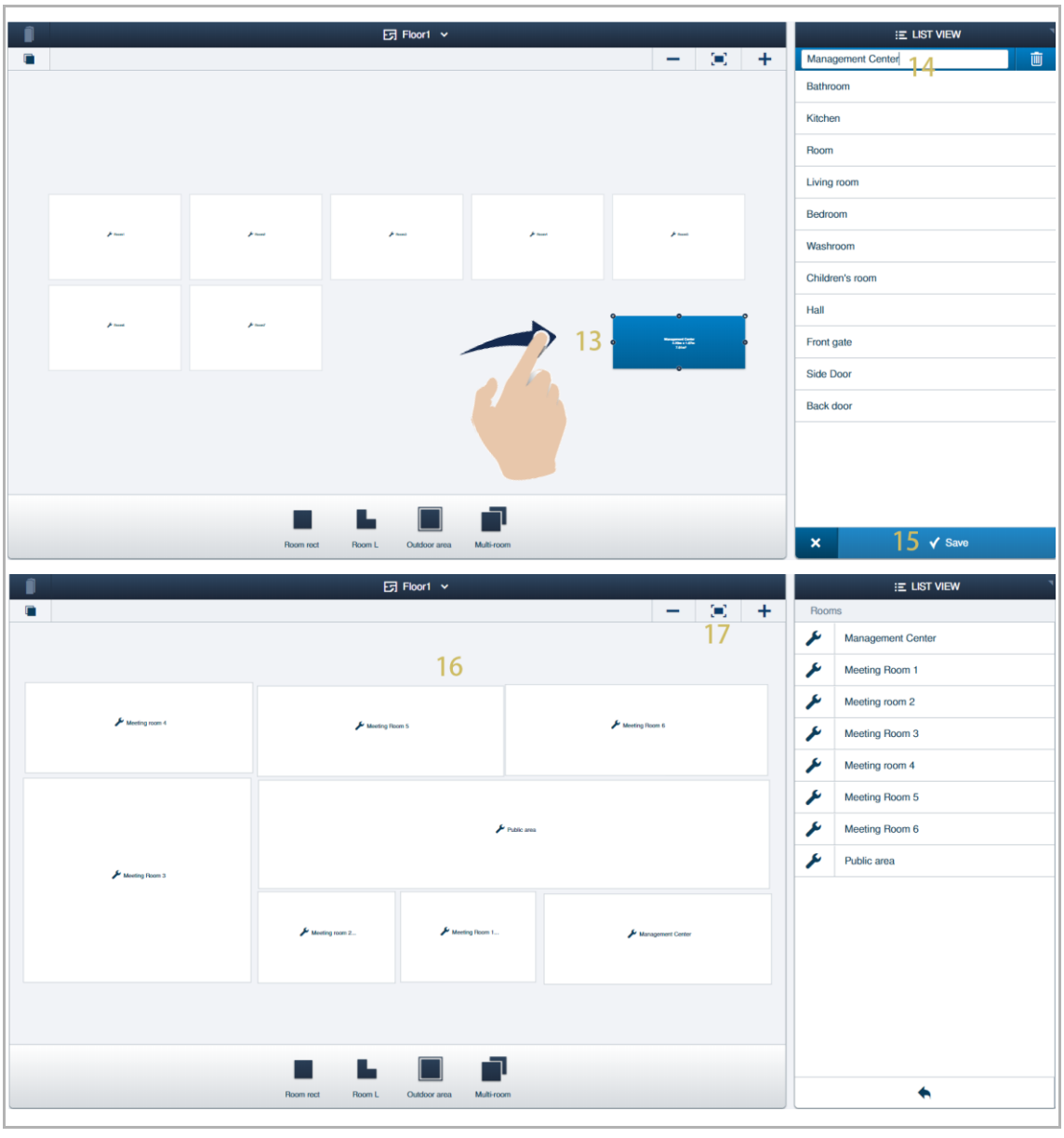
[13]Drag the designated room to move it.

[14]Edit the room name.

[15]Click " √ " to save.

[16]Repeat steps from 12-15 to change other rooms one by one.

[17]Lastly, click "  " to display all the rooms in the floor plan.

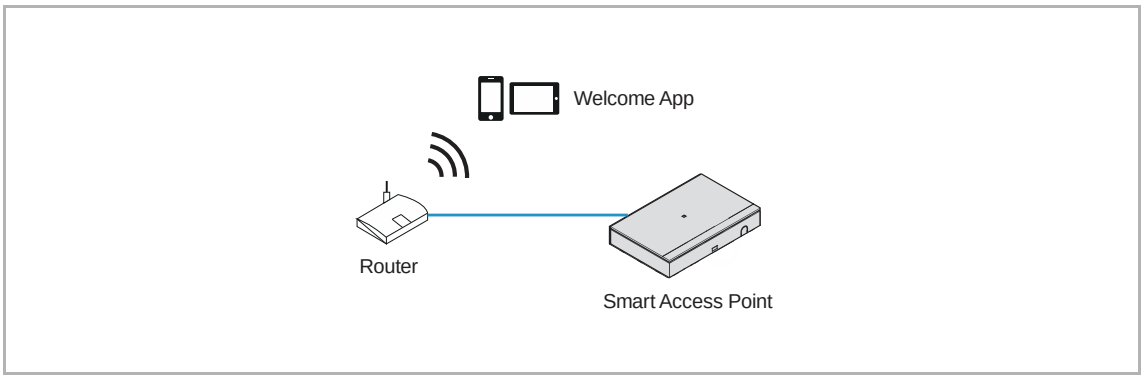


10.2.2 Creating a building via Welcome App

"Smart Access Point" can import the building created on Welcome App. You can import one building once or several buildings in batch.

Precondition

- Welcome APP must be in the same network with "Smart Access Point".
- The building has been created on Welcome App. See more details on the product manual of Welcome App.



Importing rule

Building structure will be overwritten according to the rules below:

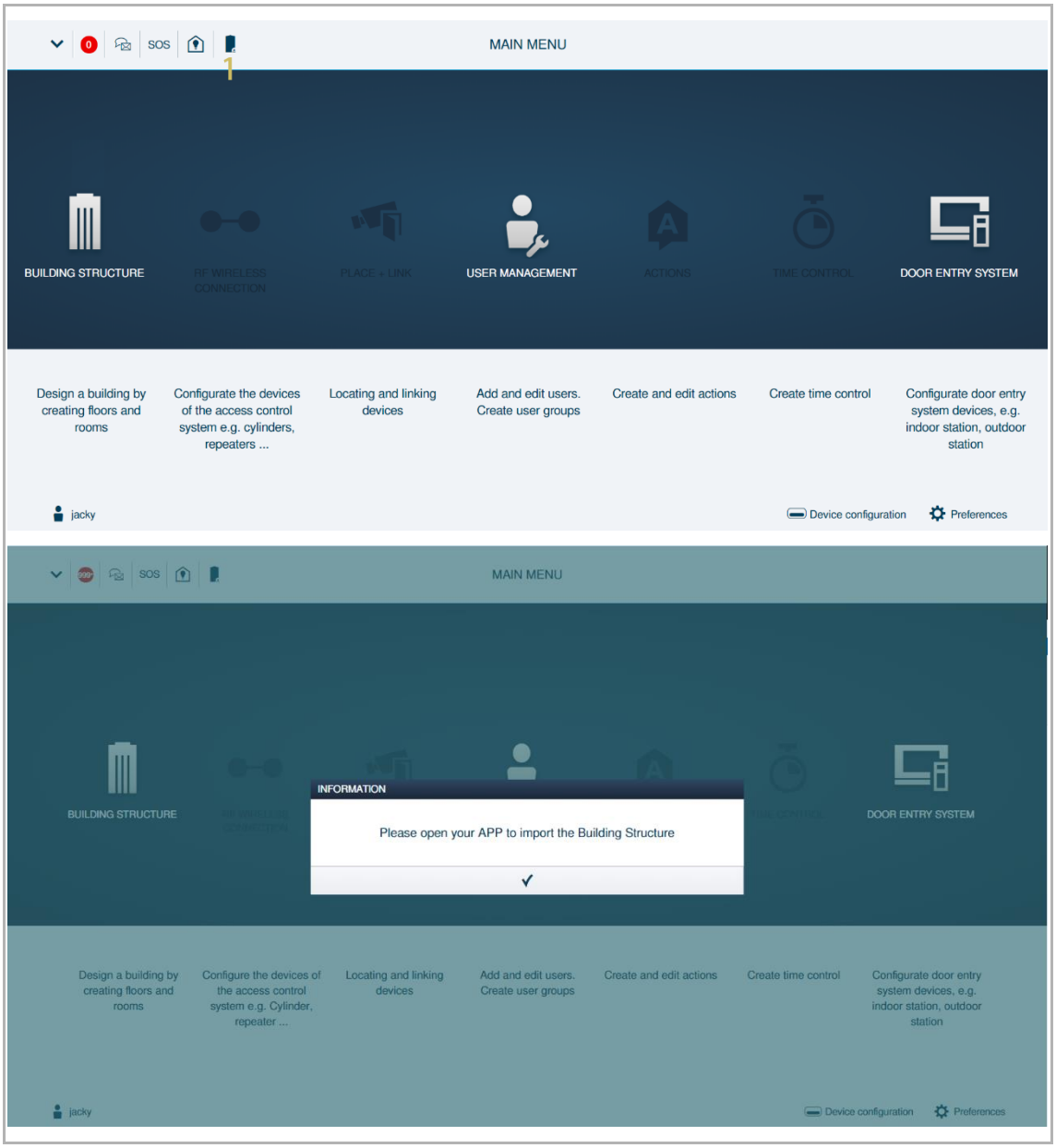
- A, B, C, D, E, F means building number.
- B and B+ has the same building number.
- + means the building structure has been changed.

Welcome App	"Smart Access Point" before	"Smart Access Point" after
B+	A, B, C	A, B+, C
B+, C+	A, B, C	A, B+, C+
D, E, F	A, B, C	A, B, C, D, E, F

Importing the building from Welcome App

Please follow the steps below:

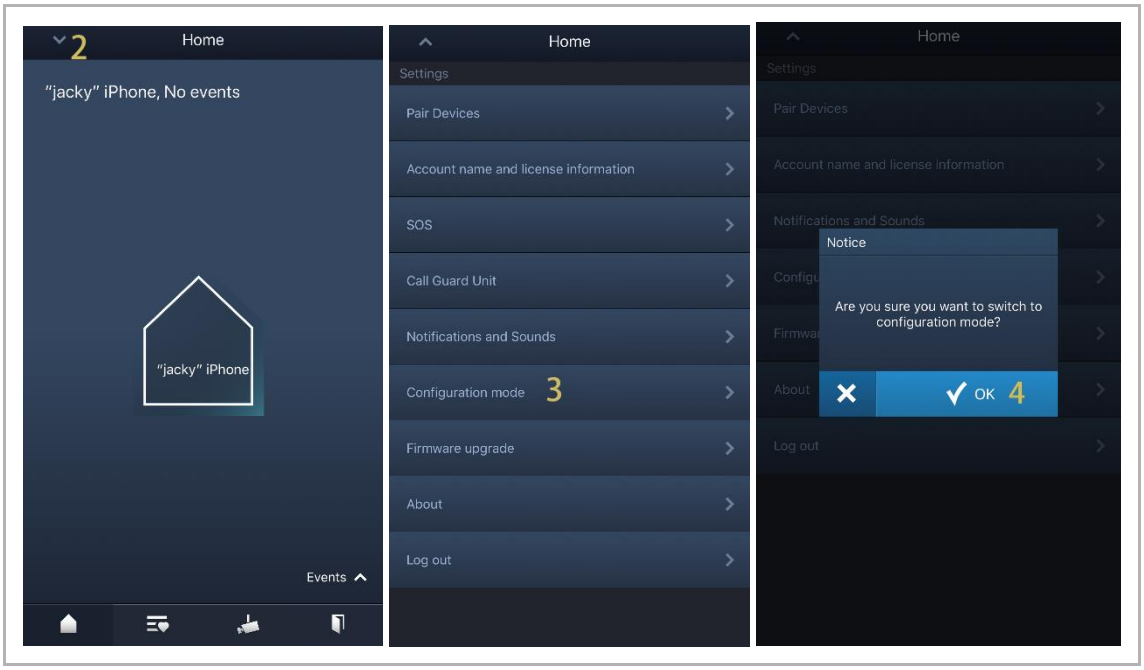
[1] On the configuration screen, click " " , a pop-up window will appear.



[2] On the Welcome App "Home" screen, tap "∨".

[3] Tap "Configuration mode".

[4] Tap " √ " to continue.



[5] On the "Projects" screen, swipe the project name to the right.

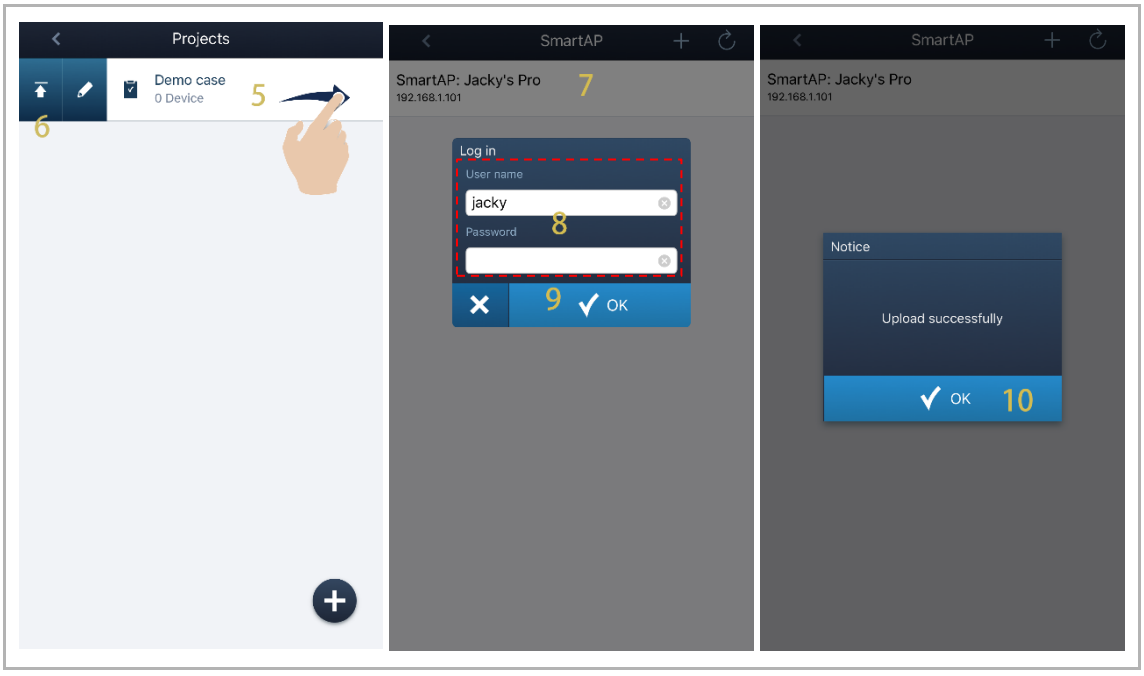
[6] Tap "  ".

[7] Tap a designated "Smart Access Point".

[8] Enter the account and password of "Smart Access Point".

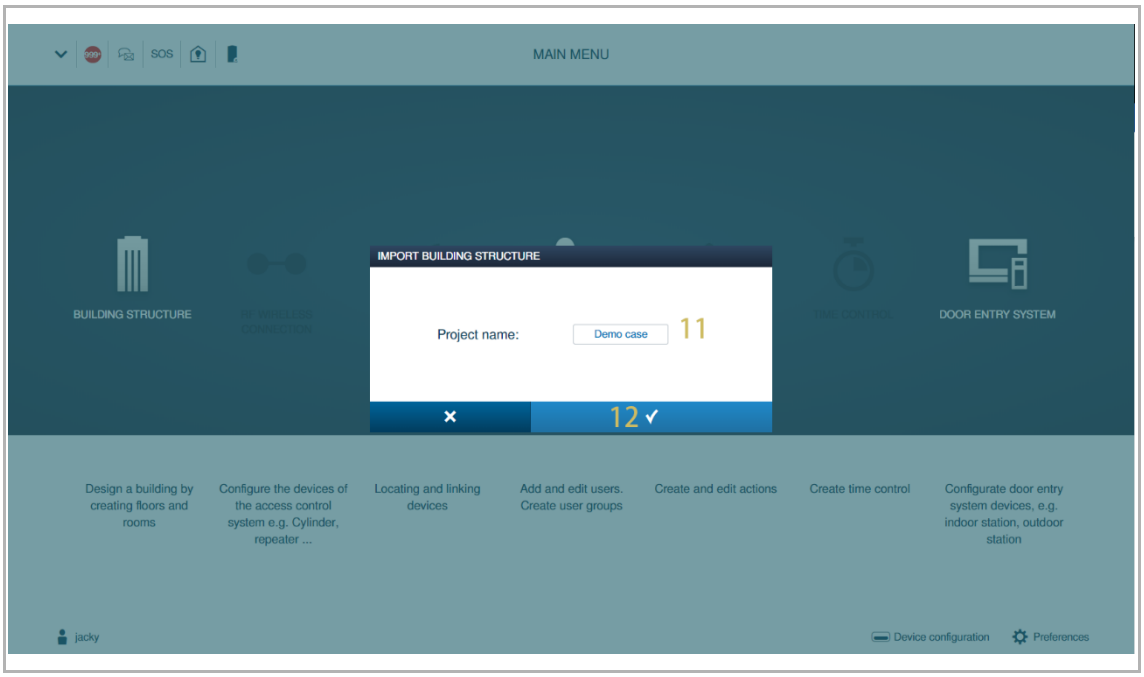
[9] Tap " √ " to continue.

[10] Tap " √ " to finish.

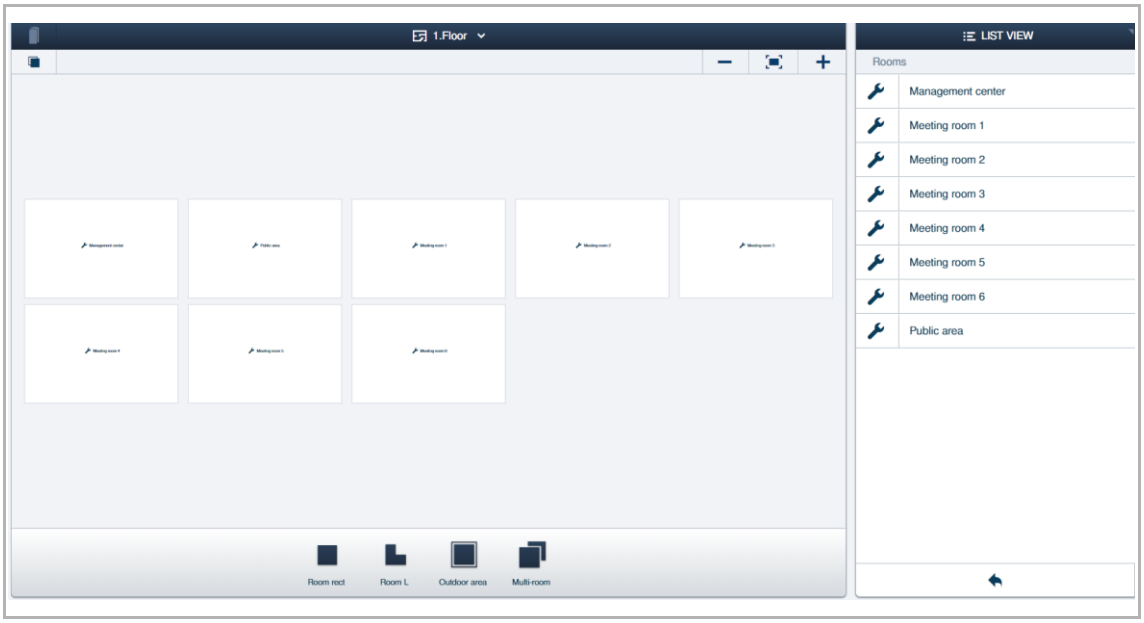


[11]Turn back to the configuration screen of "Smart Access Point", a pop-up window shows the importing status.

[12]Click " √ " to finish.



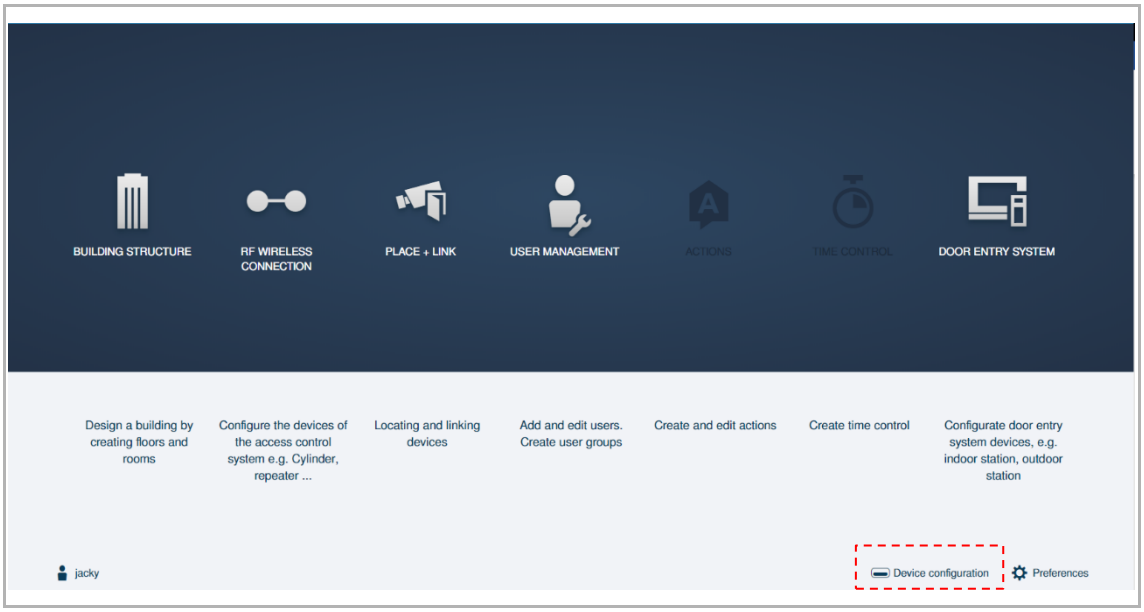
The building imported from Welcome App does not include the shape and location. You need to adjust it on "Smart Access Point". see chapter 10.2.1 “Creating a building via "Smart Access Point"“ on page 189.



10.3 Adding and locating the devices

Access the "Device configuration" screen

On the configuration screen, click "Device configuration" to access the corresponding screen.



10.3.1 Locating "Smart Access Point"

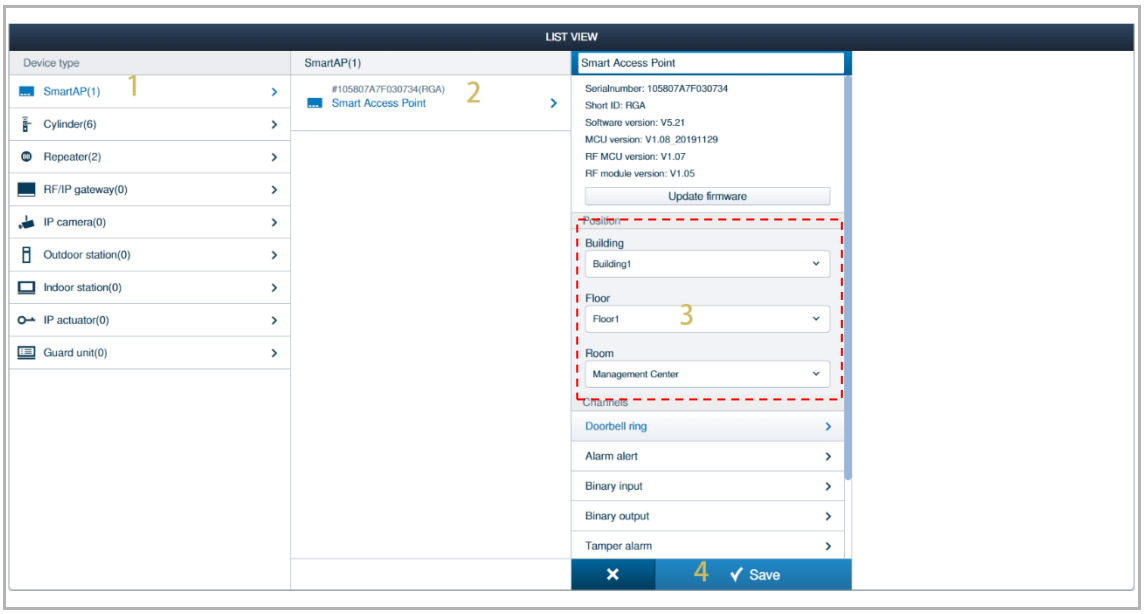
Please follow the steps below:

[1] On the "Device configuration" screen, click "SmartAP".

[2] Click "Smart Access Point".

[3] Set the position from the drop-down list (e.g. "Building 1>>Floor 1>> Public area" for demo case 1).

[4] Click " √ " to save.



10.3.2 Adding and locating "Electronic locking cylinders"

Please follow the steps below:

[1] On the "Device configuration" screen, click "Cylinder".

[2] Click "+".

[3] Click "Cylinder".

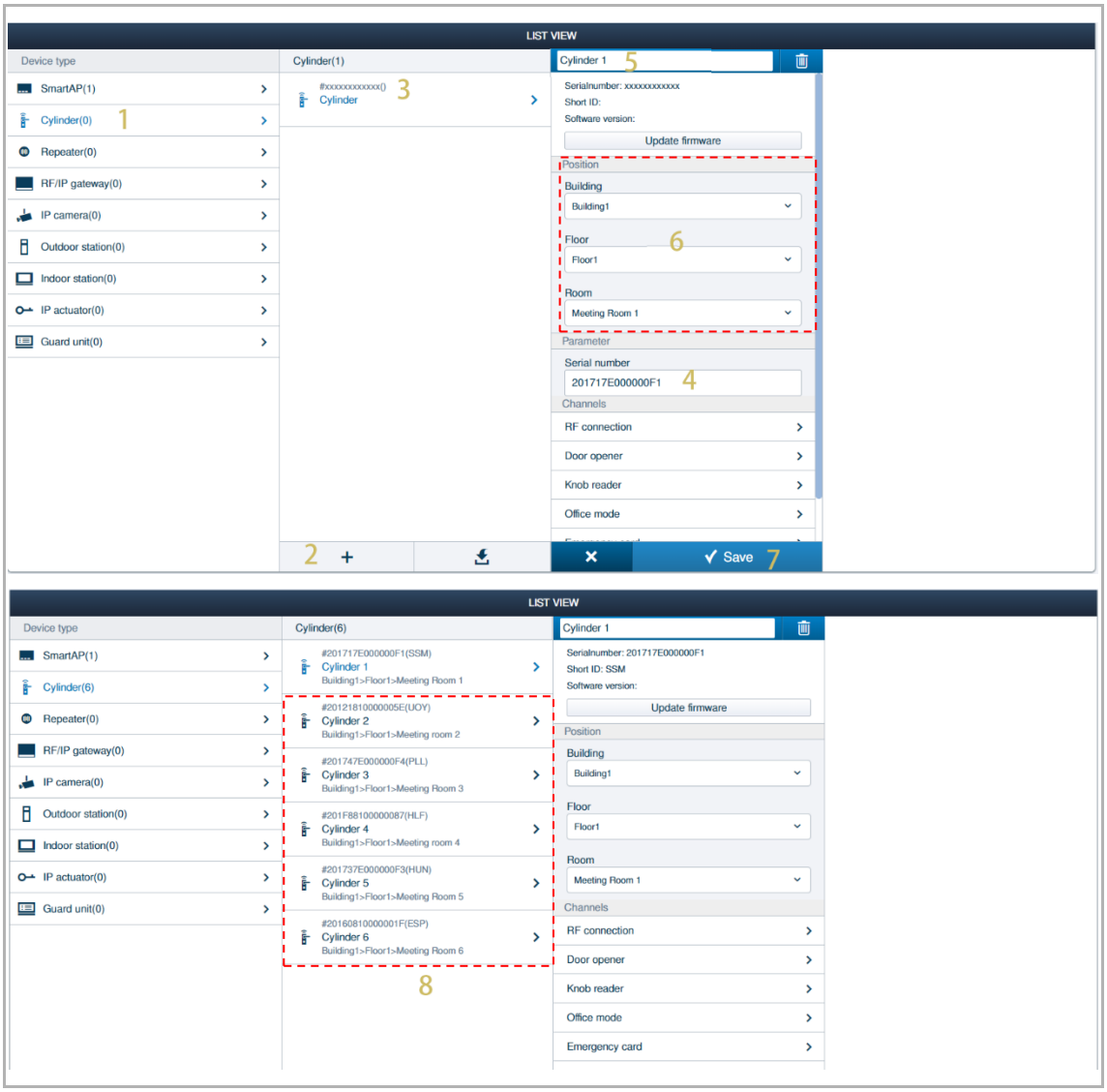
[4] Enter the serial number of the "Electronic locking cylinder".

[5] Change the name of the "Electronic locking cylinder".

[6] Set the position from the drop-down list (e.g. "Building 1>>Floor 1>> Meeting room 1" for demo case 1).

[7] Click " √ " to save.

[8] Repeat steps 2-7 to add the "Electronic locking cylinder" one by one. (e.g. "Cylinder 2~Cylinder 6" for demo case 1).



10.3.3 Adding and locating "RF Repeaters"

Please follow the steps below when you need to use "RF Repeaters".

[1] On the "Device configuration" screen, click "Repeater".

[2] Click "+".

[3] Click "Repeater".

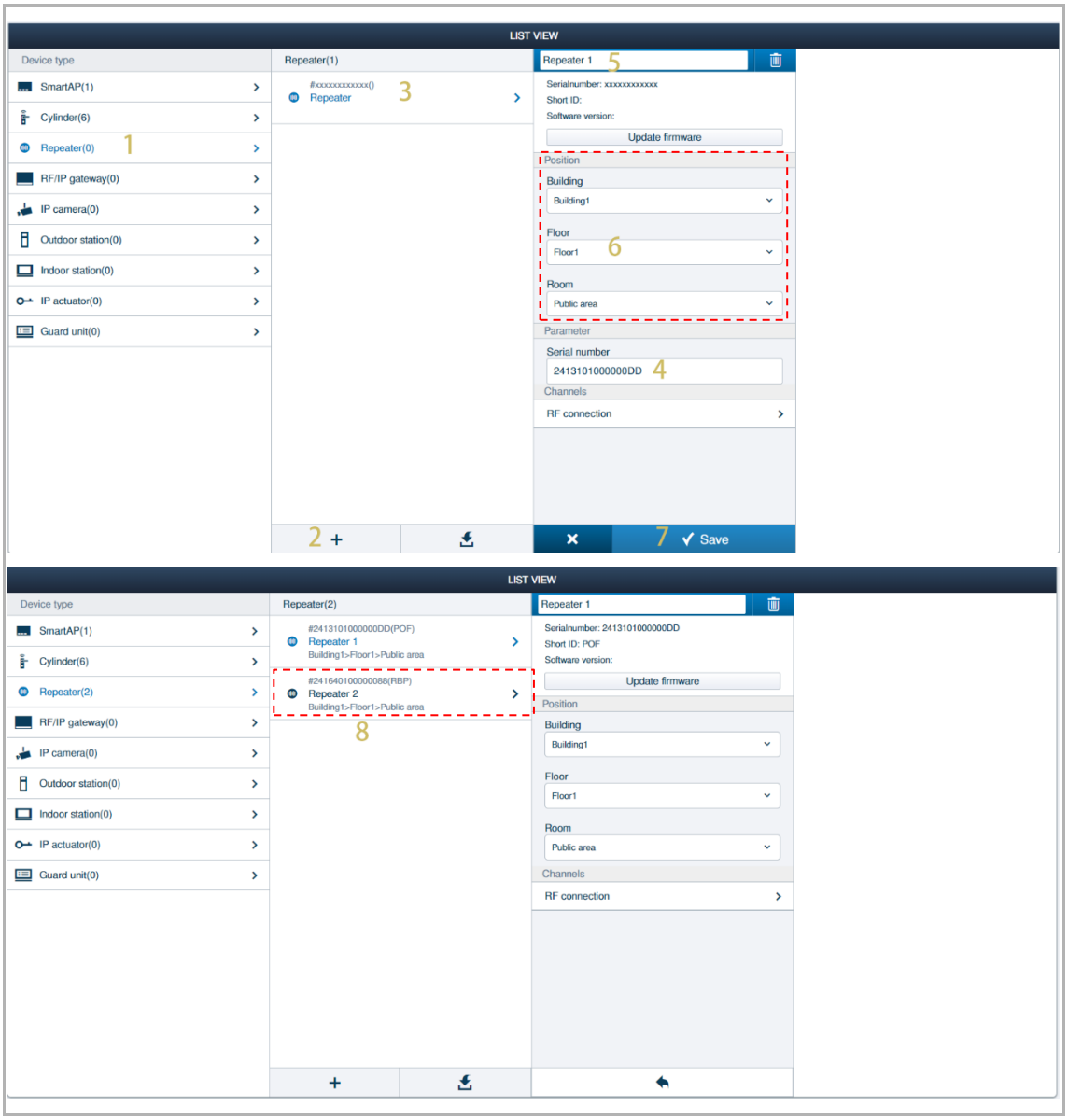
[4] Enter the serial number of the "RF Repeater".

[5] Change the name of the "RF Repeater".

[6] Set the position from the drop-down list (e.g. "Building 1>>Floor 1>> Public area" for demo case 1).

[7] Click " √ " to save.

[8] Repeat steps 2-7 to add the "RF Repeater". (e.g. "Repeater 2" for demo case 1).



10.3.4 Adding and locating "RF/IP Gateways"

Please follow the steps below when you need to use "RF/IP Gateways".

[1] On the "Device configuration" screen, click "RF/IP Gateway".

[2] Click " ".

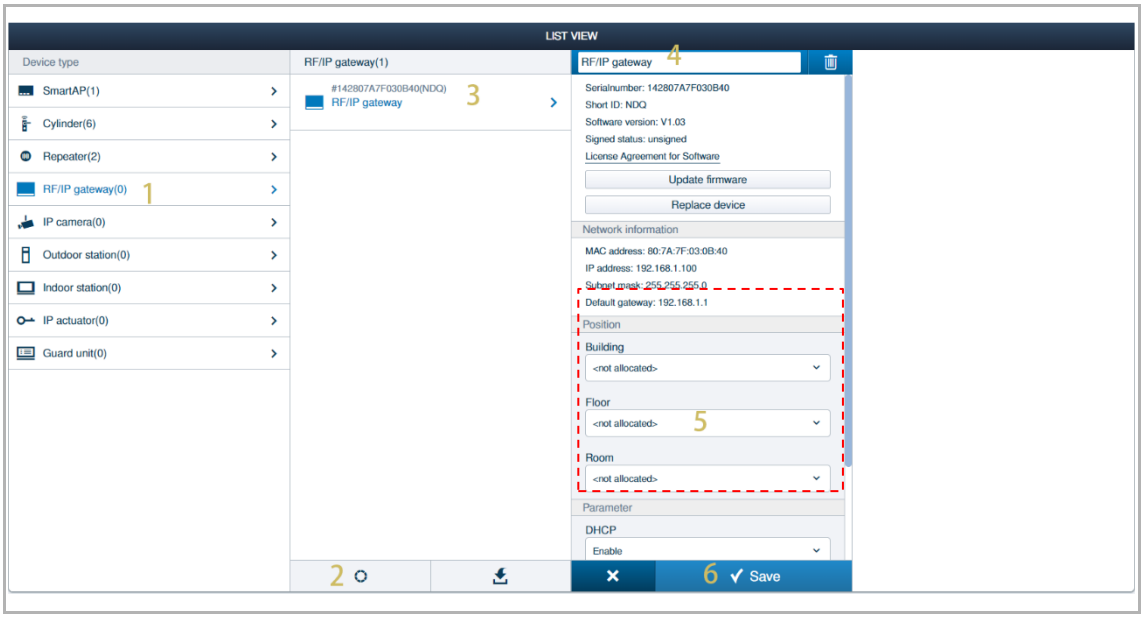
[3] Click "RF/IP Gateway".

[4] Change the name of the "Electronic locking cylinder".

[5] Set the position from the drop-down list.

[6] Click " √ " to save.

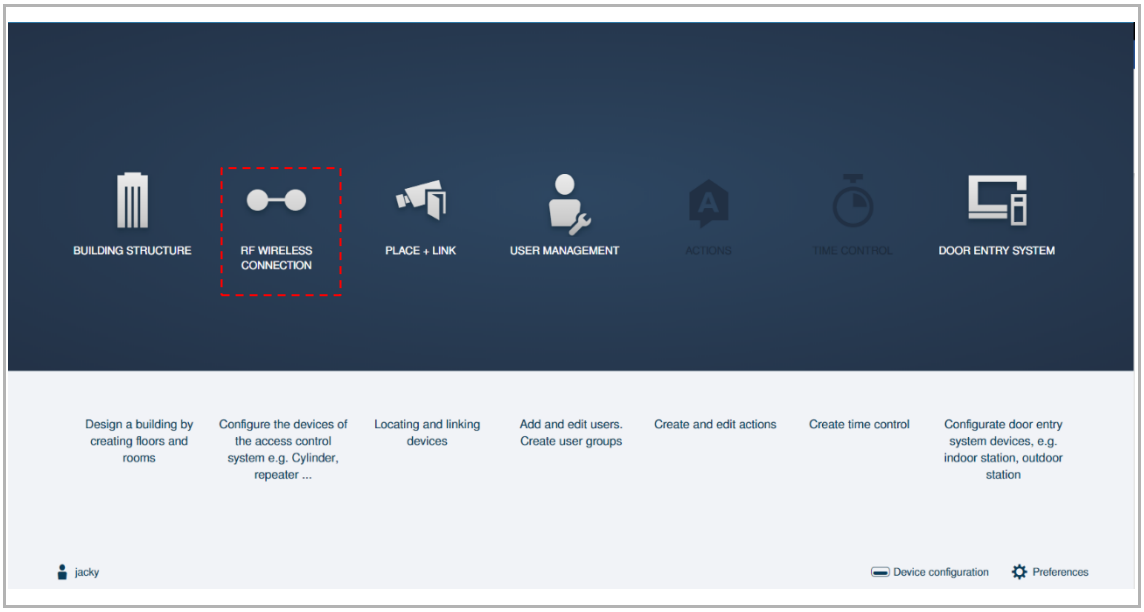
Repeat steps 2-7 to add the "RF/IP Gateways" one by one.



10.4 Connecting the devices

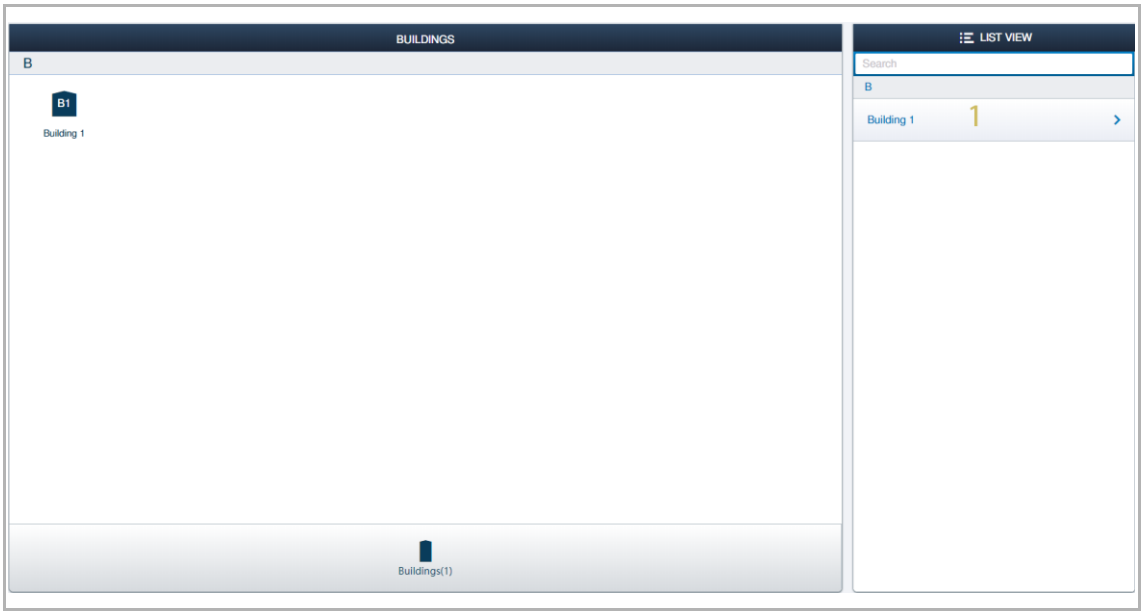
Access the RF connecting screen

On the configuration screen, click "RF Wireless connection" to access the corresponding screen.

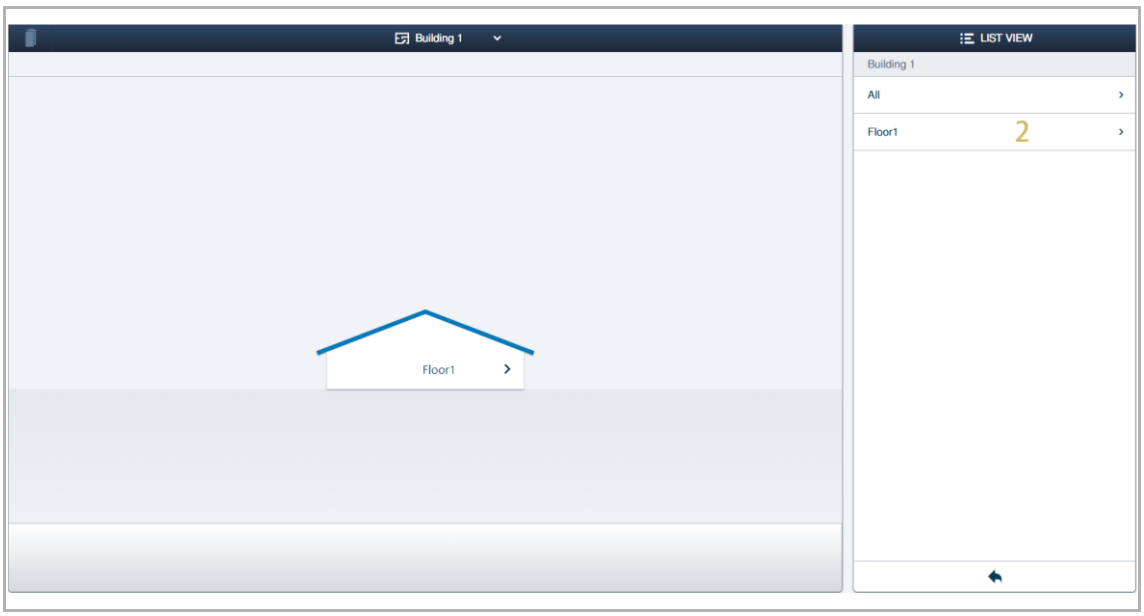


Please follow the steps below:

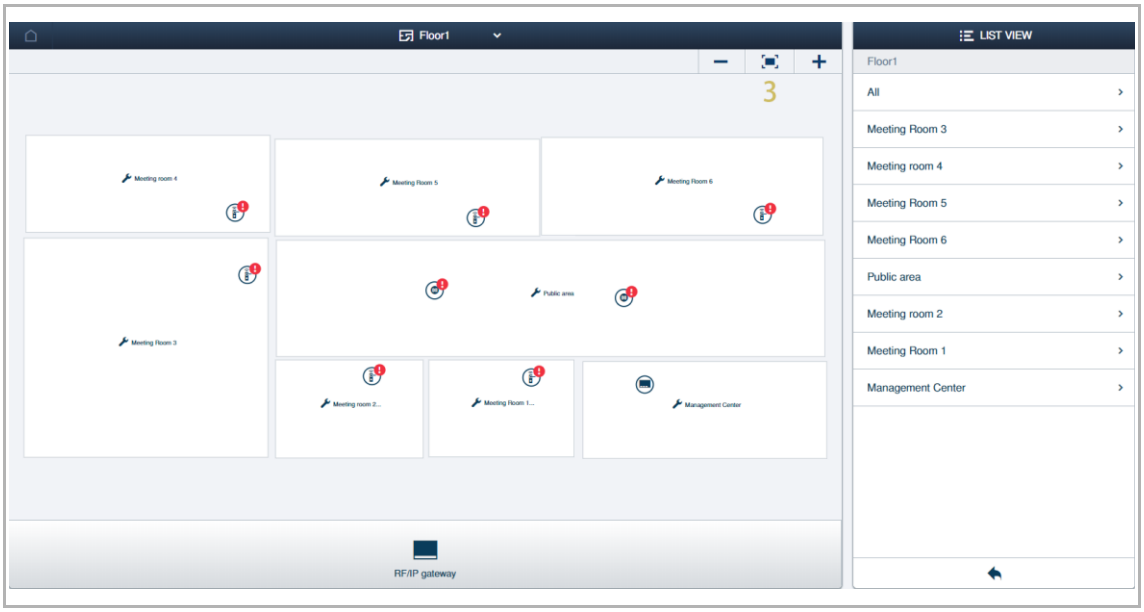
[1] On the "Buildings" screen, click the designated building (e.g. "Building 1" for demo case 1).



[2] Click the designated floor (e.g. "Floor 1" for demo case 1).



[3] Click " " to view all the devices on the floor screen, you can move the icons to a suitable postion by dragging them.



Connecting the AccessControl devices in a sequence

Please connect the AccessControl devices in a radio line according to the following sequence:

[1] Connect "Smart Access Point" or "RF/IP Gateways" to its slave devices.

[2] Connect the "RF Repeaters" to its slave devices.

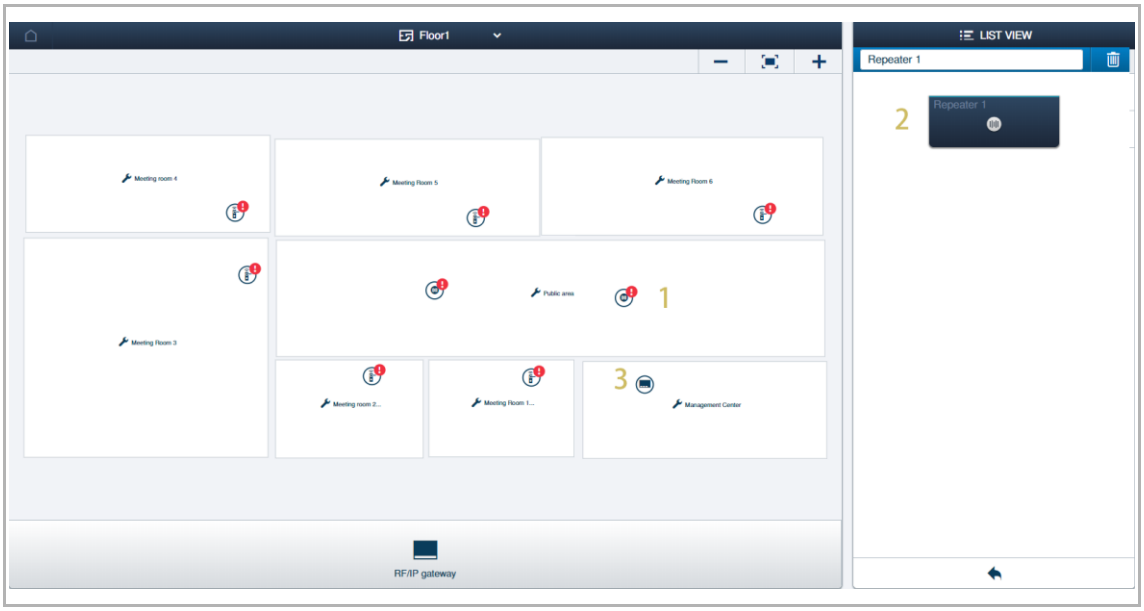
10.4.1 Connecting "RF Repeaters"

Please follow the steps below:

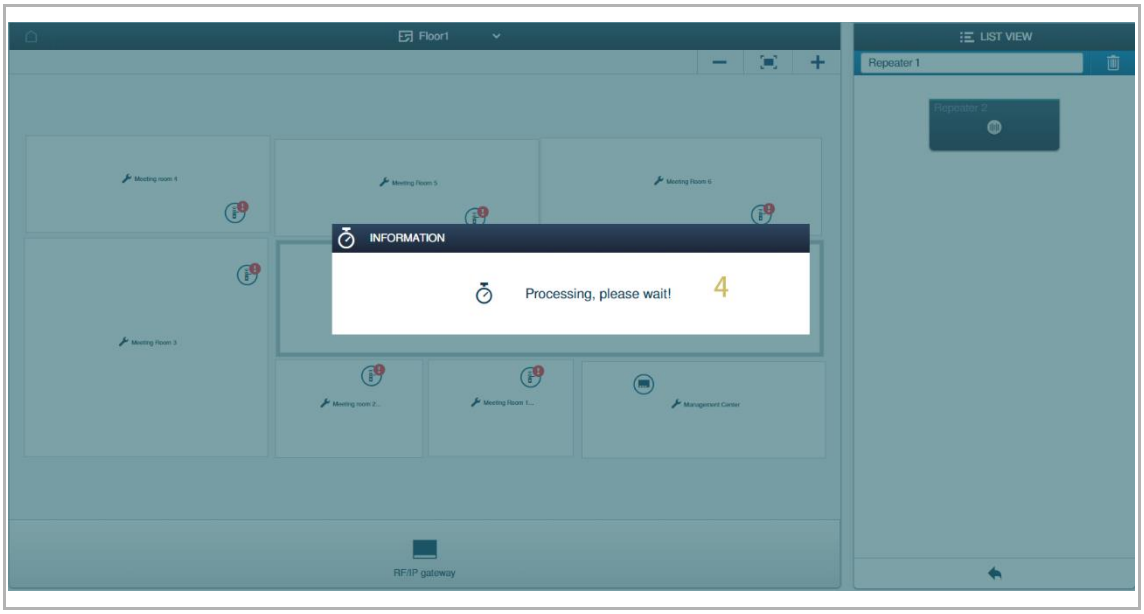
[1] On the floor screen, click a "RF Repeater" (e.g. "Repeater 1" for demo case 1).

[2] Currently no parent device is displayed in the list.

[3] Click its parent device on the floor plan (e.g. "Smart Access Point" for demo case 1).



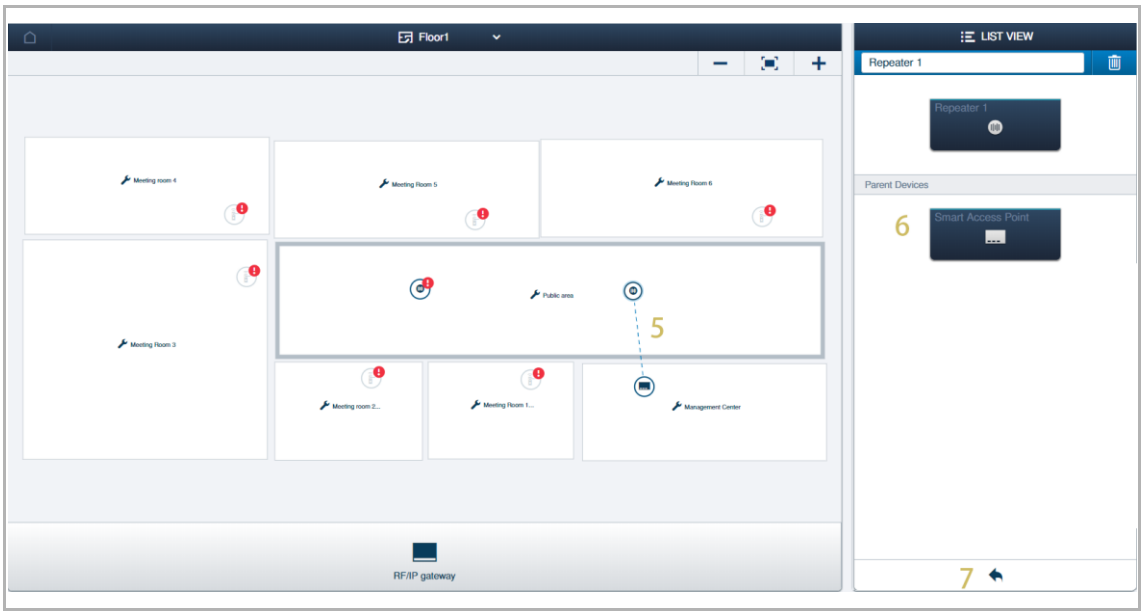
[4] Wait for the pairing process



[5] Coupling between the two devices is indicated by a dashed line if successful.

[6] Parent device is displayed on the list.

[7] Click " " to turn back to the floor screen.



Note

"RF Repeater" must unpair itself with its exist parent device before it is paired with a new device. see chapter 10.11.2 “Disconnecting "RF Repeaters"“ on page 265.

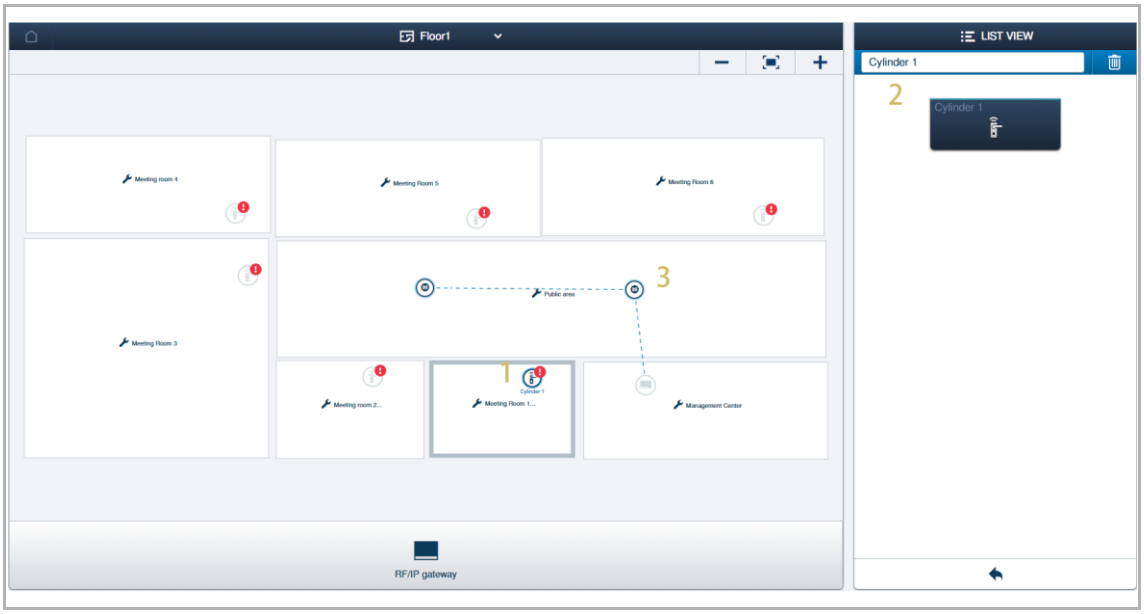
10.4.2 Connecting "Electronic locking cylinders"

Please follow the steps below:

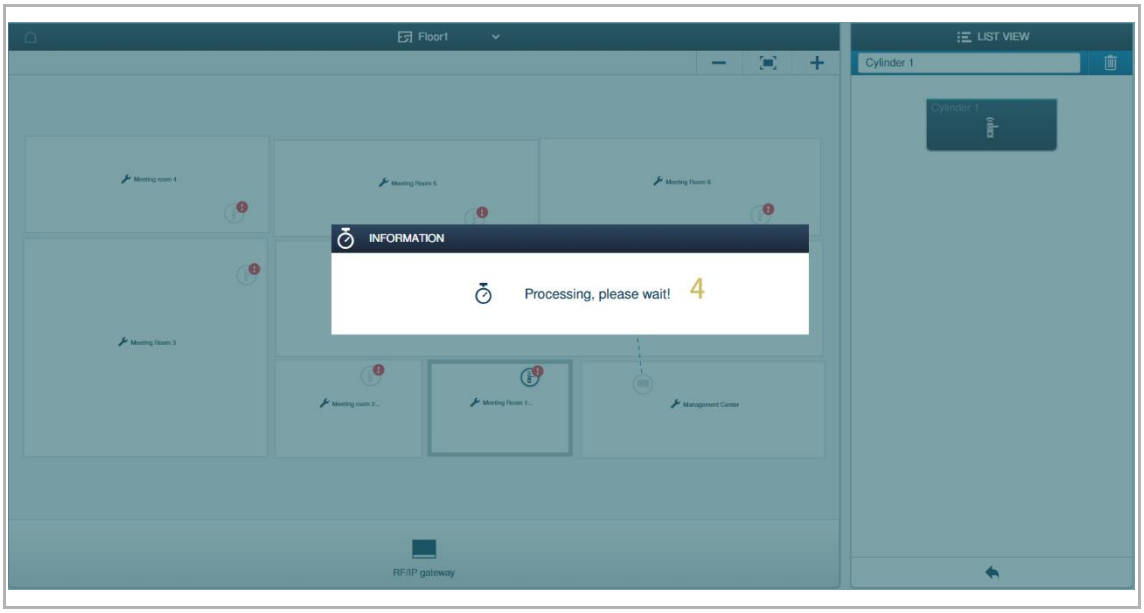
[1] On the floor screen, click an "Electronic locking cylinder" (e.g. "Cylinder 1" for demo case 1).

[2] Currently no parent device is displayed in the list.

[3] Click its parent device (e.g. "Repeater 1" for demo case 1).

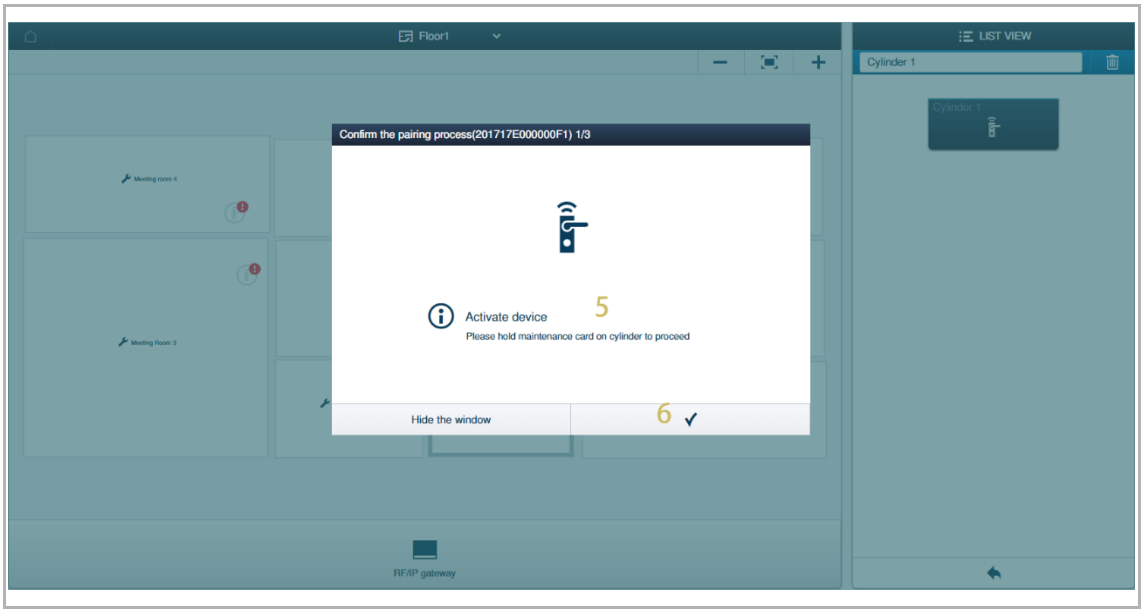


[4] Wait for the pairing process.

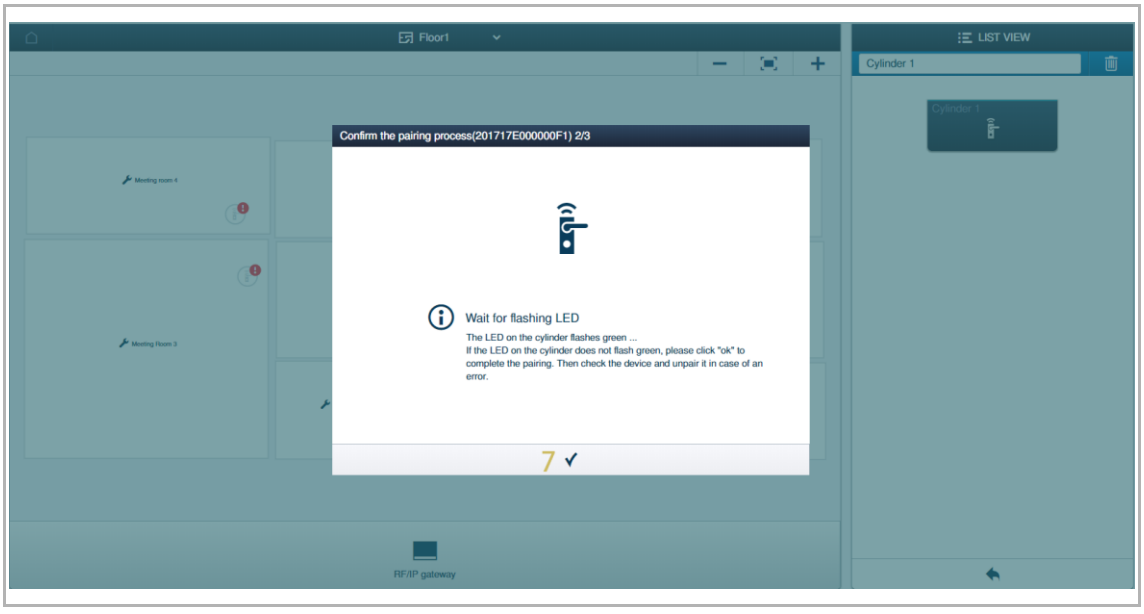


[5] Hold the maintenance card on the slave "Electronic locking cylinders".

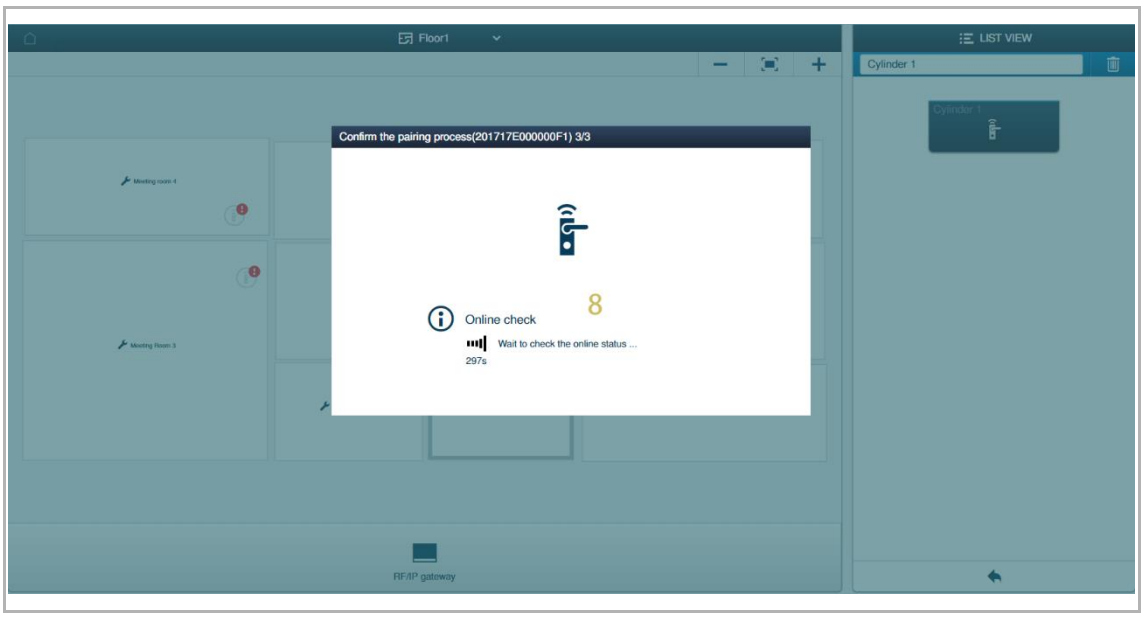
[6] Click " √ " to continue.



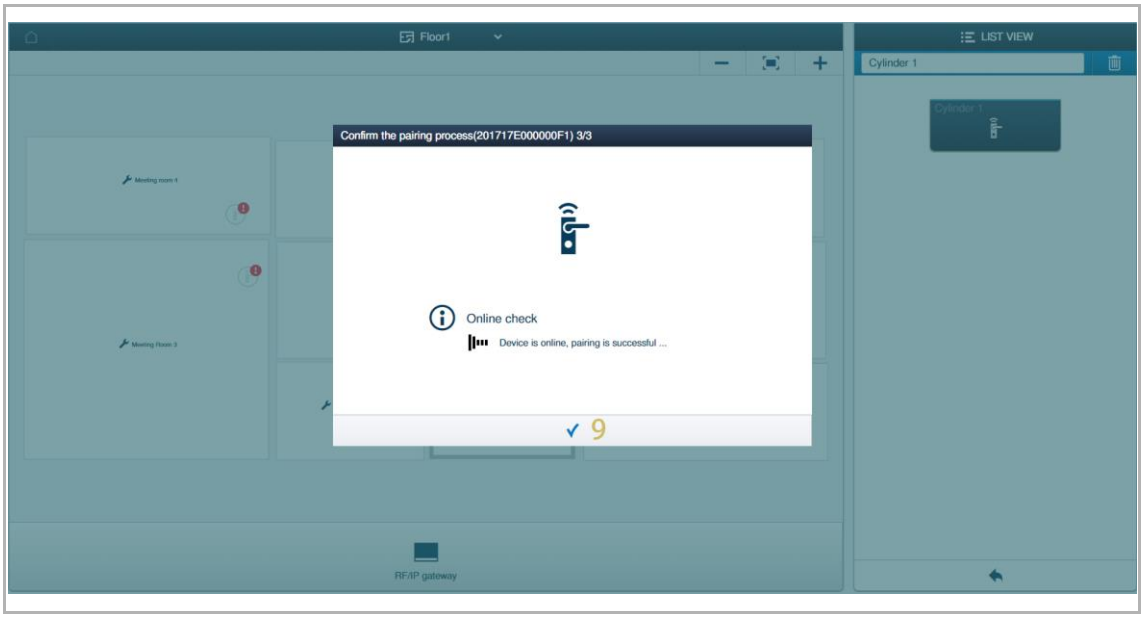
[7] If the LED on the "Electronic locking cylinder" flashes green or the "Electronic locking cylinder" sounds a beep, click " √ " to continue.



[8] Wait for the online check.



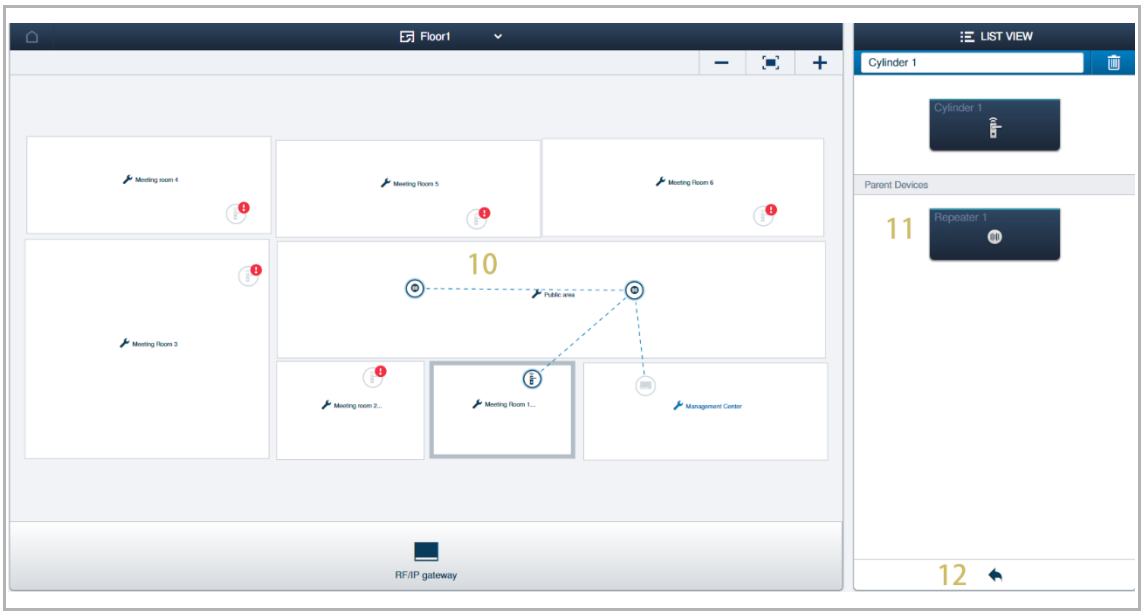
[9] If the "Electronic locking cylinder" is online, click " √ " to continue. Otherwise you need to wait 300 s before doing the next step.



[10]Pair between the two devices is indicated by a dashed line if successful.

[11]Parent device is displayed on the list.

[12]Click " " to turn back to the floor screen.



Note

"Electronic locking cylinder" must unpair itself from its existing parent device before it is paired with a new device. Page 261.

10.4.3 AccessControl device is offline

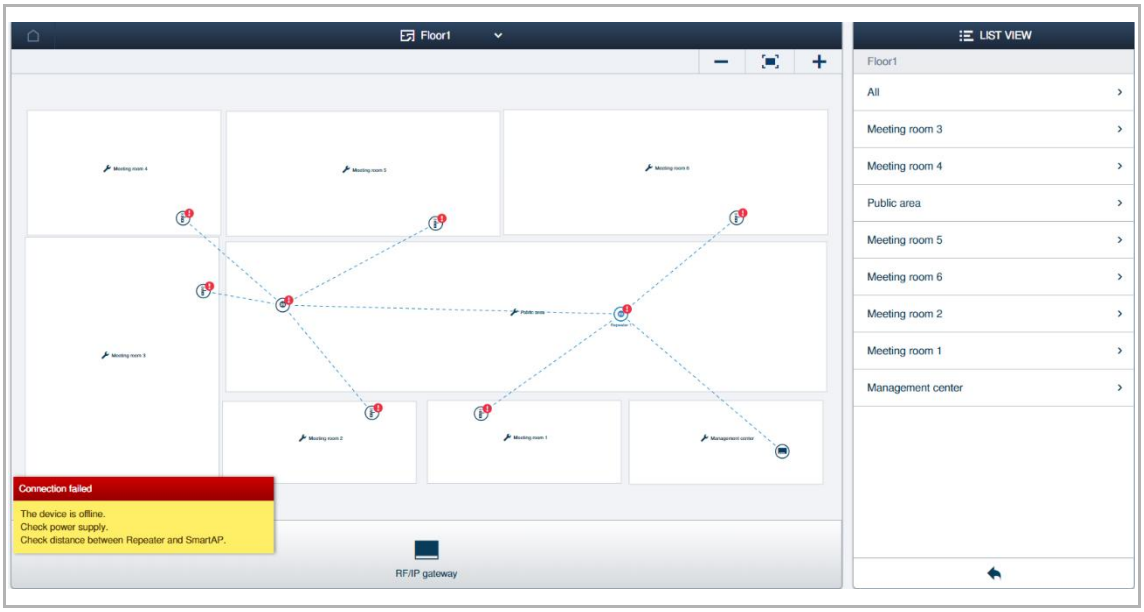
Displaying an offline icon when AC devices are offline

An offline icon " " will be displayed on the AccessControl device if it is offline.

1. "RF Repeater" is offline

When you find " " on a "RF Repeater", please carry out the following operations:

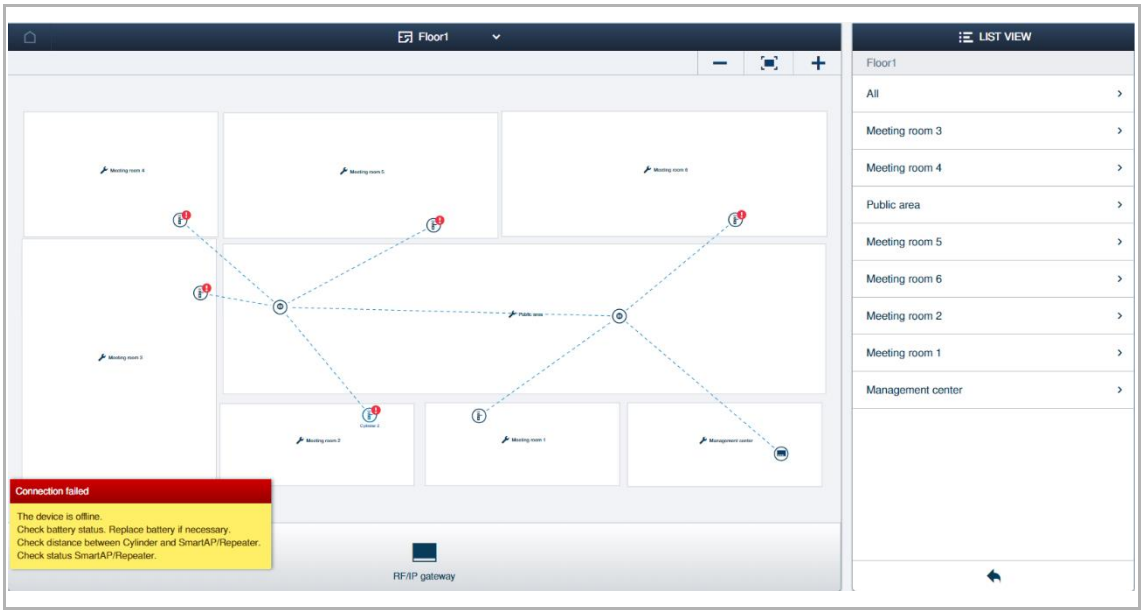
- Check if the "RF Repeater" is powered on.
- Check if its parent "RF Repeater" is powered on.
- Check if the distance between the "RF Repeater" and its parent device exceeds 10 metres.



2. "Electronic lock cylinder" is offline

When you find " " on an "Electronic lock cylinder", please carry out the following operations:

- Check if the battery of the "Electronic lock cylinder" is empty. Page 222.
- Check if its parent device "RF Repeater" is offline.
- Check if the distance between the "Electronic lock cylinder" and its parent device exceeds 10 metres.



Note

In some cases, you can hold the maintenance card against the designated "Electronic lock cylinder" to activate it.

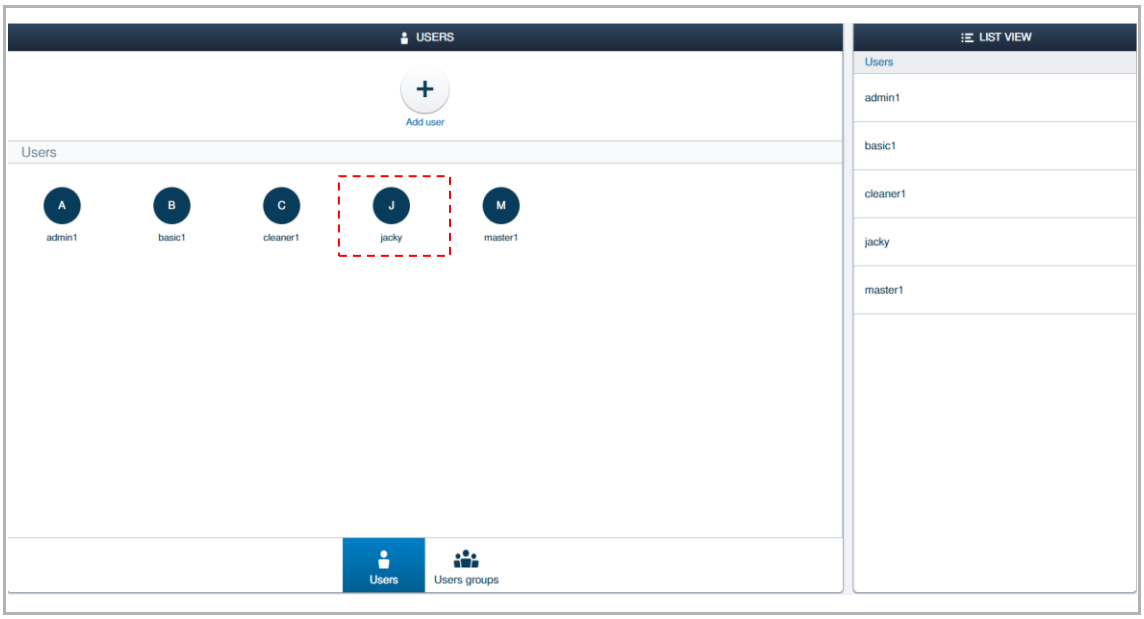
10.5 Assigning permissions

10.5.1 Assigning permissions to a user

You can assign permissions to a user by assigning both the ID authentications and the "Electronic locking cylinder" to the user.

Access the designated user screen

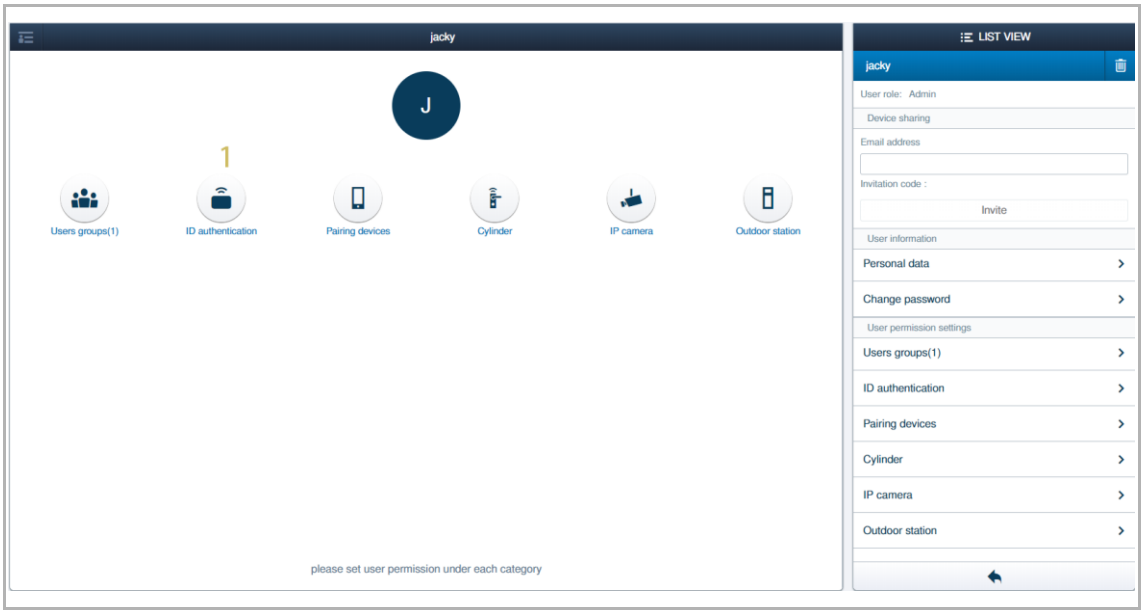
On the "Users" screen, click the designated user to access the designated user screen.



1. Assigning the ID authentications to a user

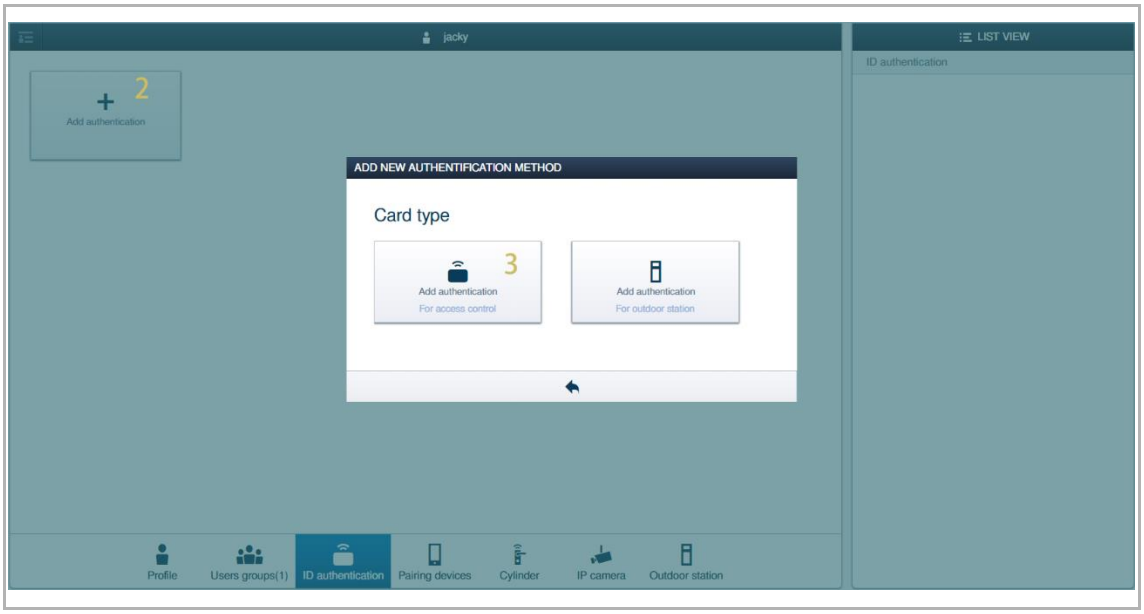
Please follow the steps below:

[1] On the designated user screen, click "ID authentication".



[2] Click "Add authentication".

[3] Click "Add authentication for access control".



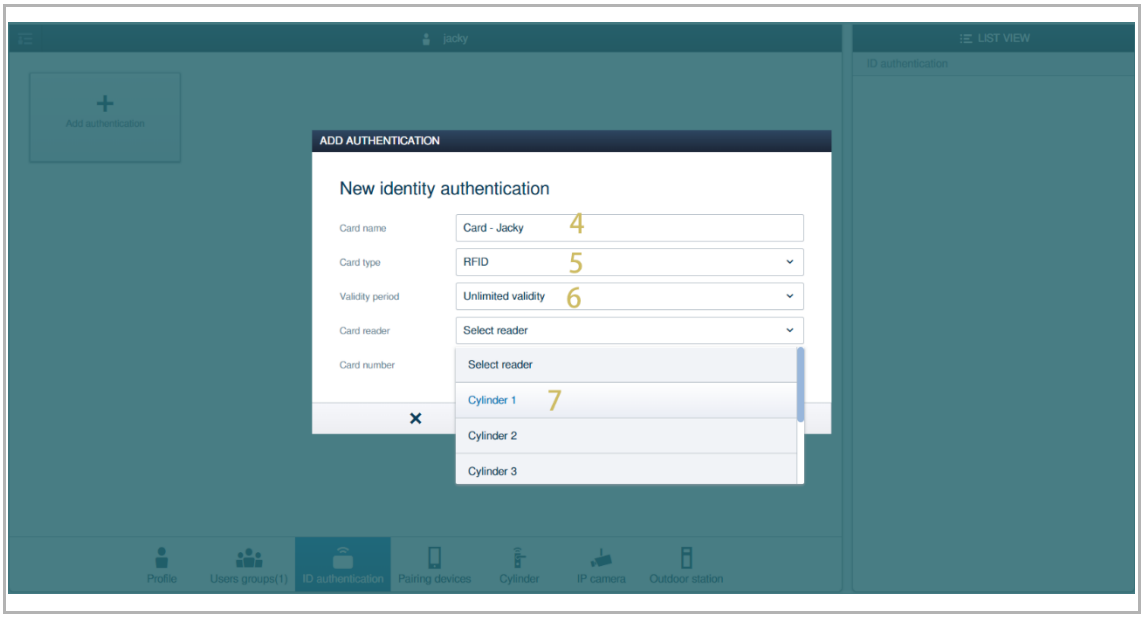
[4] Enter the card name.

[5] Set card type to "RFID".

[6] Set validity period, there are 2 options:

- Unlimited validity, it this type is selected, you can continue to the next step.
- Limited validity, if this type is selected, you need to set the start date and end date by clicking " 31 ".

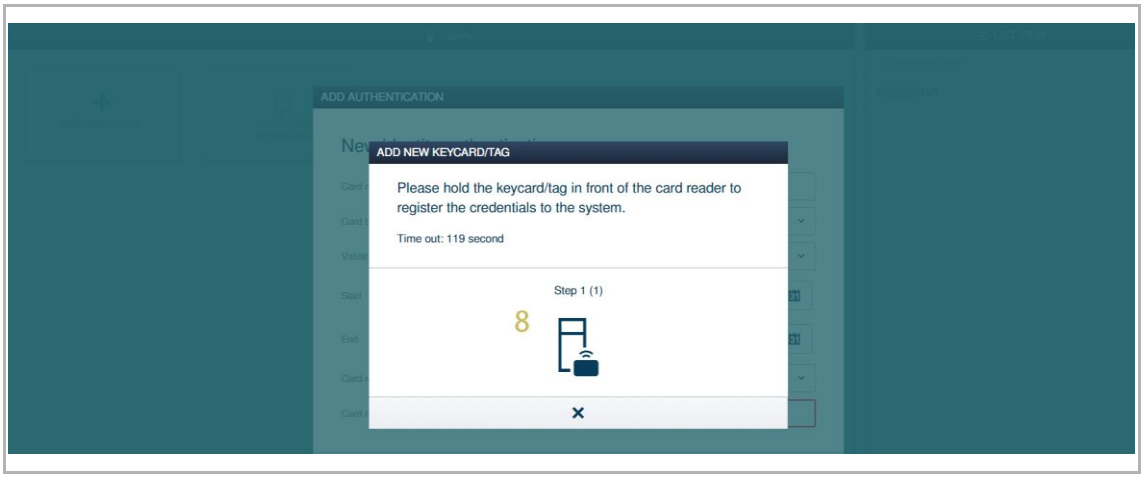
[7] Select any "Electronic locking cylinder" from the drop-down list for swiping the ID authentications.



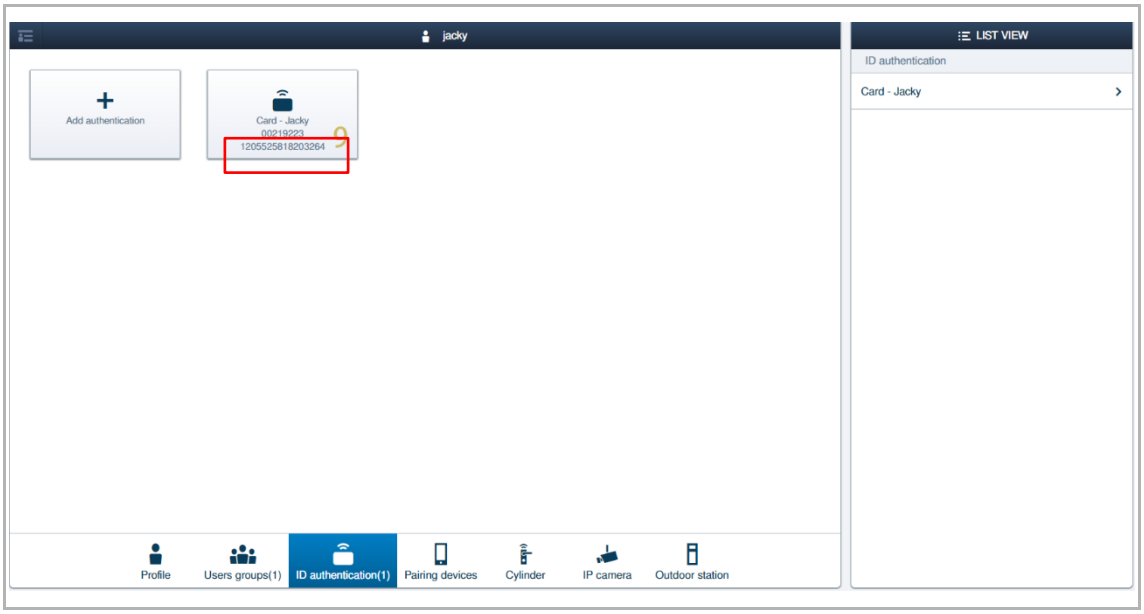
Note

"Electronic locking cylinder" needs to be paired in a radio line before swiping the ID authentications. see chapter 10.4.2 “Connecting "Electronic locking cylinders"“ on page 207.

[8] Hold the keycard or tag in front of the "Electronic locking cylinder". The LED of the "Electronic locking cylinder" will flash green or sound a beep if successful.



[9] The card number is displayed on the screen.



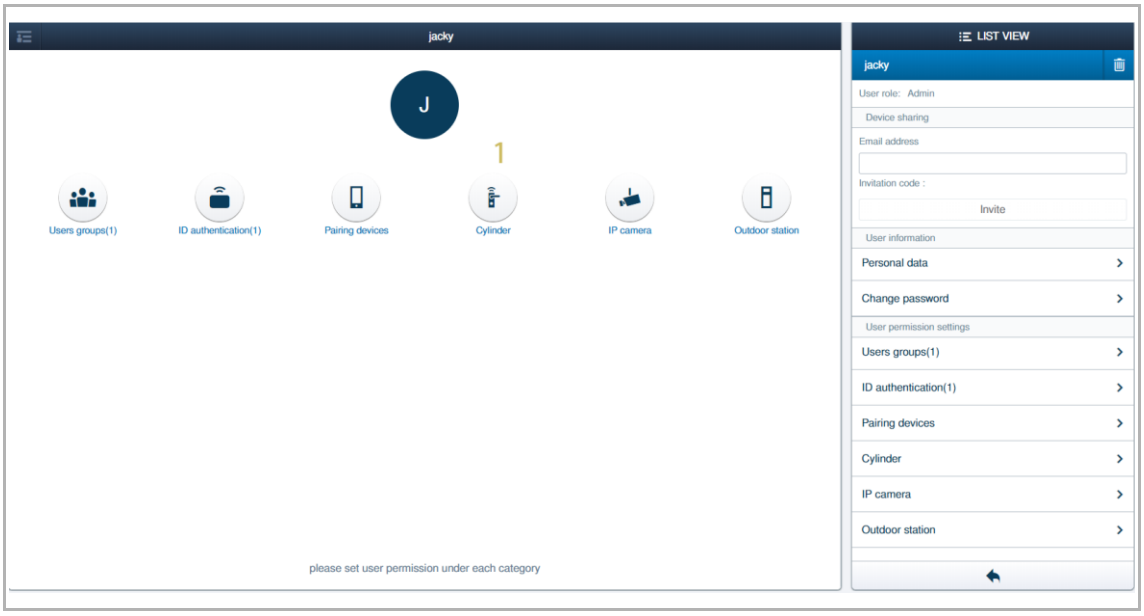
Repeat steps from 2-9 to assign the ID authentications one by one.

Note
Up to 200 ID authentications can be assigned to a user.

2. Assigning the "Electronic locking cylinder" to a user.

Please follow the steps below:

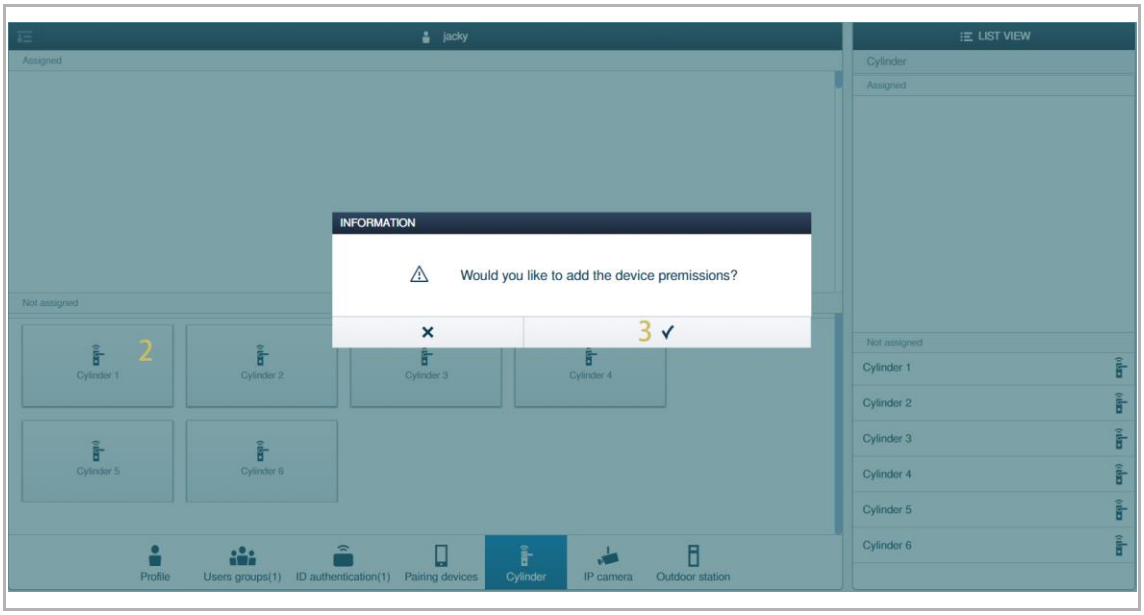
[1] On the designated user screen, click "Cylinder".



[2] Click the designated "Electronic locking cylinder" on the "Not assigned" section.

[3] Click " √ " to confirm.

Repeat steps from 2-3 to assign the "Electronic locking cylinders" one by one.



10.5.2 Assigning the permission to users

You can assign the permission for multiple users by assigning the permission to the user group.

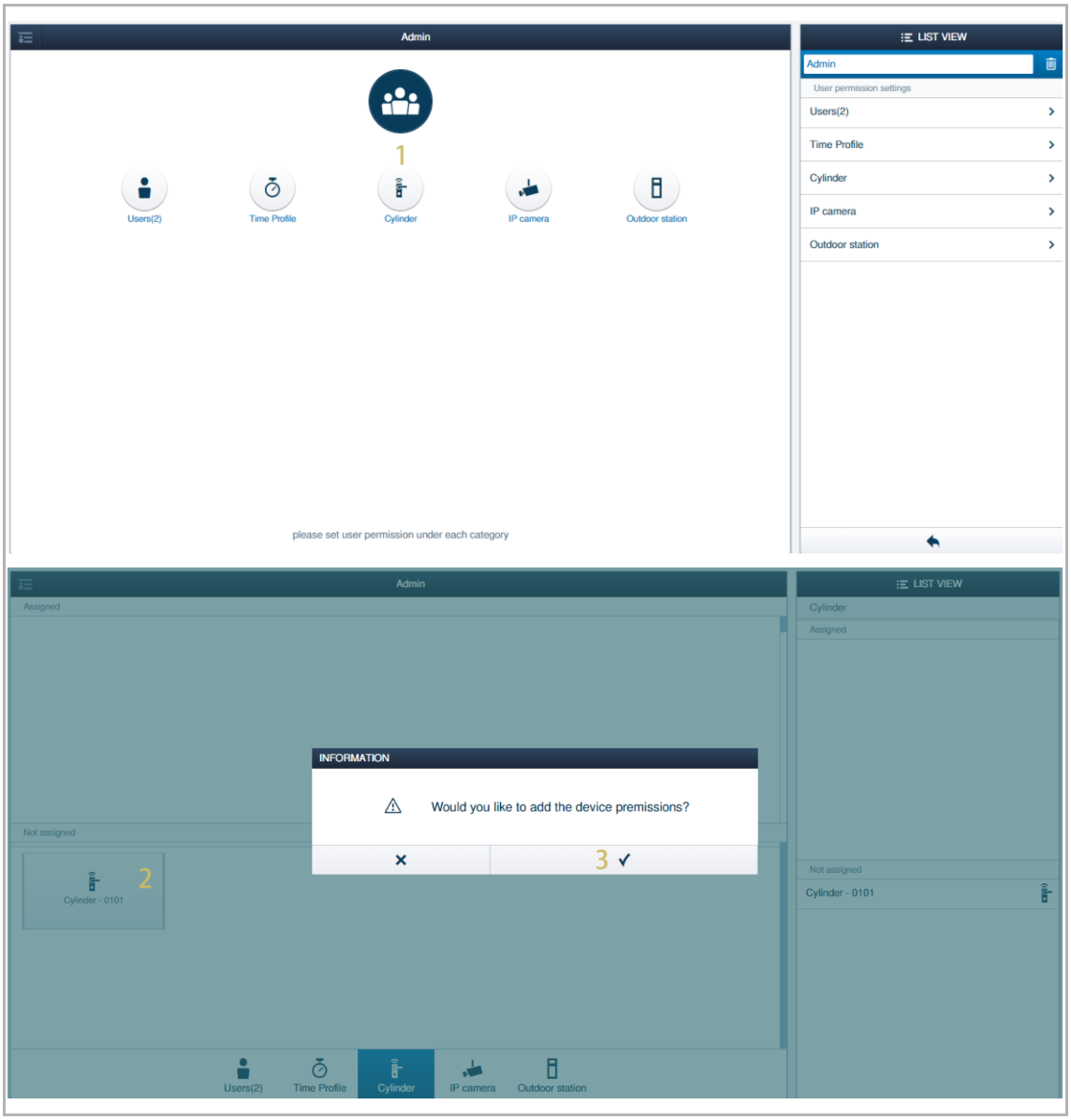
Please follow the steps below:

[1] On the designated user group screen, click "Cylinder".

[2] Click the designated "Electronic locking cylinder" on the "Not assigned" section.

[3] Click " √ " to confirm.

Repeat steps from 2-3 to assign the "Electronic locking cylinder" one by one.



10.5.3 Setting the offline day

In some cases, "Electronic locking cylinder" will be offline. see chapter 10.4.3 “AccessControl device is offline“ on page 211.

In this case, only emergency cards and the cards that meet the offline day can be used.

Note

It is recommended to set the offline day or emergency cards before use.

Offline day

When an "Electronic locking cylinder" is offline, only the ID authentications within the offline days can be used.

For example, if the offline day is set to "5", only the ID authentications used within 5 days can be used. The ID authentications used 6 days ago can no longer be used.

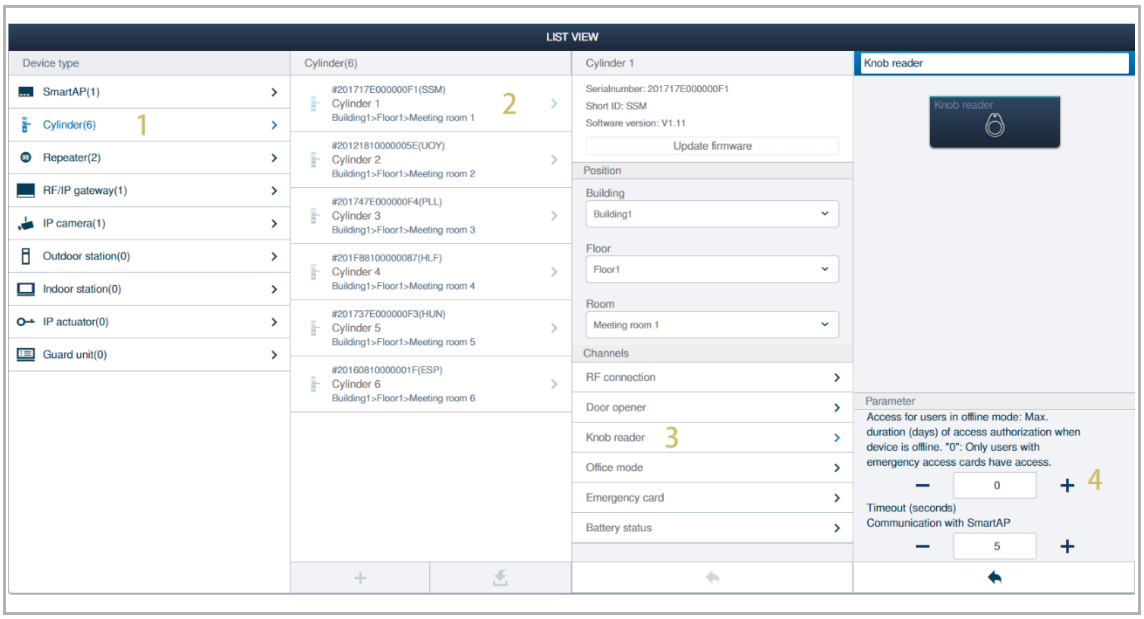
Please follow the steps below:

[1] On the configuration screen, click "Device configuration", click "Cylinder".

[2] Click the designated "Electronic locking cylinder".

[3] Click "Knob reader".

[4] Enter the number for the offline day. If the offline day is set to "0", only emergency cards can be used. see chapter 10.5.4 “Managing the emergency cards“ on page 220.



10.5.4 Managing the emergency cards

Emergency cards can be used when the "Electronic locking cylinder" is offline.

1. Adding the emergency cards

Please follow the steps below:

[1] On the configuration screen, click "Device configuration", click "Cylinder".

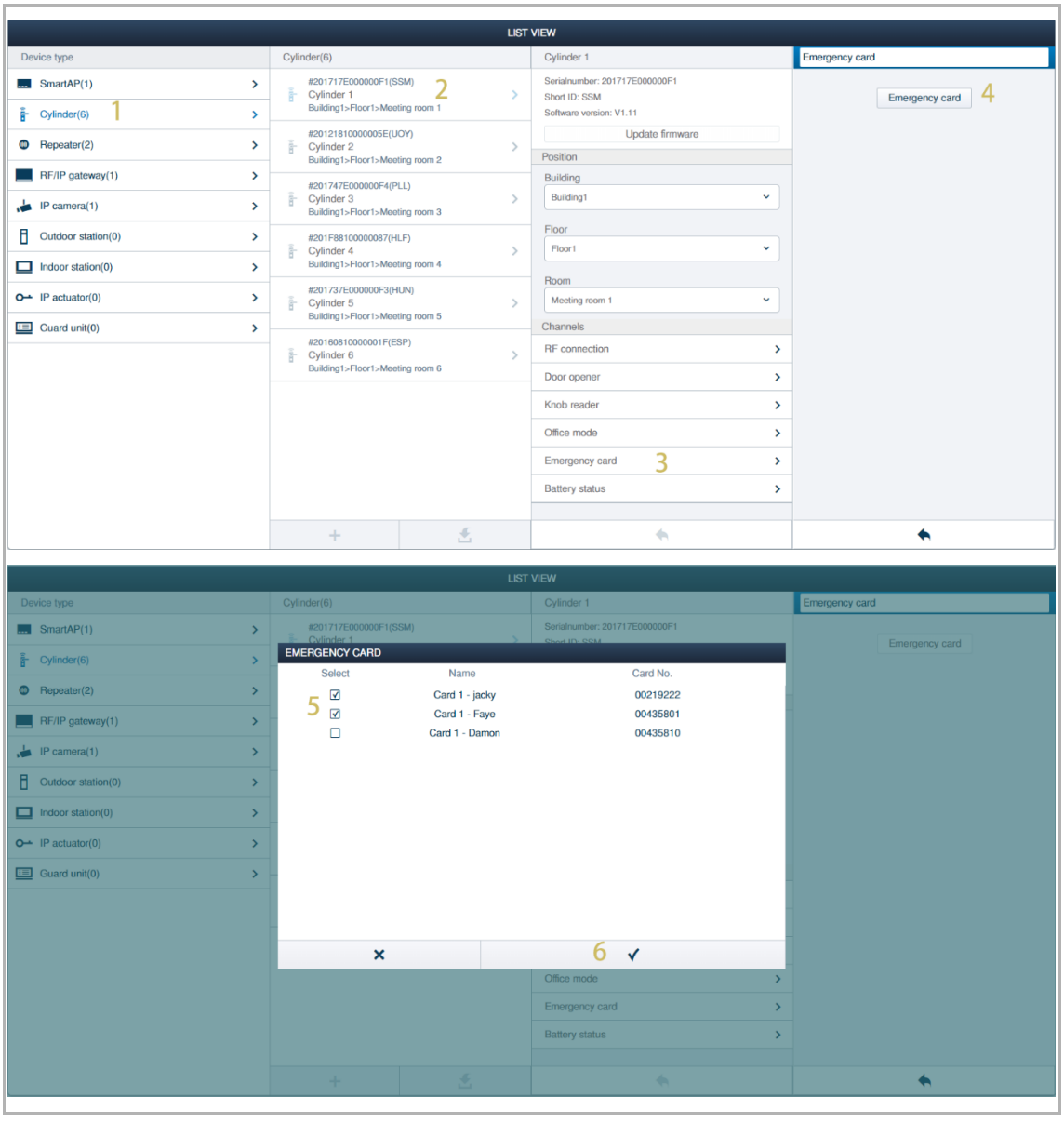
[2] Click the designated "Electronic locking cylinder".

[3] Click "Emergency card".

[4] Click "Emergency card".

[5] Tick the check box to add the emergency cards.

[6] Click " √ " to confirm.



2. Removing the emergency cards

Please follow the steps below:

[1] On the configuration screen, click "Device configuration", click "Cylinder".

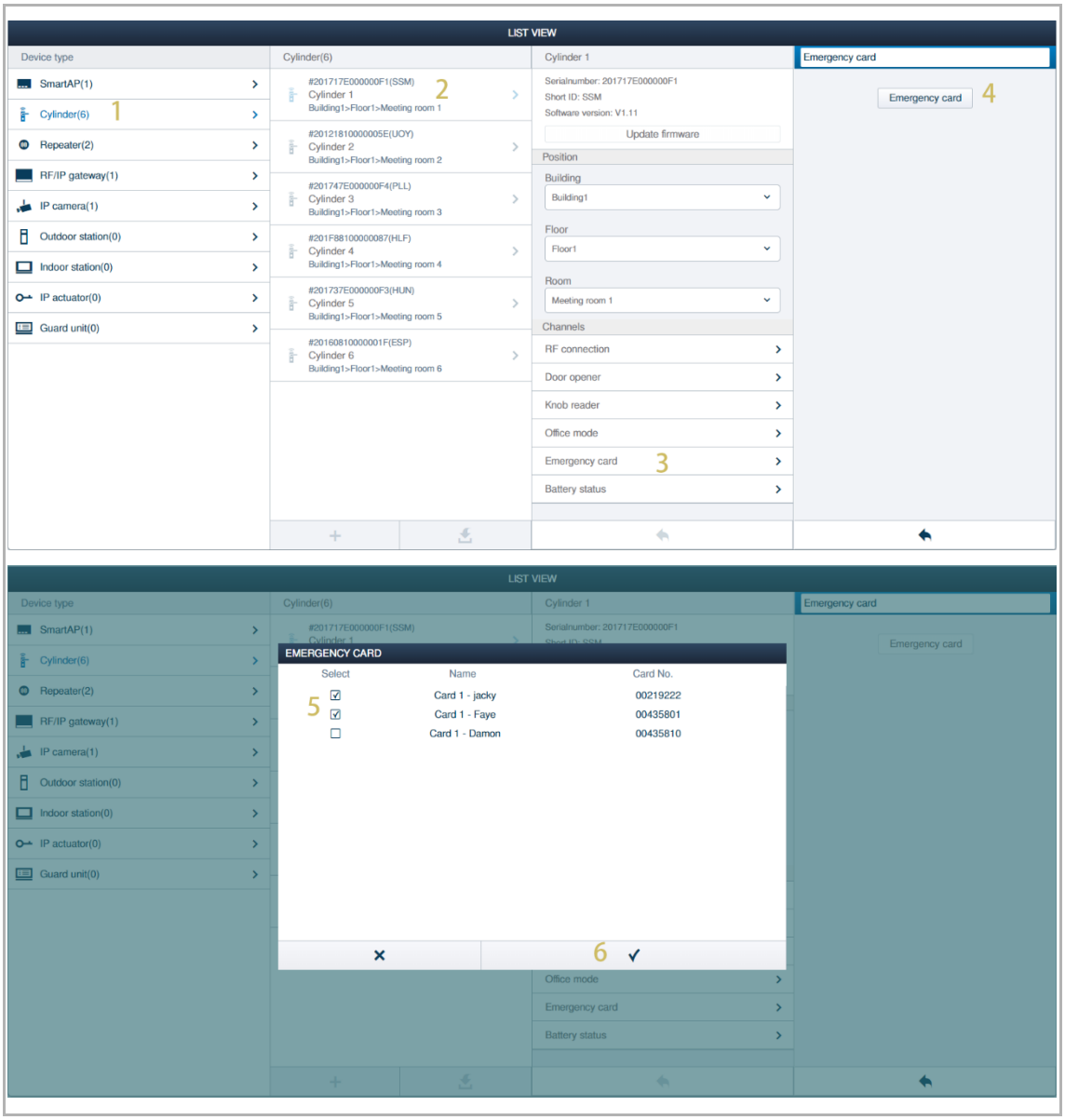
[2] Click the designated "Electronic locking cylinder".

[3] Click "Emergency card".

[4] Click "Emergency card".

[5] Untick the check box to remove the emergency cards.

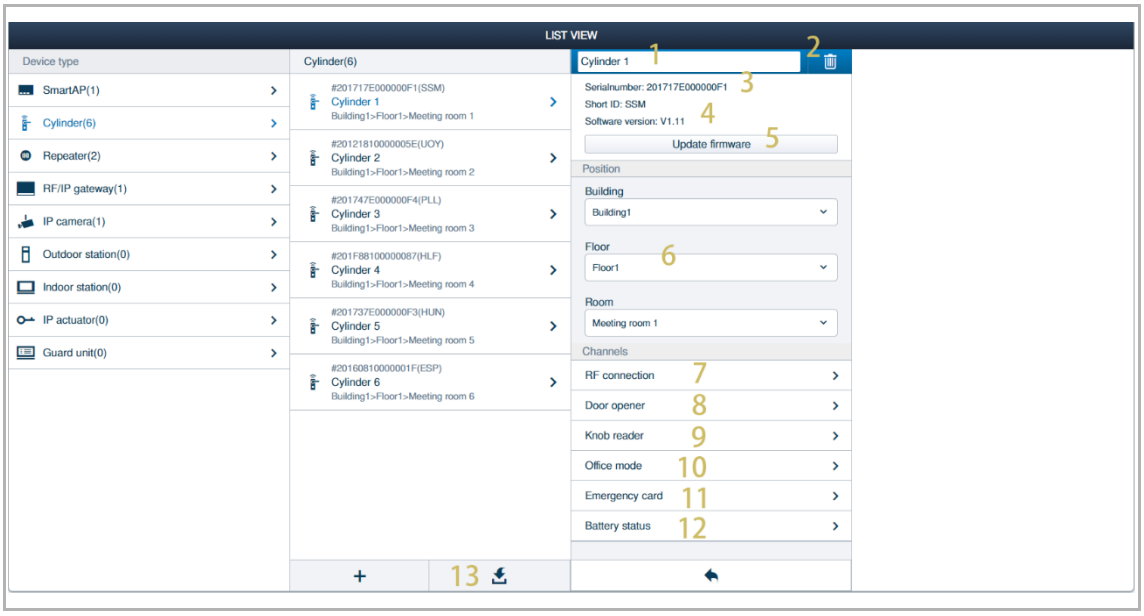
[6] Click " √ " to confirm.



10.6 Configuring the devices

10.6.1 Configuring "Electronic locking cylinders"

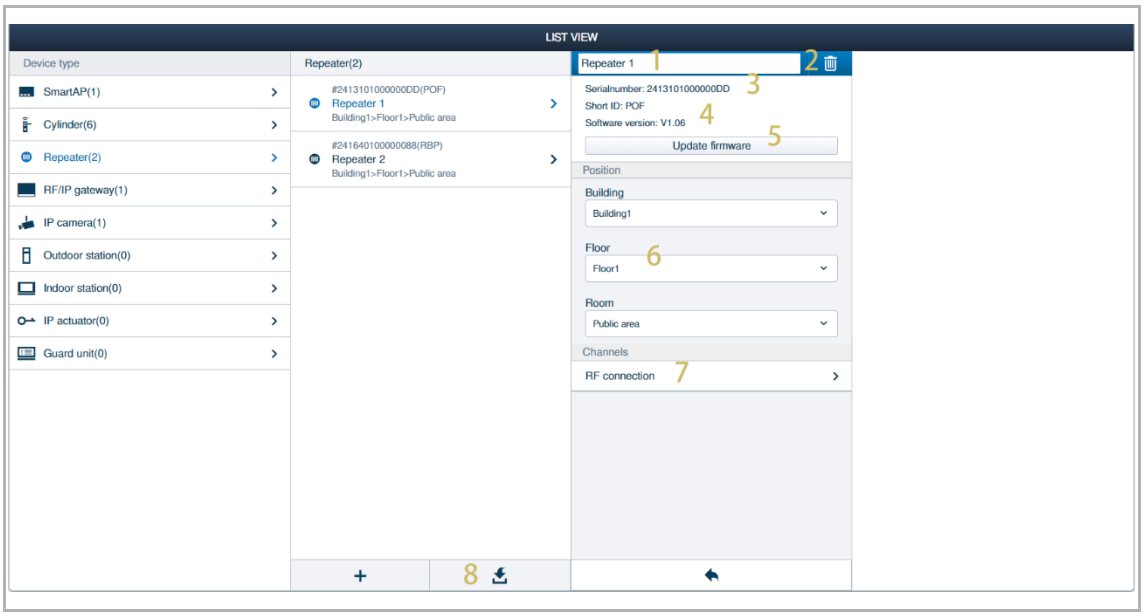
On the configuration screen, click "Device configuration", "Cylinder", "Cylinder 1" to access the configuration screen.



No.	Description
1	Rename the device.
2	**Remove the device** The "Electronic locking cylinder" needs to be unpaired before removing.
3	Serial number of the device.
4	Firmware version of the device.
5	Update the firmware via the website.
6	Assign the location for the device.
7	View RF connection status of the device.
8	Set the unlock time for the "Electronic locking cylinder".
9	**Set the offline day for the cylinder** see chapter 10.5.3 “Setting the offline day“ on page 219.
10	**Enable/disable the "Office mode" function** see chapter 10.6.4 “Office mode“ on page 229.
11	**Managing emergency cards** see chapter 10.5.4 “Managing the emergency cards“ on page 220.
12	Check the battery status of the device.
13	Update the firmware locally or remotely for several devices in batch.

10.6.2 Configuring "RF Repeaters"

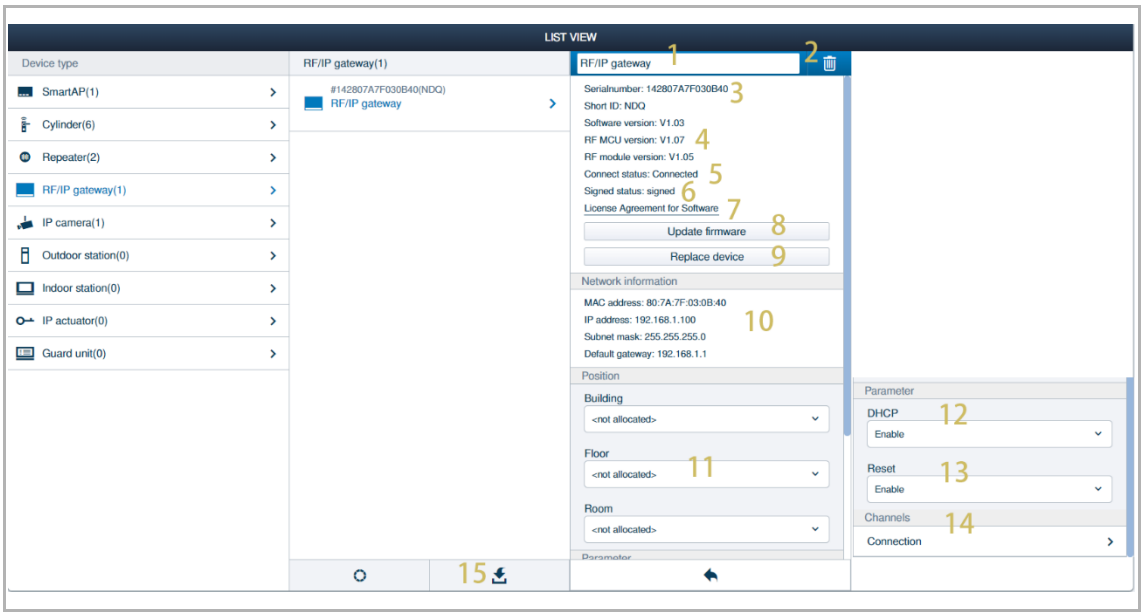
On the configuration screen, click "Device configuration", "Repeater", "Repeater 1" to access the configuration screen.



No.	Description
1	Rename the device.
2	**Remove the device** The device needs to be unpaired before removing.
3	Serial number of the device.
4	Firmware version of the device.
5	Update the firmware via the website.
6	Assign the location for the device.
7	View RF connection status of the device.
8	Update the firmware locally or remotely for several devices in batch.

10.6.3 Configuring "RF/IP Gateways"

On the configuration screen, click "Device configuration", "RF/IP Gateway", "Cylinder 1" to access the configuration screen.



No.	Description
1	Rename the device.
2	**Remove the device** Click "  ", followed by " √ " to remove the device.
3	Serial number of the device.
4	Firmware version of the device.
5	"Connected" means "RF/IP Gateway" is connected to "Smart Access Point" via LAN connection.
6	"Signed" means "RF/IP Gateway" is signed successfully on "Smart Access Point".
7	Click to view the "License agreement for software".
8	Update the firmware via the website.
9	See page 225.
10	View the network information.
11	Assign the location for the device
12	If "DHCP" is set to "Disabled", you need to set the static IP address for the device.
13	If "Reset" is set to "Disabled", the reset button of the devices cannot be used anymore.
14	View RF connection status of the device.
15	Update the firmware locally or remotely for several devices in batch.

Replacing a new device

You can use a new "RF/IP Gateway" to replace the old one if the old one is broken. All the data (including the position and connection) on the old one will be copied to the new one.

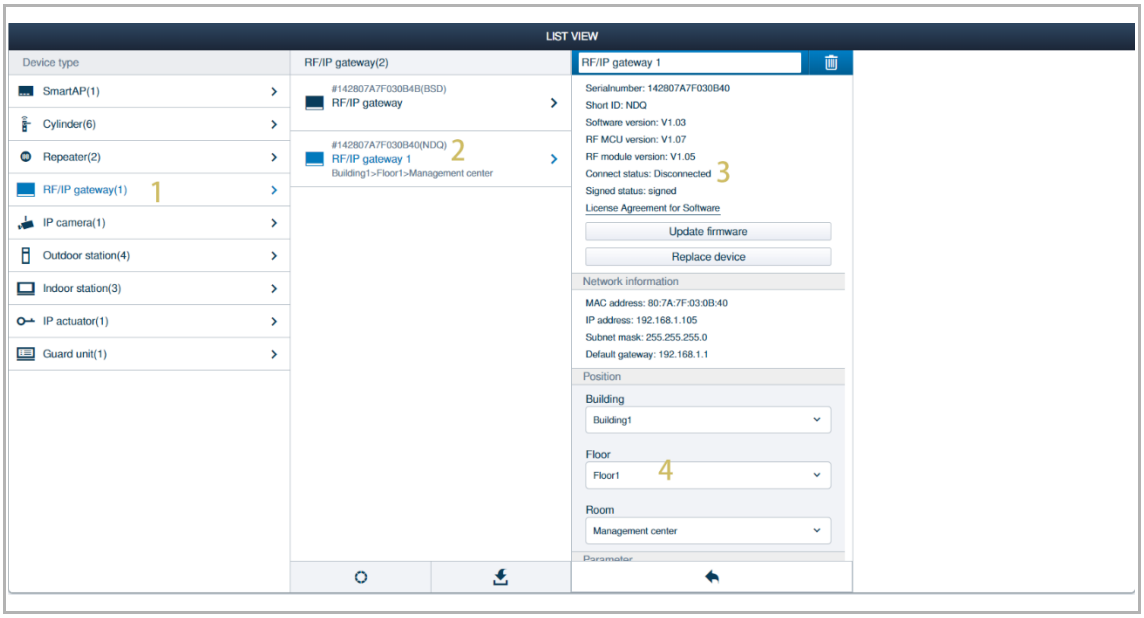
Please follow the steps below:

[1] On the "Device configuration" screen, click "RF/IP Gateway".

[2] Click the "RF/IP Gateway 1".

[3] The connected status should be "Disconnected" if this old one is broken.

[4] The position of the old one is displayed on the screen.



[5] Add a new one without position. see chapter 10.3.4 “Adding and locating "RF/IP Gateways"“ on page 202.

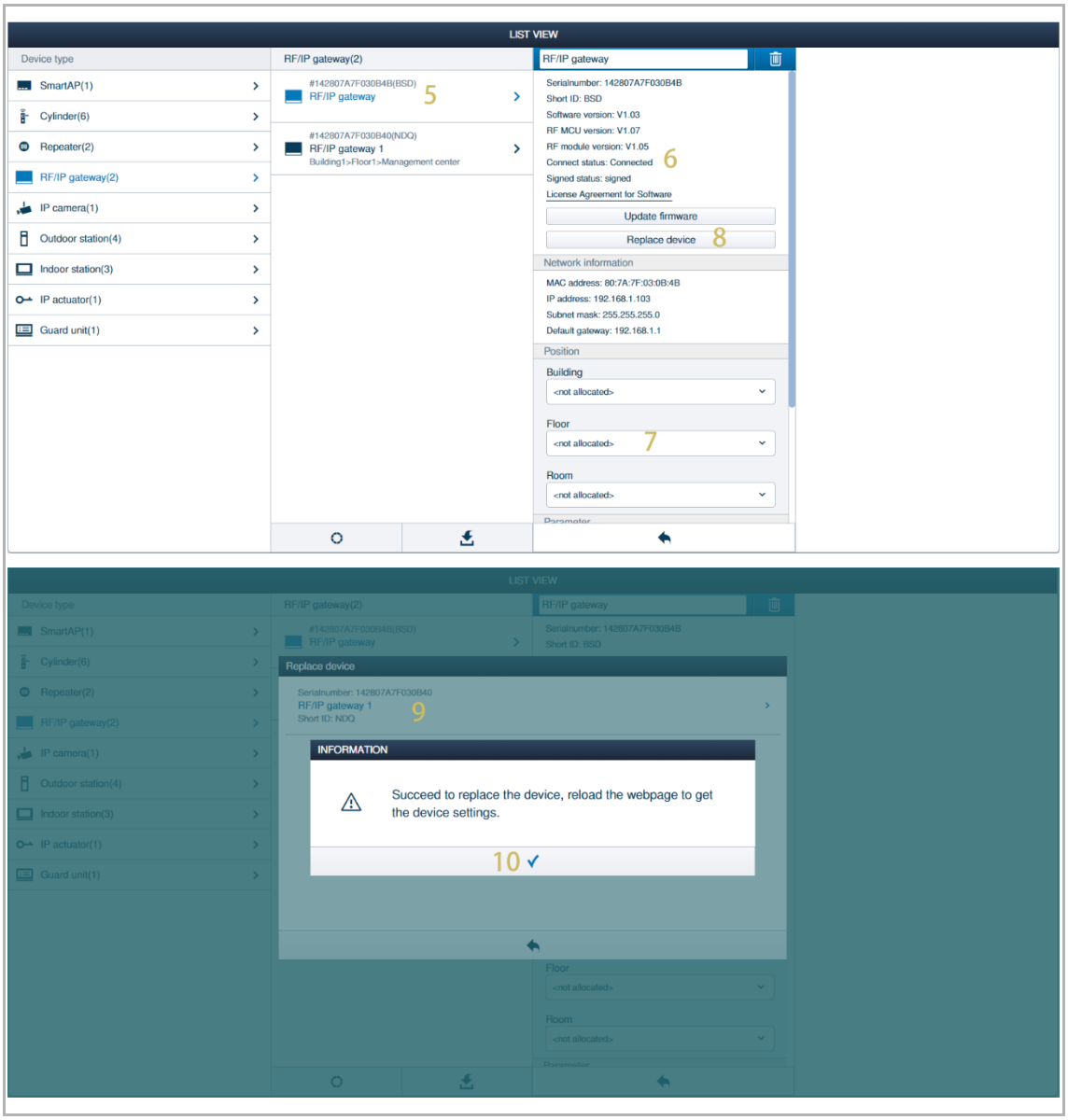
[6] The connected status of the new one should be "Connected".

[7] The position of the new one is empty currently.

[8] Click "Replace device" on the new one.

[9] Click the old one on the list.

[10] Click " √ " to continue if the device is replaced successfully.

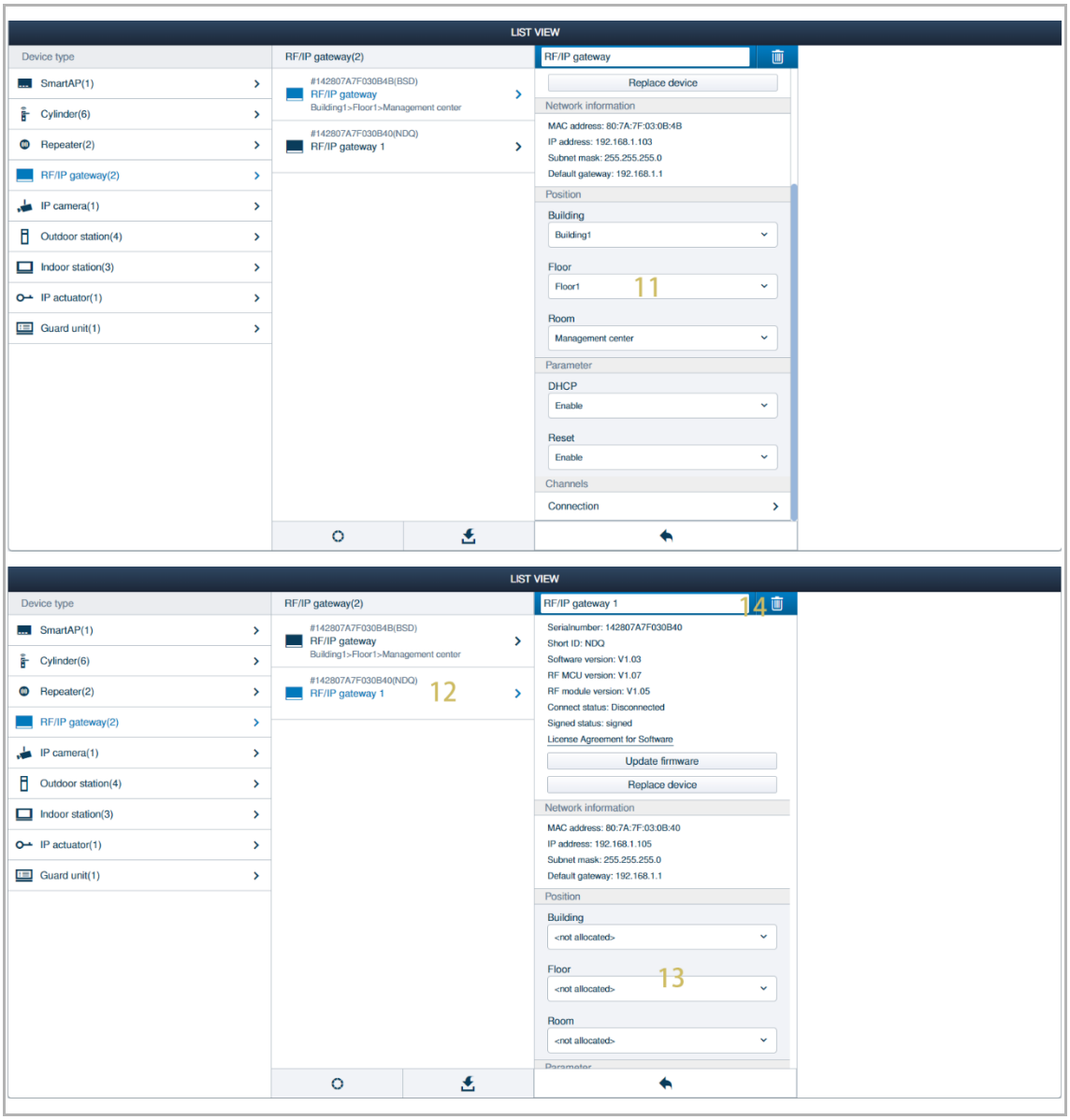


[11]The position of the old one is copied to the new one (The connections on the old one are also copied to the new one).

[12]Click the old one.

[13]The position of the old is empty. (The connections on the old one are also cleared).

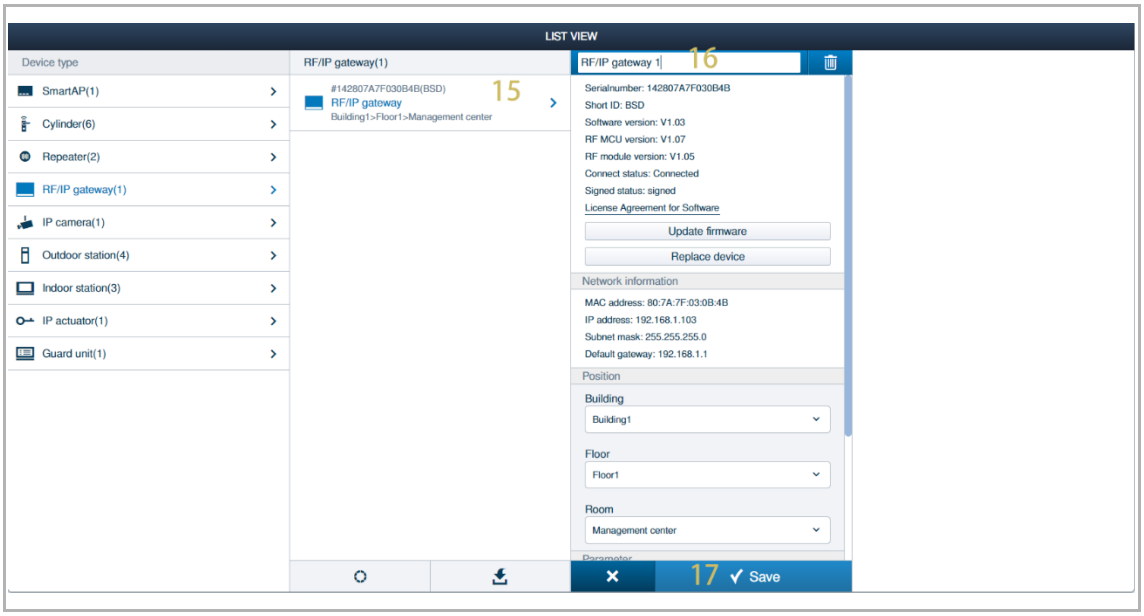
[14]Click " " , followed by " √ " to remove the old one.



[15]Click the new one.

[16]Rename the new one.

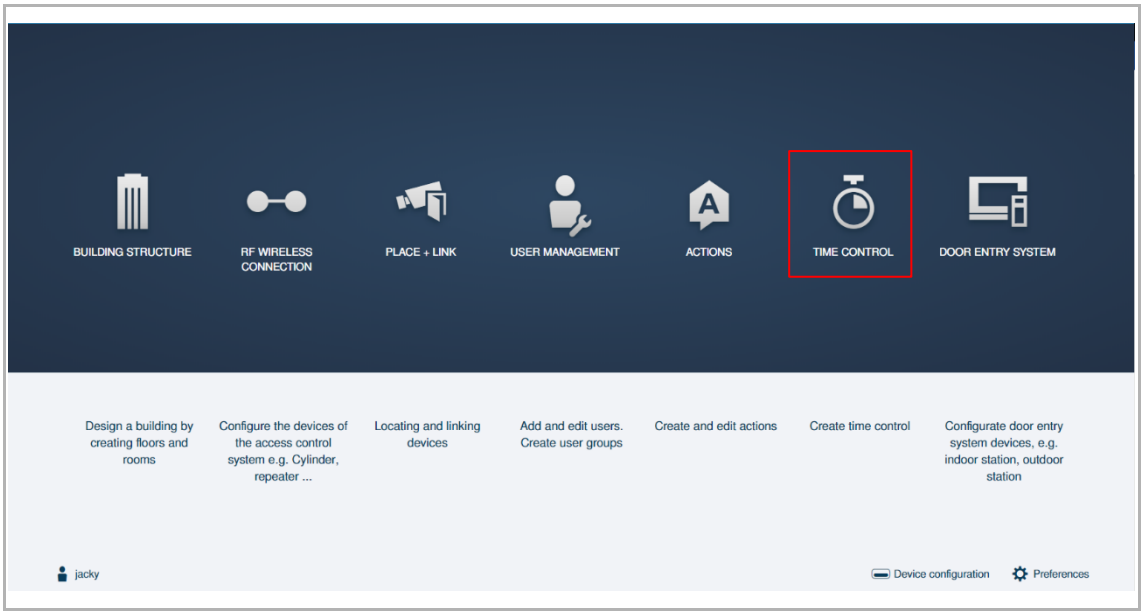
[17]Click " √ " to save.



10.6.4 Office mode

Access the "Time control" screen

On the configuration screen, click "Time control" to access the "Time control" screen.



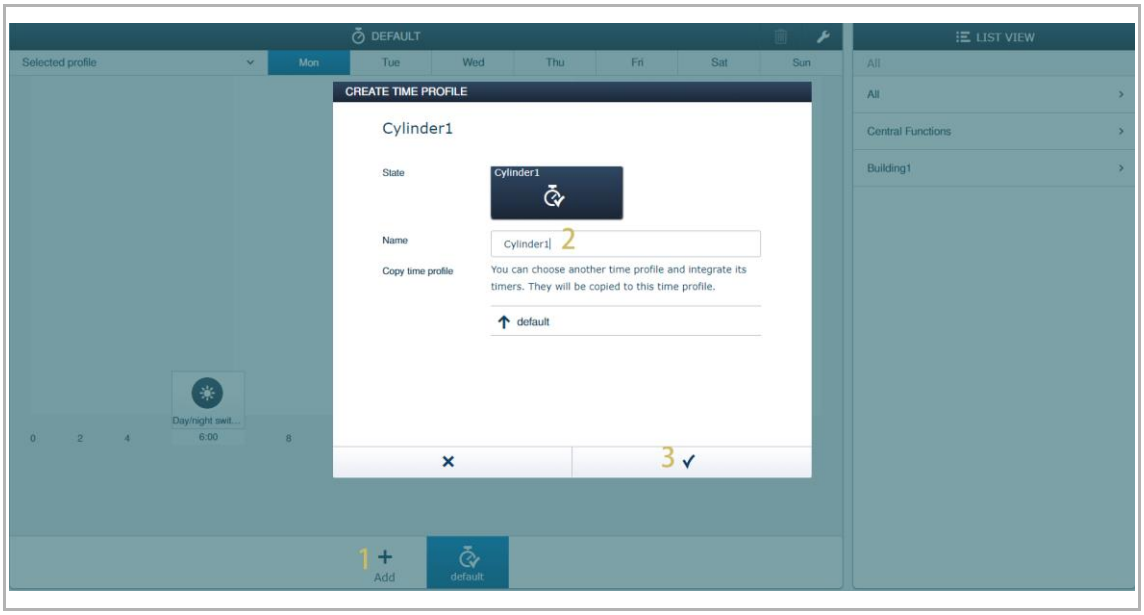
1. Adding "Office mode" time profile for the designated "Electronic locking cylinder"

Please follow the steps below:

[1] On the "Time control" screen, click "Add".

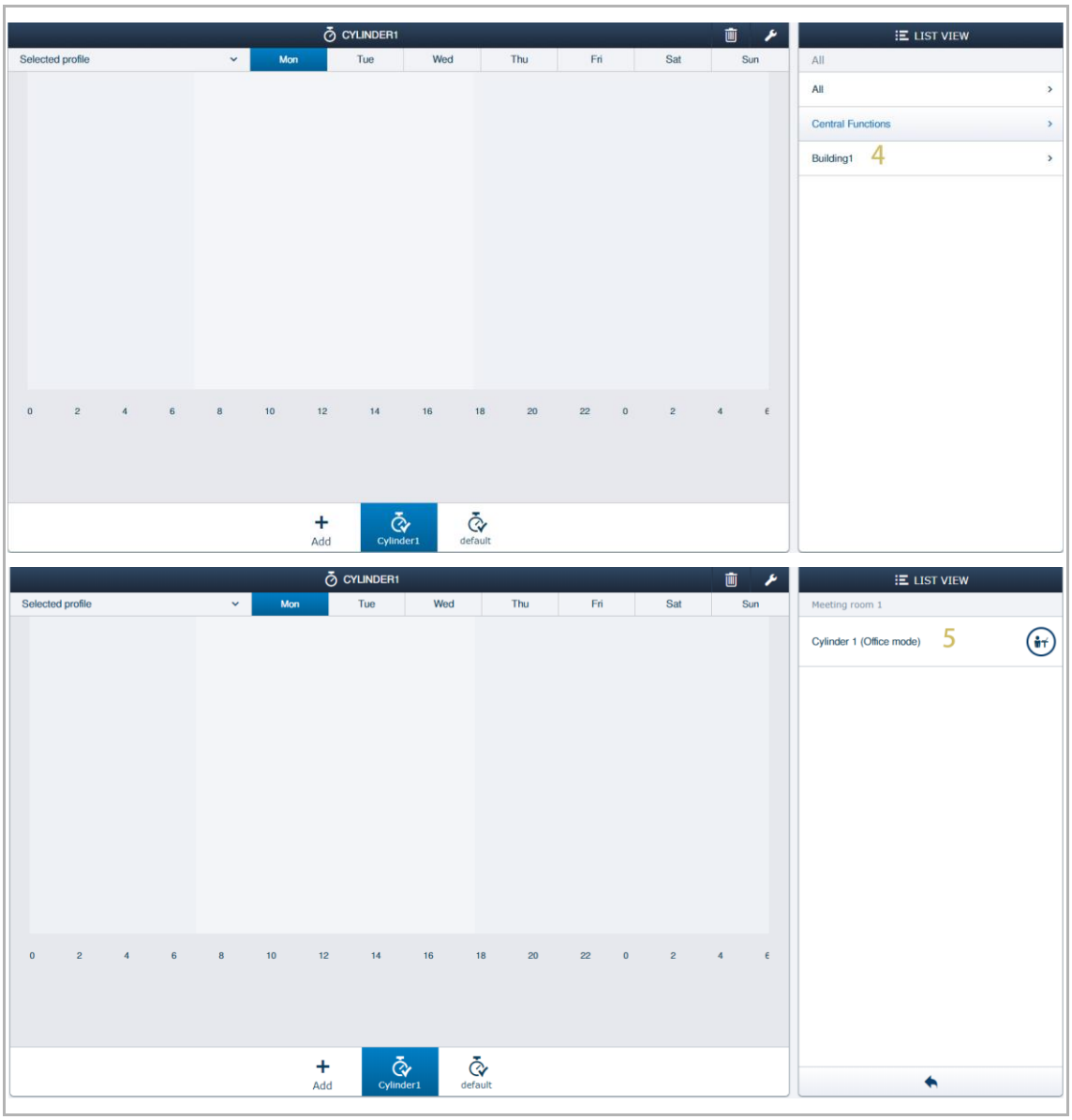
[2] Enter the name (e.g. "Cylinder1").

[3] Click " √ " to save.



[4] Click "Building1">>"Floor 1">>"Meeting room 1" to access the location of the designated "Electronic locking cylinder".

[5] Click the designated "Electronic locking cylinder" (e.g. "Cylinder 1")

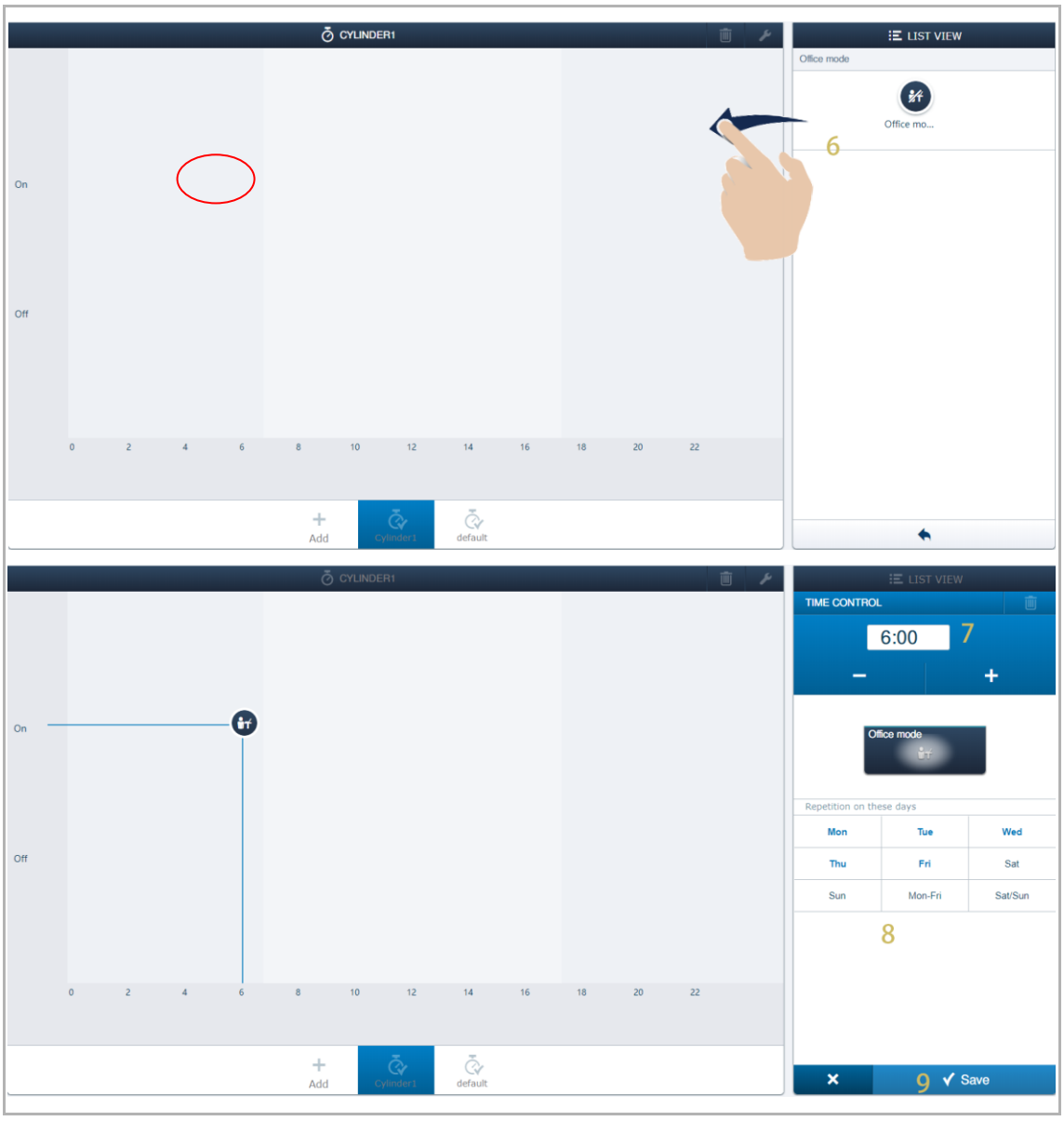


[6] Drag the "Office mode" icon onto the "On" position on the screen.

[7] Enter the precise time.

[8] Click the designated day to cancel the selection (optional).

[9] Click " √ " to save.

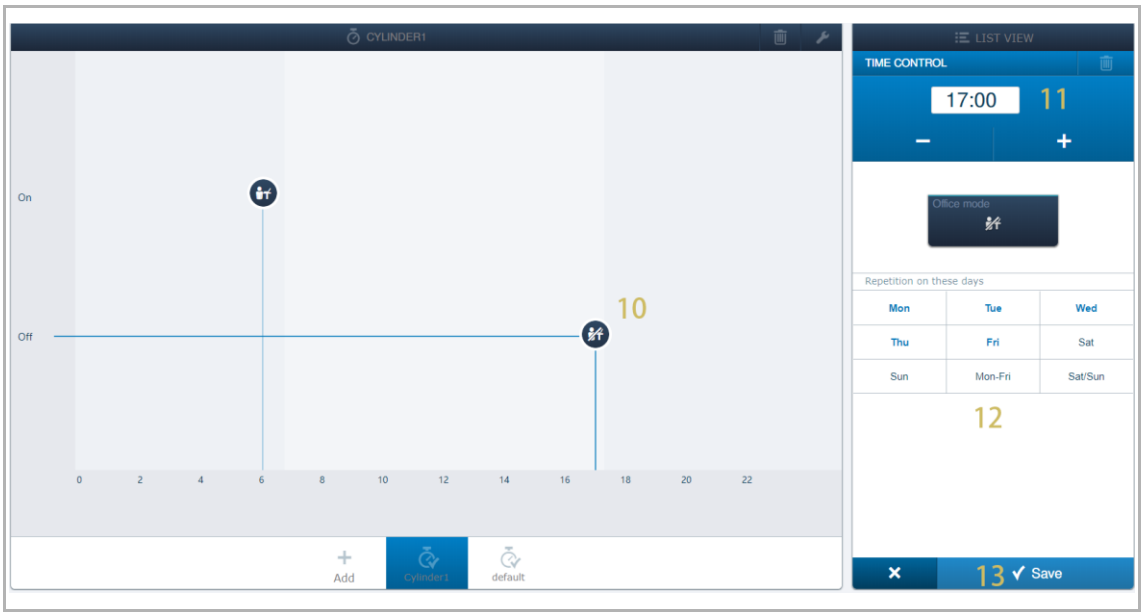


[10]Drag the "Office mode" icon into the "Off" position on the screen.

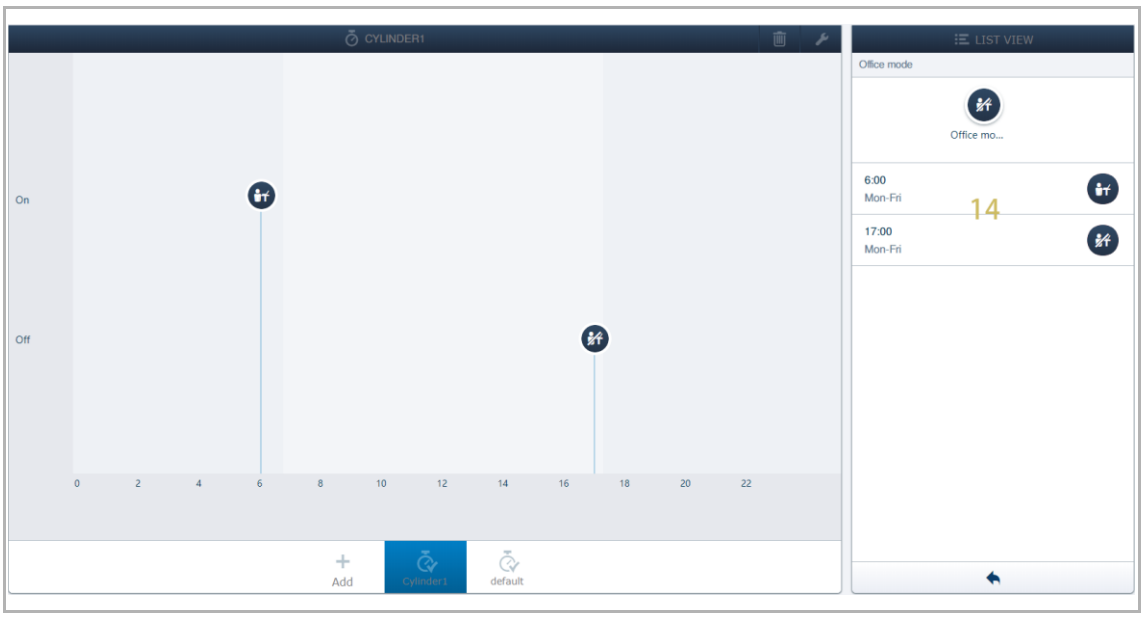
[11]Enter the precise time.

[12]Click the designated day to cancel the selection (optional).

[13]Click " √ " to save.



[14]The result is displayed on the screen.



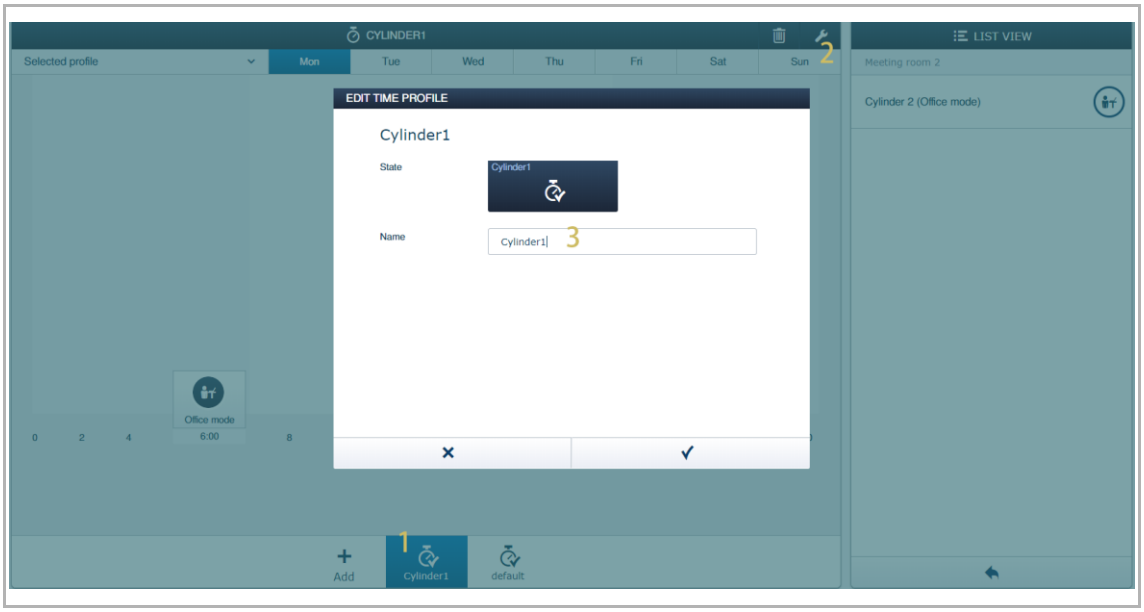
2. Renaming "Office mode" time profile for the designated "Electronic locking cylinder"

Please follow the steps below:

[1] On the "Time control" screen, click the designated "Electronic locking cylinder" (e.g. "Cylinder 1").

[2] Click " " ".

[3] Enter a new name.



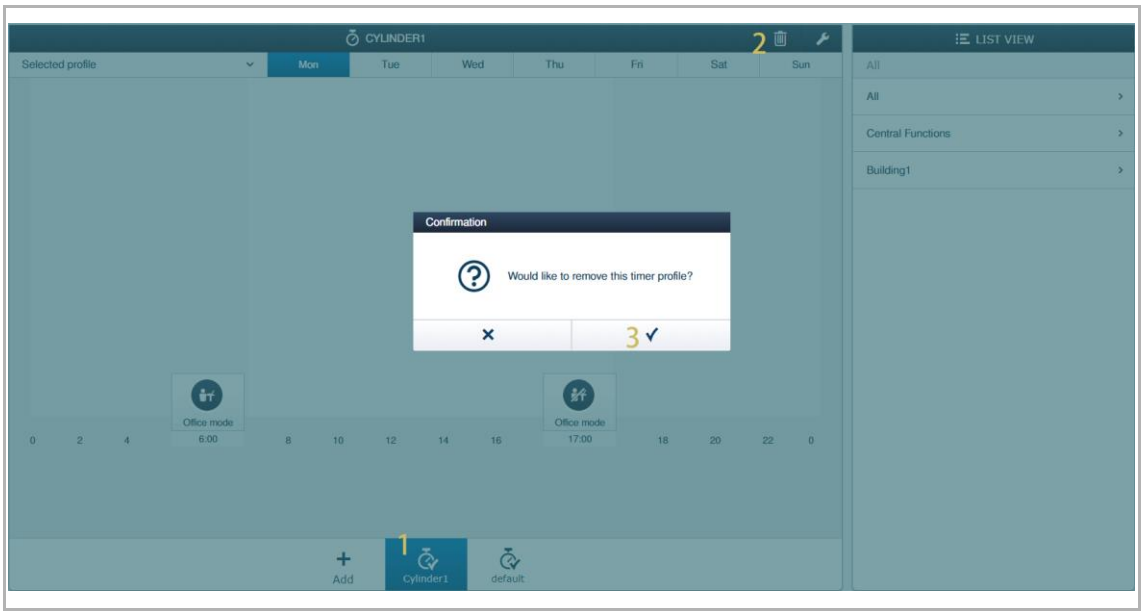
3. Removing "Office mode" time profile for the designated "Electronic locking cylinder"

Please follow the steps below:

[1] On the "Time control" screen, click the designated "Electronic locking cylinder" (e.g. "Cylinder 1").

[2] Click " " ".

[3] Click " √ " to confirm.

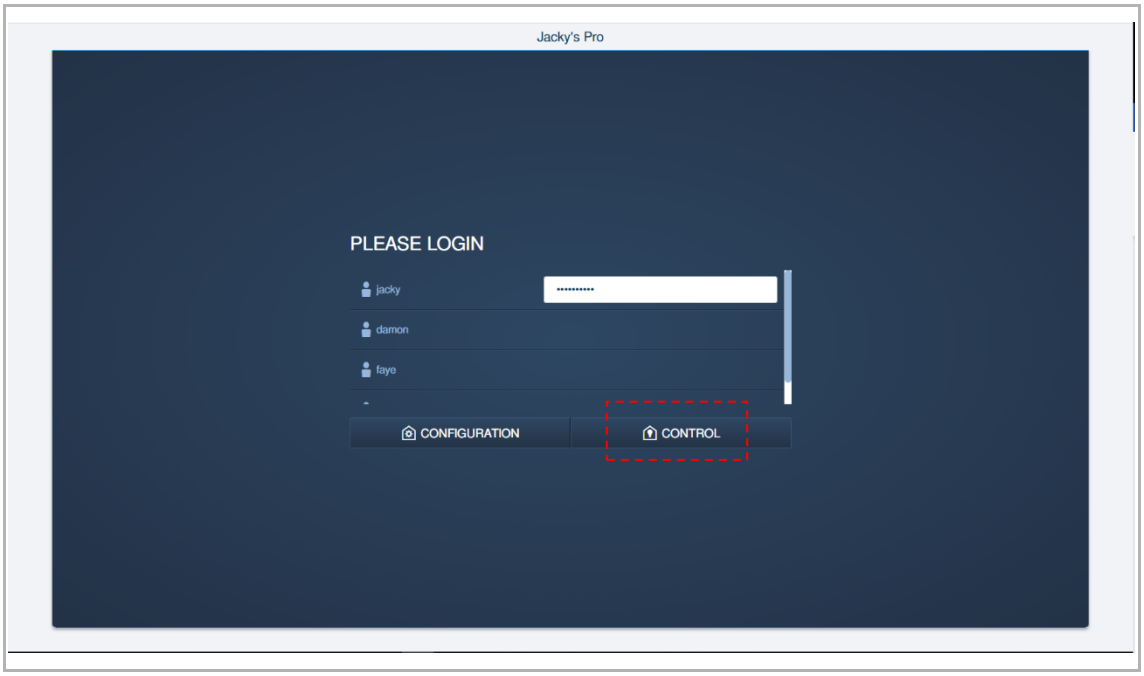


10.7 Controlling the devices via "Smart Access Point"

Accessing the control screen

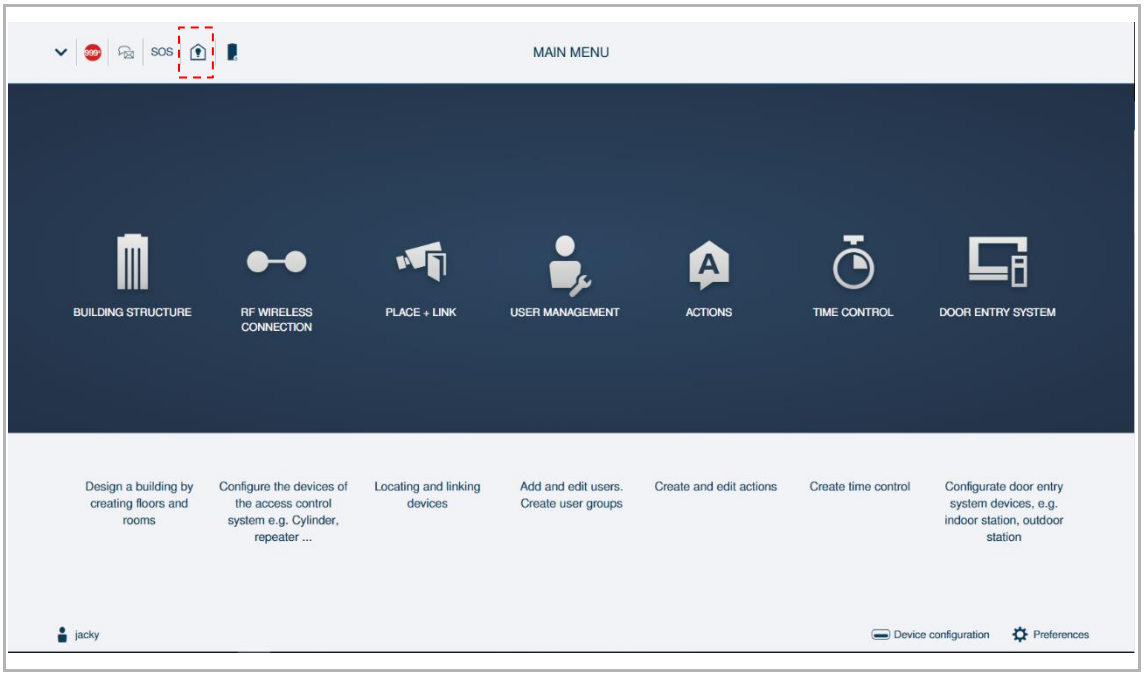
1. The following operation can be operated by all users:

On the login screen, enter the password and click "Control" to access the corresponding screen.



2. The following operation can only be operated by admin users:

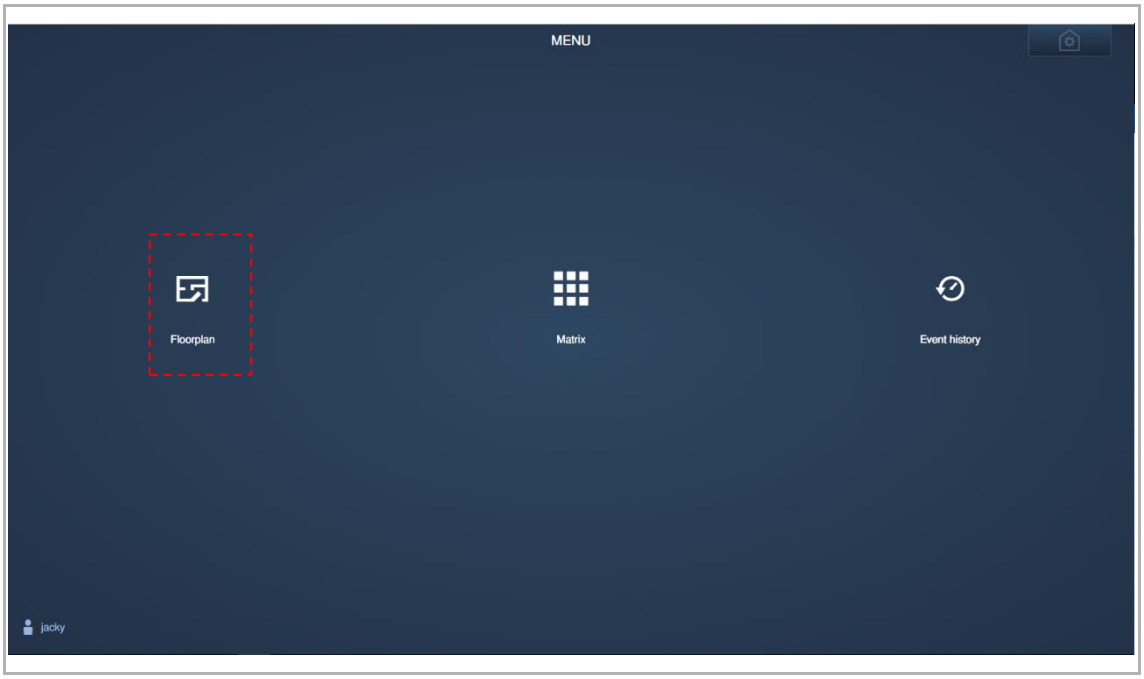
On the configuration screen, click " " to access the control screen.



10.7.1 Controlling the devices via floorplan

Accessing the floorplan screen

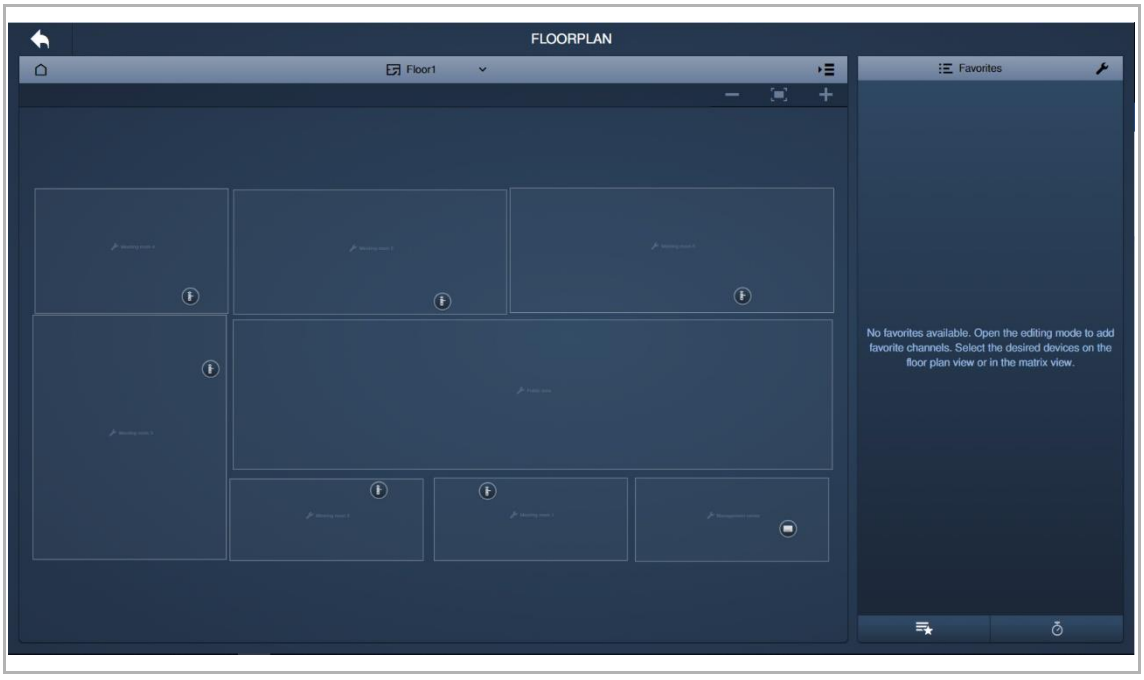
On the control screen, click "Floorplan" to access the corresponding screen.



Note

The following operations are based on demo case. You need to adjust your operations when you are operating an actual project.

Click "Building 1","Floor 1" to access the floorplan screen.

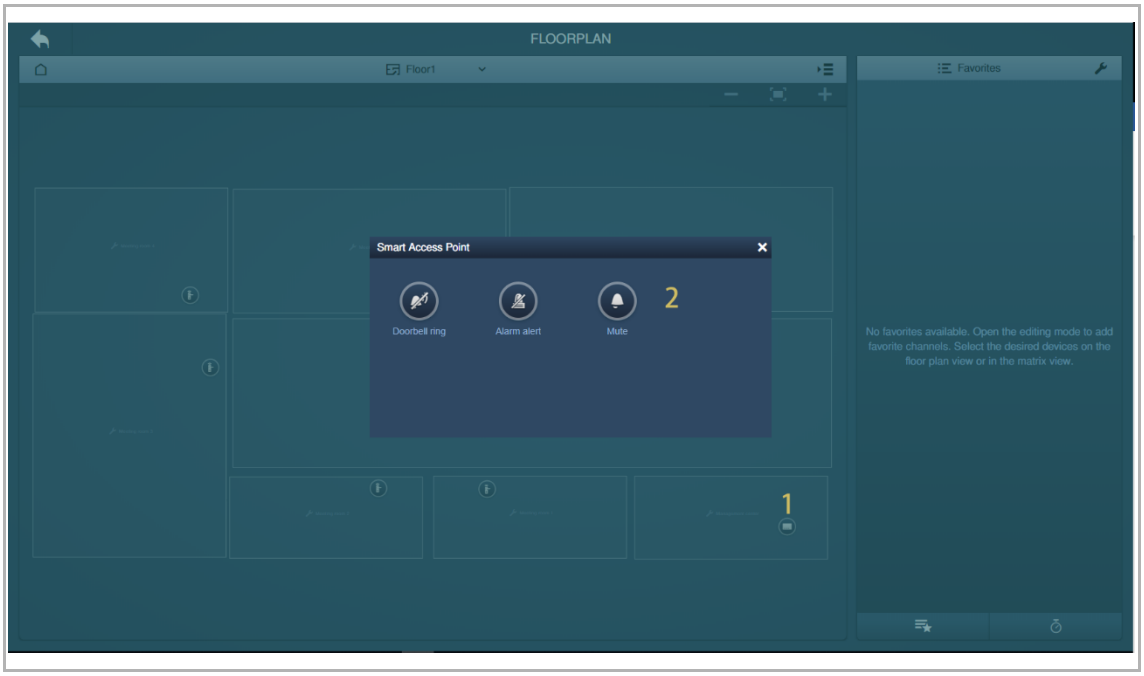


1. Control the function of "Smart Access Point"

Please follow the steps below:

[1] On the floorplan screen, click "Smart Access Point".

[2] Click a function icon to operate the function.

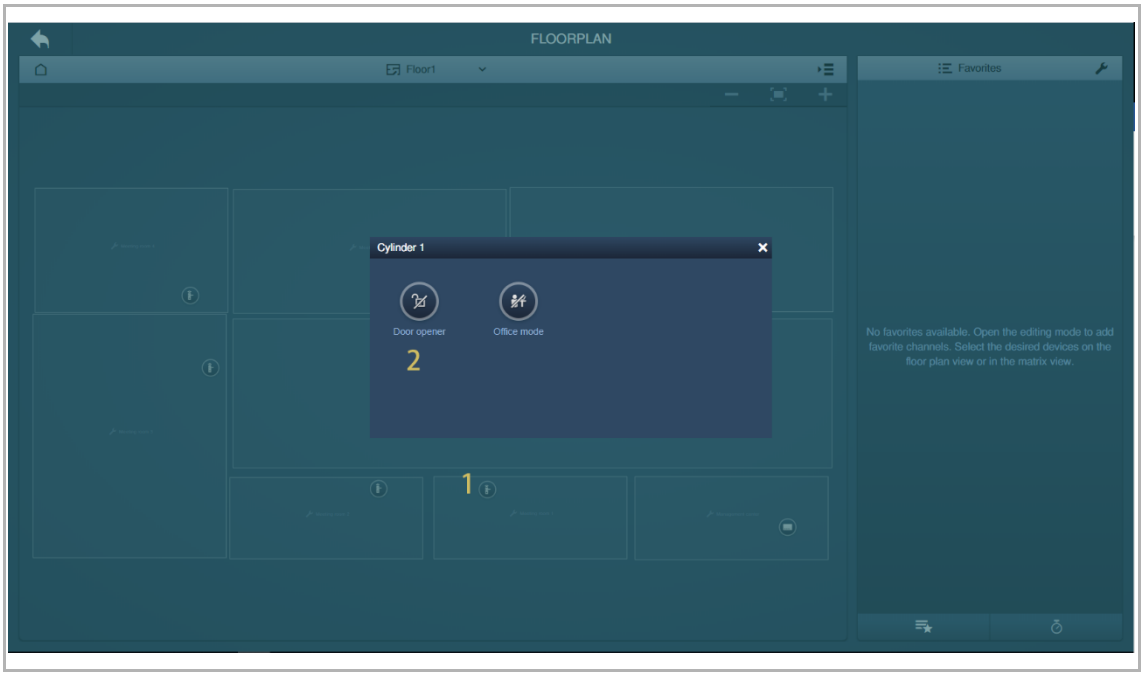


2. Release the designated "Electronic locking cylinder"

Please follow the steps below:

[1] On the floorplan screen, click the designated "Electronic locking cylinder" (e.g. "Cylinder 1" for demo case 1).

[2] Click "Door opener" icon to release the "Electronic locking cylinder".

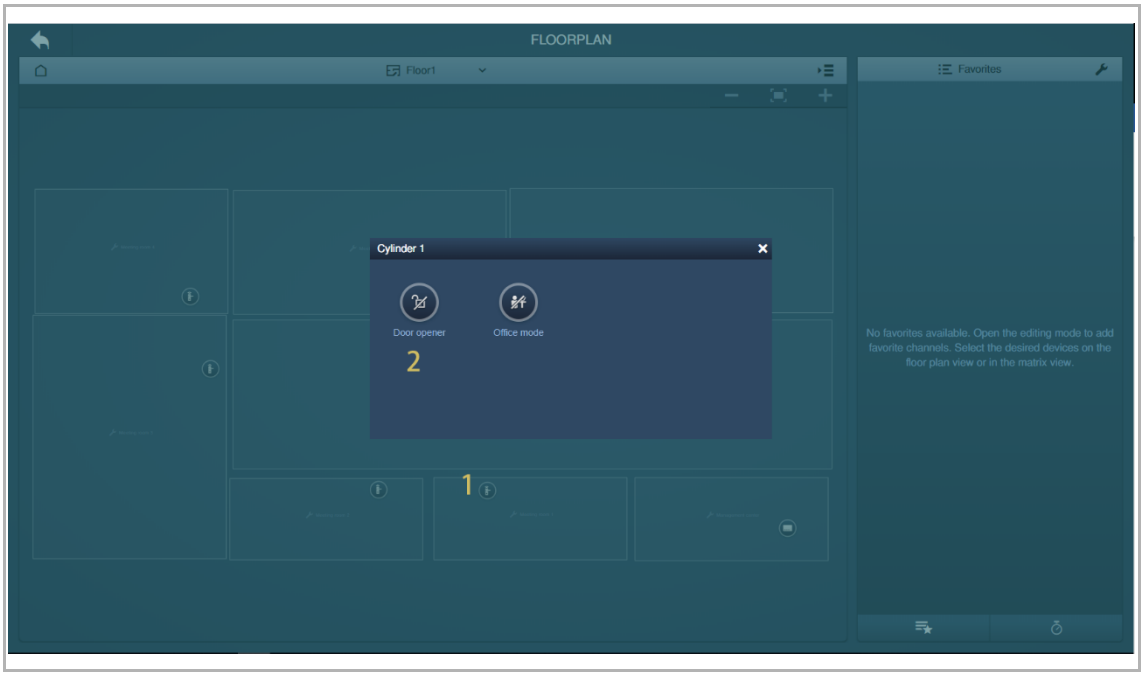


3. Enable/disable the office mode for the designated "Electronic locking cylinder"

Please follow the steps below:

[1] On the floorplan screen, click the designated "Electronic locking cylinder" (e.g. "Cylinder 1" for demo case 1).

[2] Click "Office mode" icon to enable/disable the "office mode" function, see chapter 10.6.4 “Office mode“ on page 229.

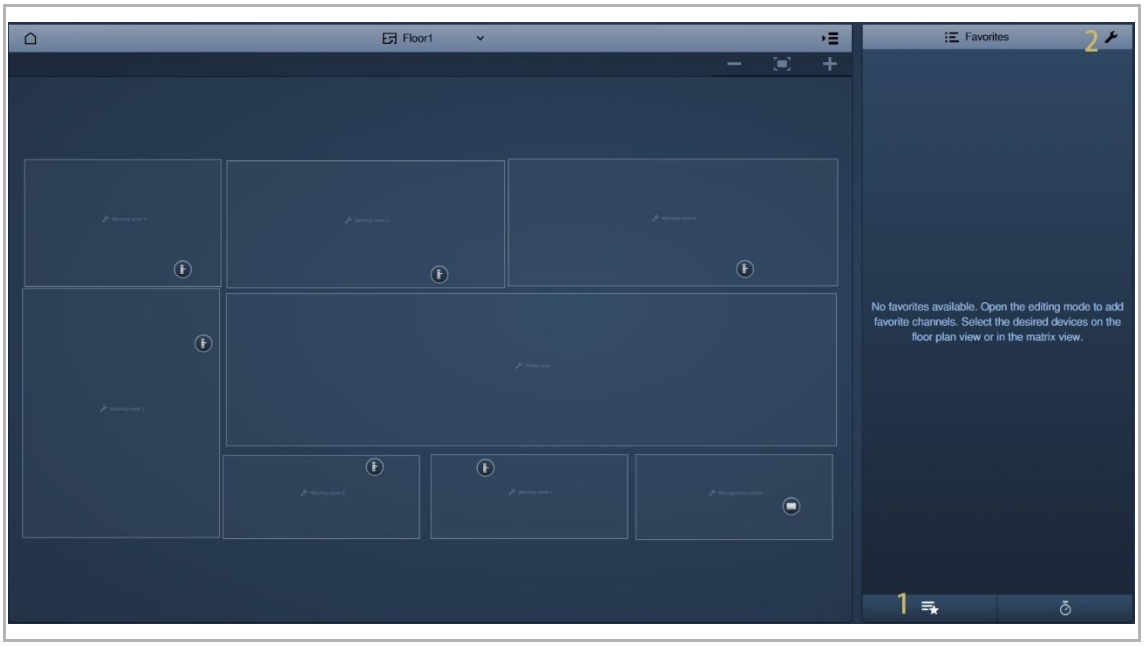


4. Add the designated operations to the favorites list

Please follow the steps below:

[1] On the floorplan screen, click " ".

[2] Click " ", a highlight indicates the setting status.



[3] On the setting status, click an AccessControl devices (e.g. "Cylinder 1").

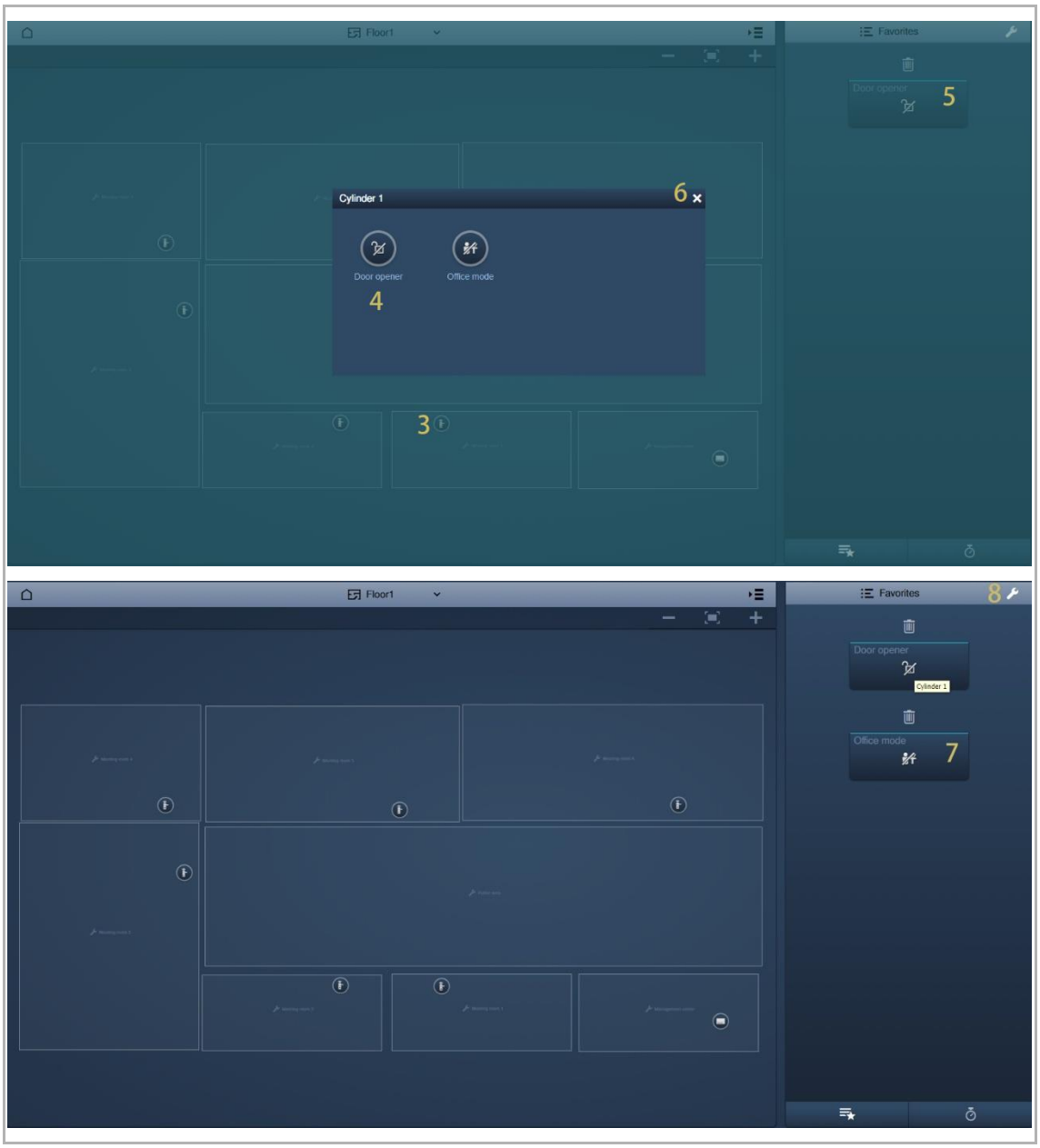
[4] Click a function icon (e.g. "Door opener").

[5] The function icon will be added to the favorites list.

[6] Click "x" to close the pop-up window.

[7] Repeat the steps 3~6 to add other operations one by one.

[8] Click " " to quit the setting status.

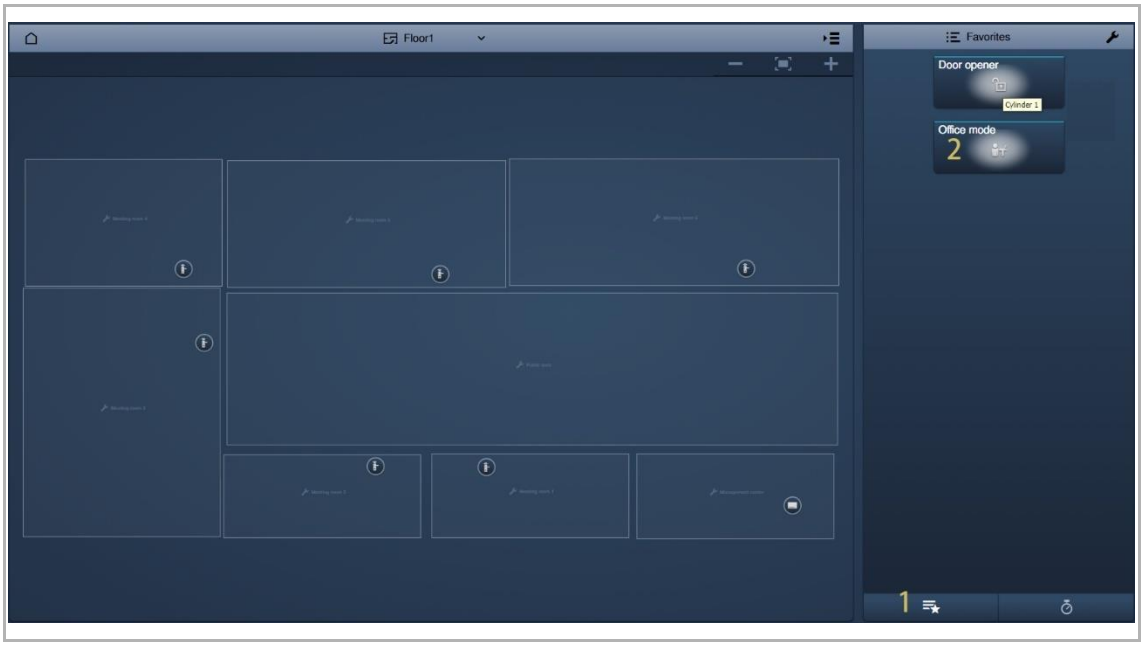


5. Operate the functions on the favorite list

Please follow the steps below:

[1] On the floorplan screen, click " ".

[2] Click the designated function icon on the favorites list to activate/deactivate the function, the highlight indicates the activated status.



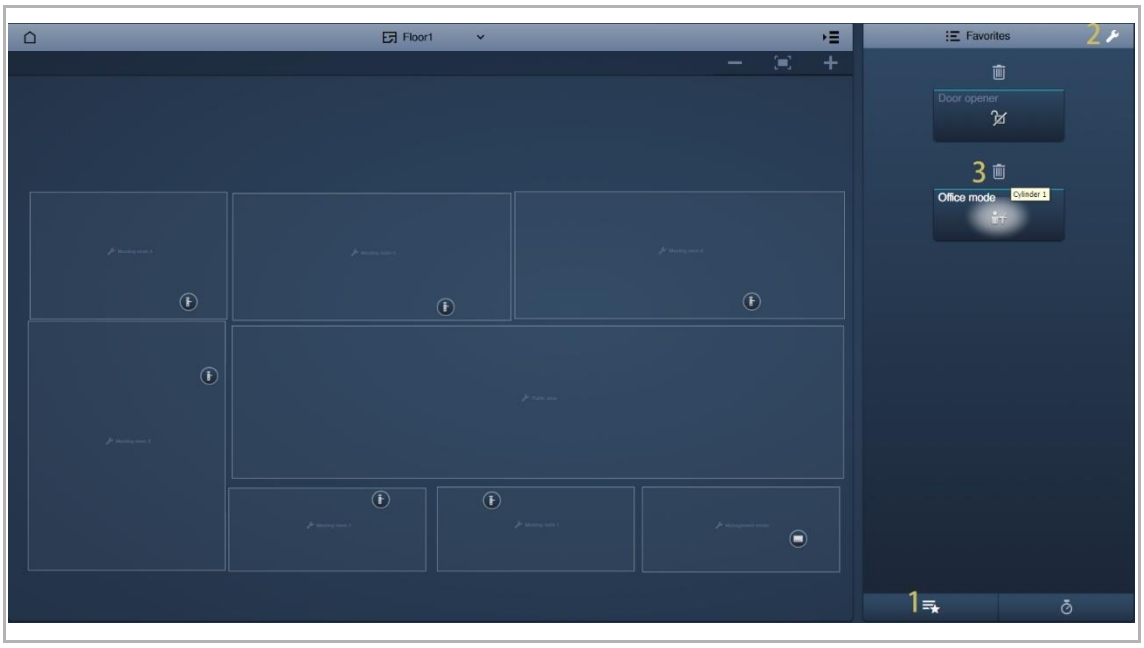
6. Remove the functions from the favorites list

Please follow the steps below:

[1] On the floorplan screen, click " ".

[2] Click " ", a highlight indicates the setting status.

[3] Click " " to remove it directly.



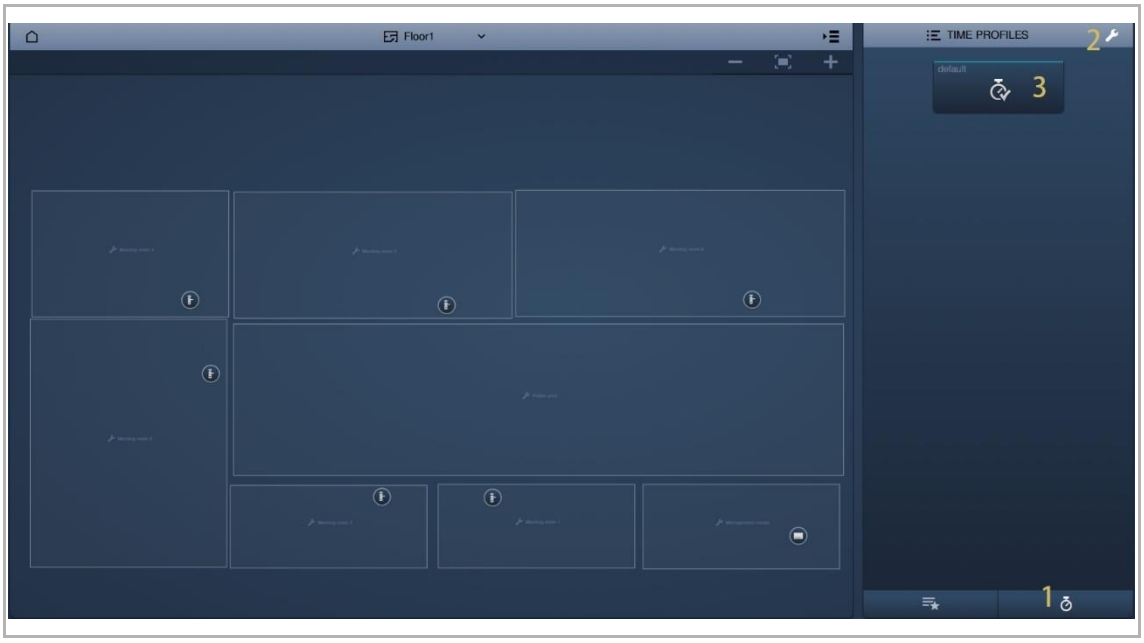
7. Enable/disable the time profiles

Please follow the steps below:

[1] On the floorplan screen, click " ".

[2] Click " ", a highlight indicates the setting status.

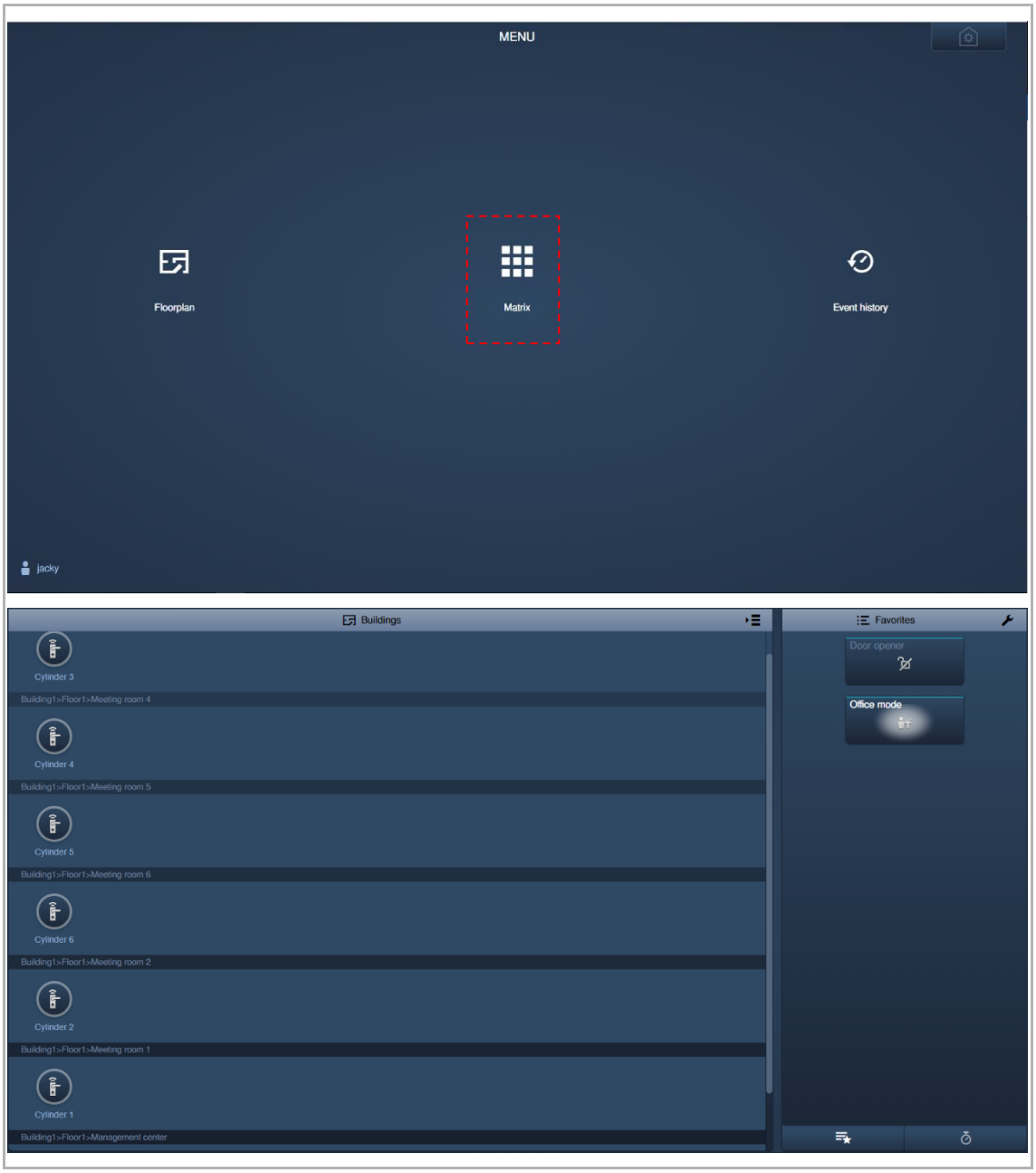
Click "Time profile" icon to enable/disable the "Time profile" funciton.



10.7.2 Controlling the devices via matrix

Accessing the matrix screen

On the control screen, click "Matrix" to access the corresponding screen.



Note

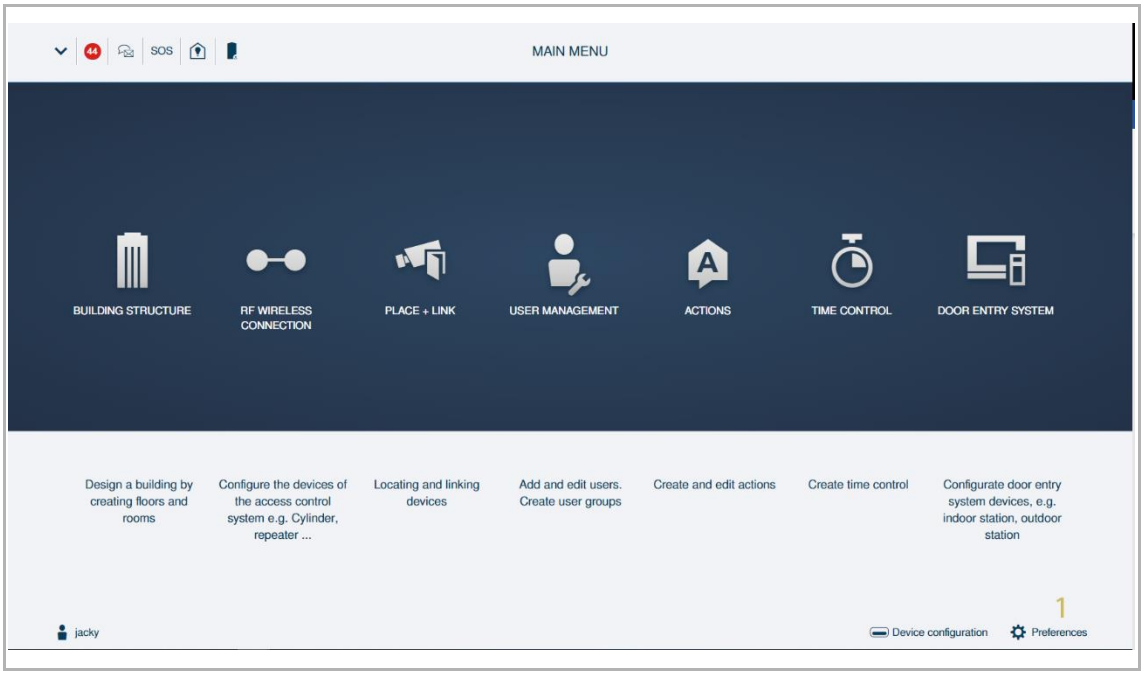
The operations on the matrix screen are the same to floorplan screen. see chapter 10.7.1 “Controlling the devices via floorplan“ on page 237.

10.8 Controlling the devices via Welcome App

10.8.1 Pairing "Smart Access Point" with Welcome App

Please follow the steps below:

[1] On the configuration screen, click "Preference".



[2] Click "MyBuildings Account".

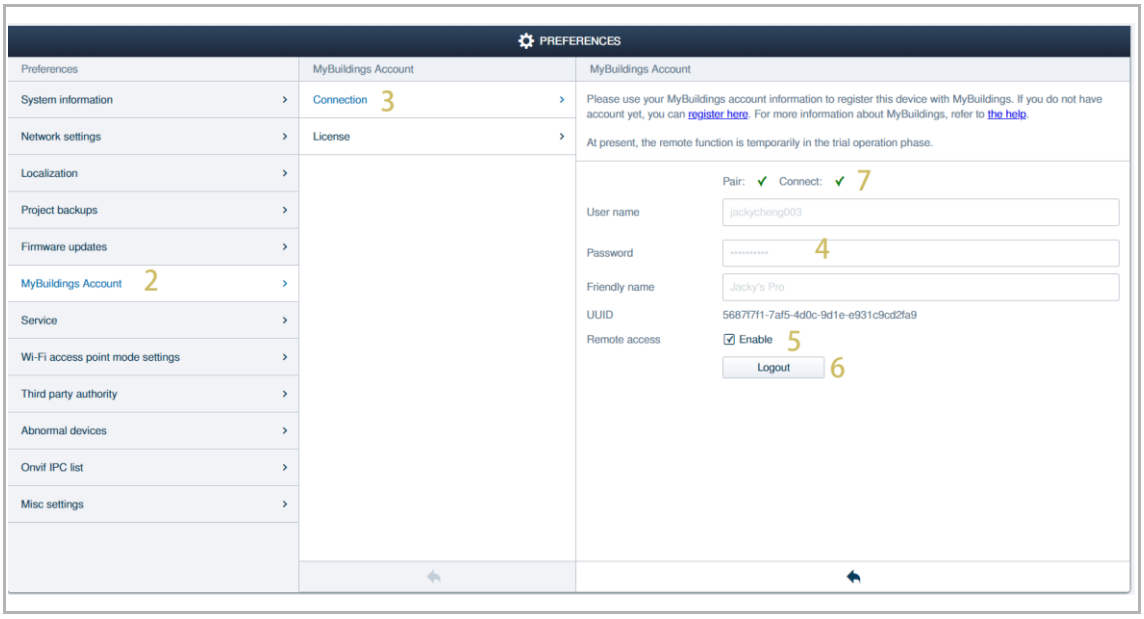
[3] Click "Connection".

[4] Enter the account, password and friendly name.

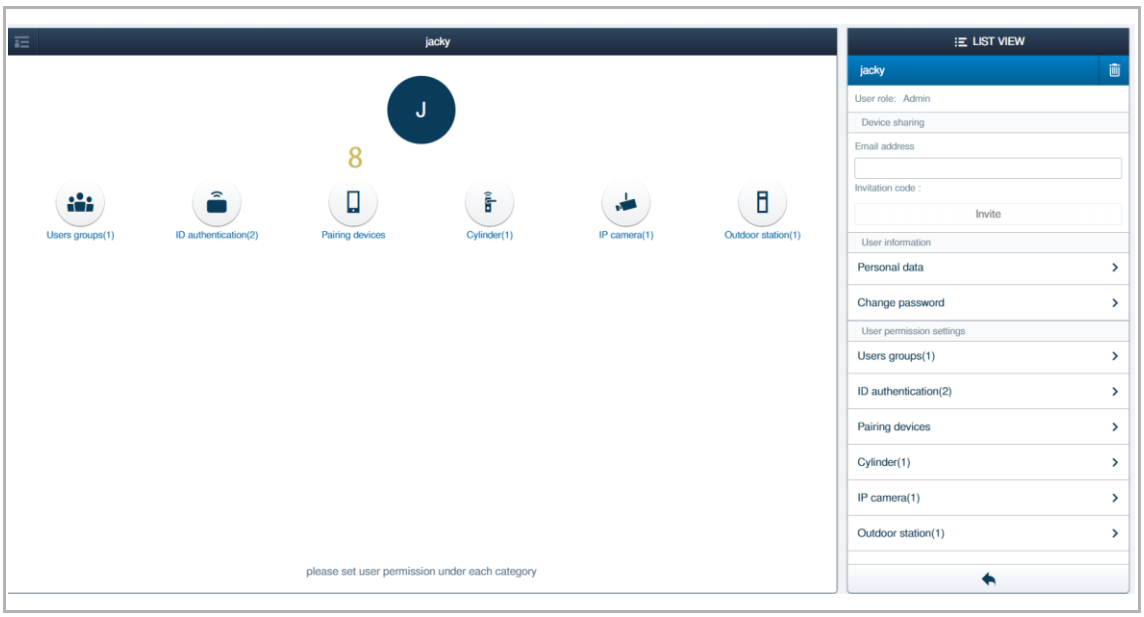
[5] Tick "Enable" to activate "Remote access" function. (optional).

[6] Click "Login".

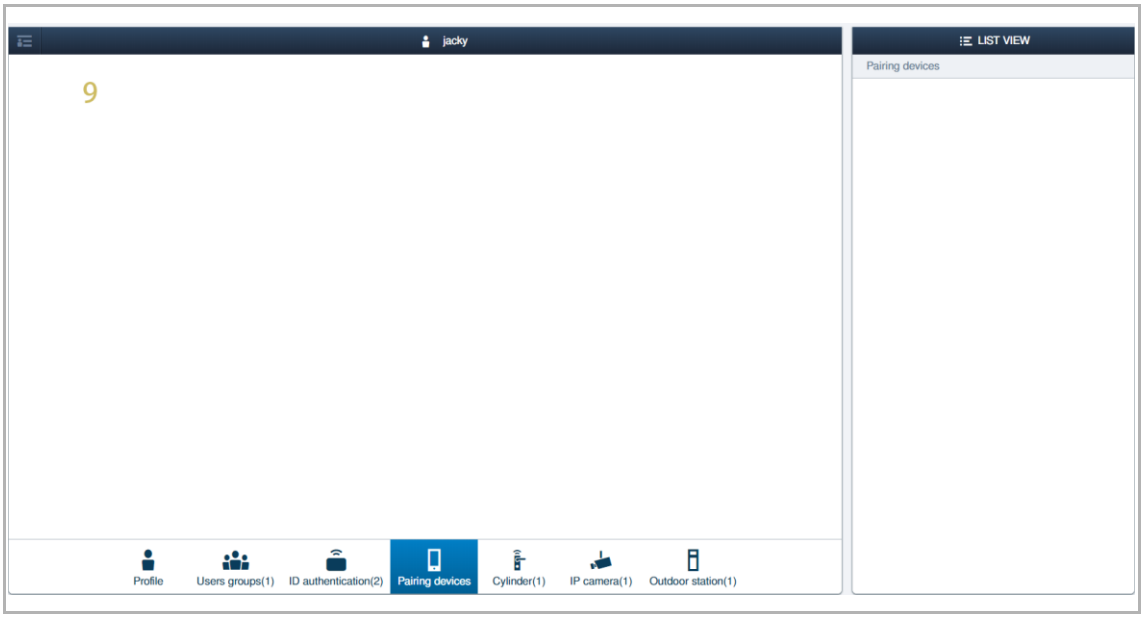
[7] Check the pair status and connect status. Green " √ " will be displayed if the connection is successful.



[8] Return to the designated user screen, click "Pairing devices".



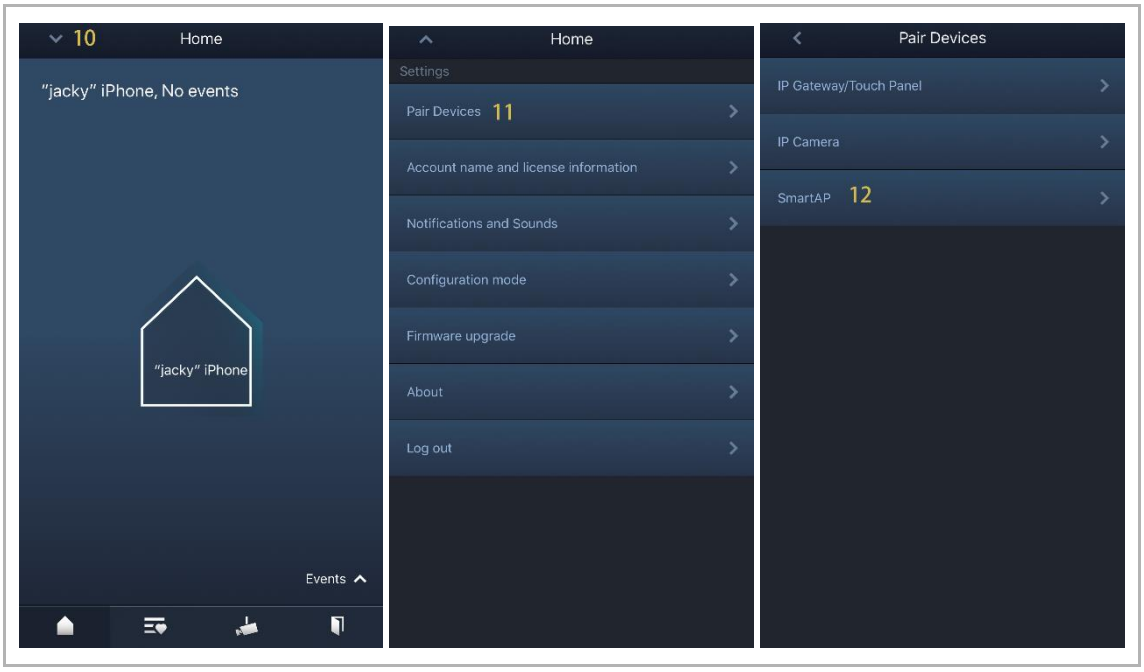
[9] Currently, no device is displayed. You need to continue to the next step on Welcome App.



[10]On the Welcome App "Home" screen, tap "√" (Welcome App needs to login using the same MyBuildings account with "Smart Access Point").

[11]Tap "Pair devices".

[12]Tap "SmartAP".

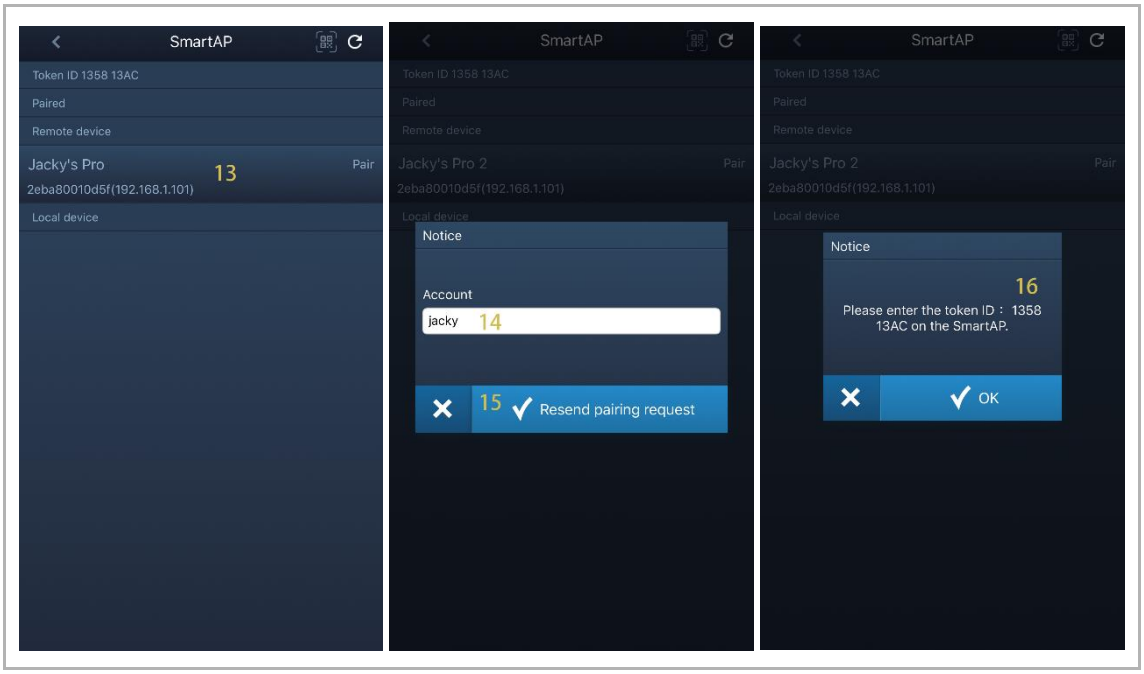


[13]Tap the designate "Smart Access Point" on the "Remote device" section.

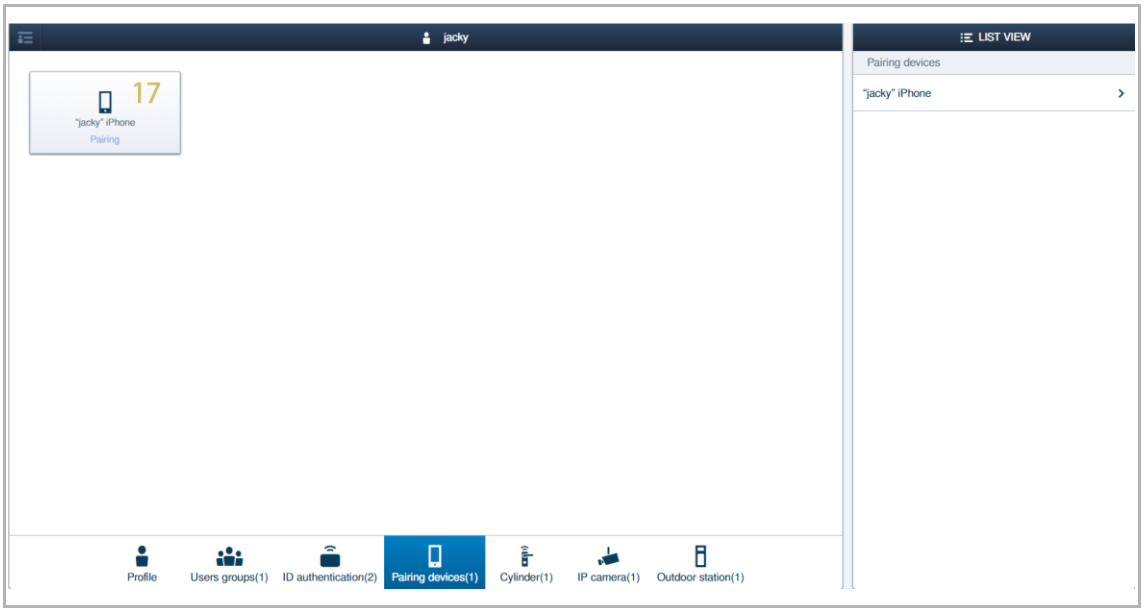
[14]Enter the designated user name used on "Smart Access Point".

[15]Tap " √ " to confirm.

[16]A token ID is displayed on a pop-up window. This token ID will be used on step 18 on "Smart Access Point".



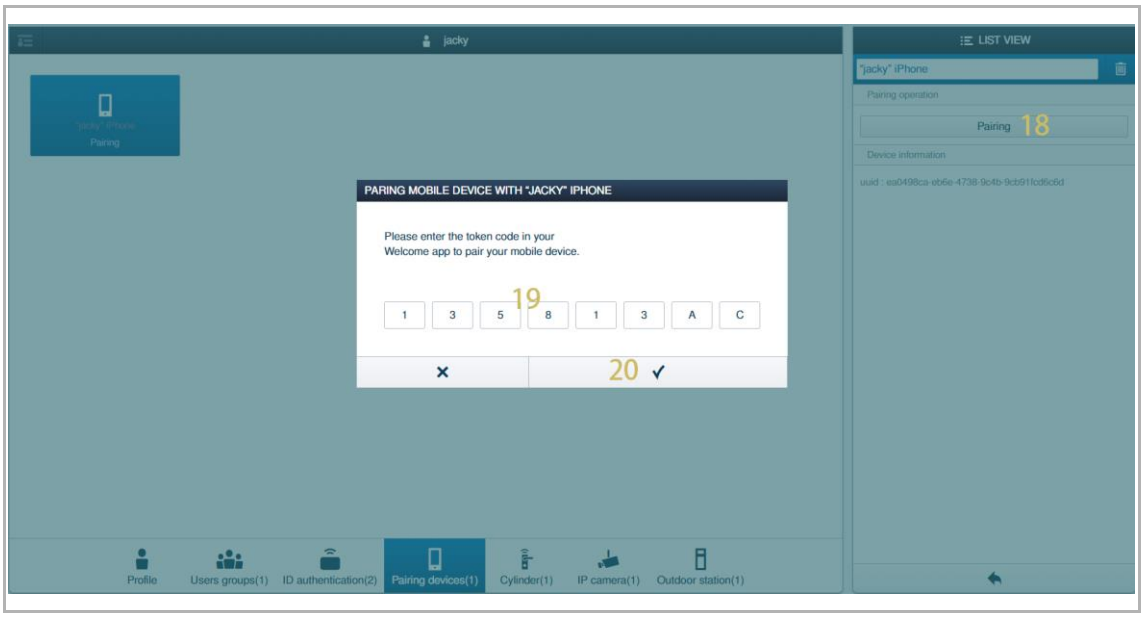
[17]Go to "Smart Access Point", on the "Pairing devices" screen (refer to step 9), a device with a friendly name used by Welcome App is displayed on the screen. Click this device.



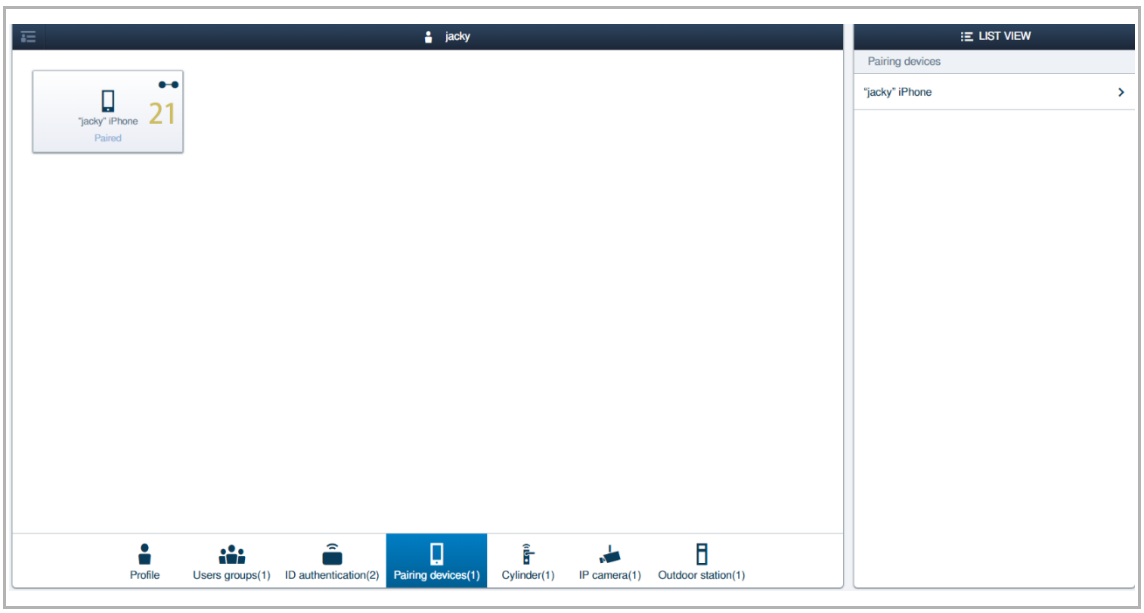
[18]Click "Pairing".

[19]Enter the token ID (refer to step 16).

[20]Click "√" to confirm.



[21]"Paired" status is displayed on the screen if successful.



10.8.2 Controlling "Electronic locking cylinders" via Welcome App

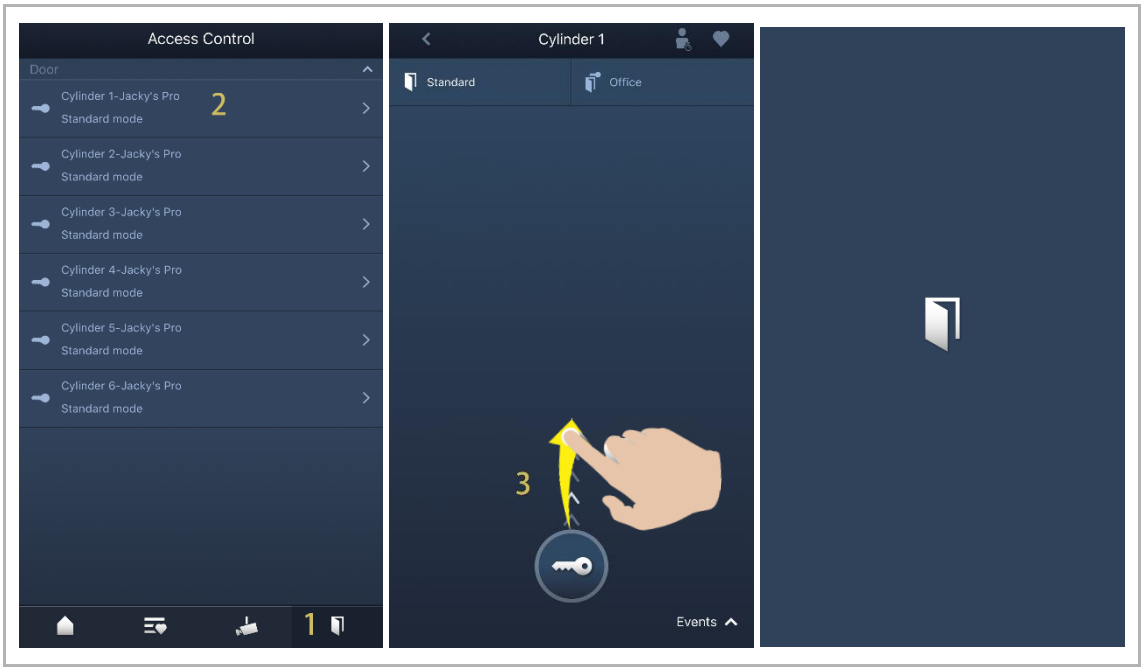
Releasing the "Electronic locking cylinder"

Please follow the steps below:

[1] On the Welcome App "Home" screen, tap " ".

[2] On the AccessControl screen, tap the designated "Electronic locking cylinder" to access the correspondng screen.

[3] Swiping the lock icon up to release the "Electronic locking cylinder".



Enable/disable "Office mode"

Please follow the steps below:

[1] On the Welcome App "Home" screen, tap " ".

[2] On the AccessControl screen, tap the designated "Electronic locking cylinder" to access the corresponding screen.

[3] Click "Office".

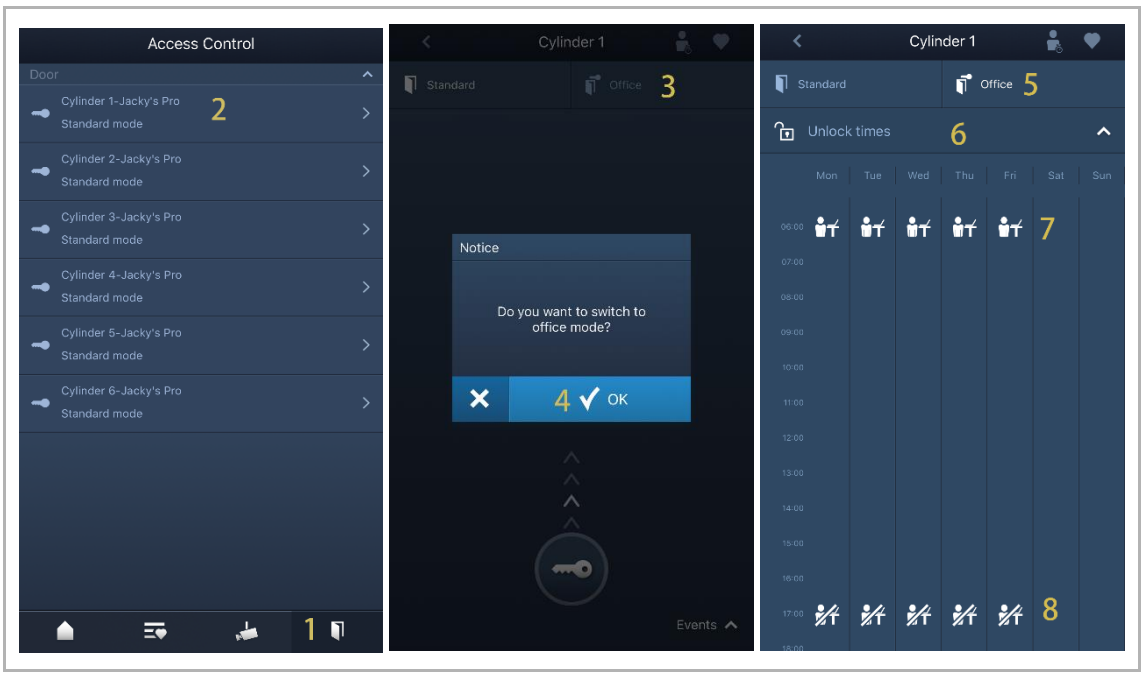
[4] Click "√" to confirm.

[5] Click "Office".

[6] Click "Unlock times".

[7] Office mode is enabled on the time.

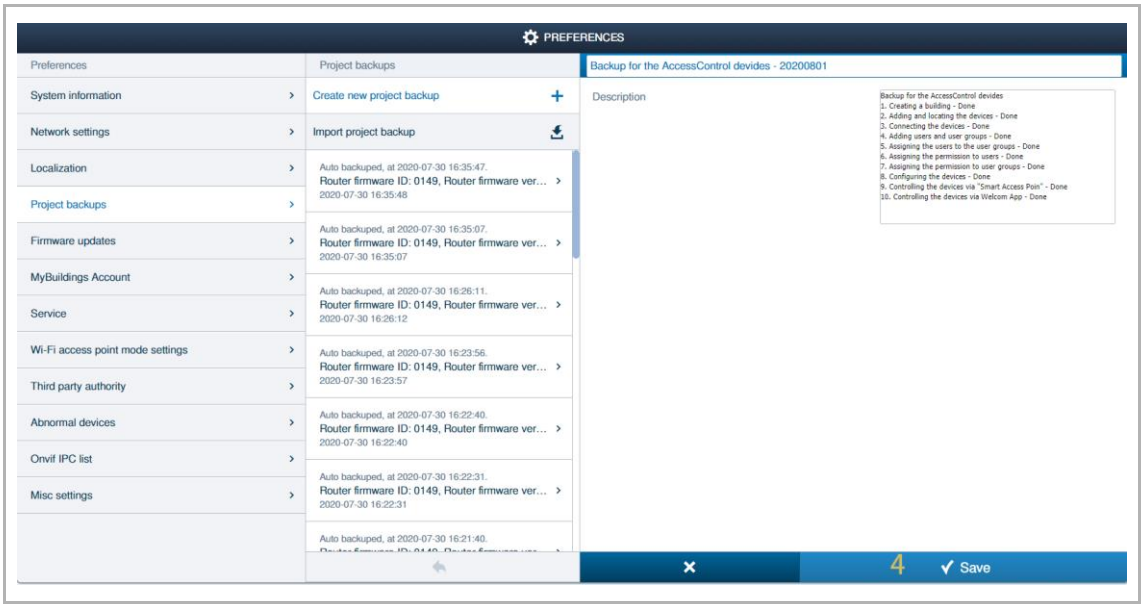
[8] Office mode is disabled on the time.



10.9 Managing the backup

It is important to create a backup regularly.

For more information, see chapter 13.5 “Managing the backup“ on page 326.



10.10 Removing permissions

10.10.1 Removing permissions for a user

1. Removing the "Electronic locking cylinder" from a user

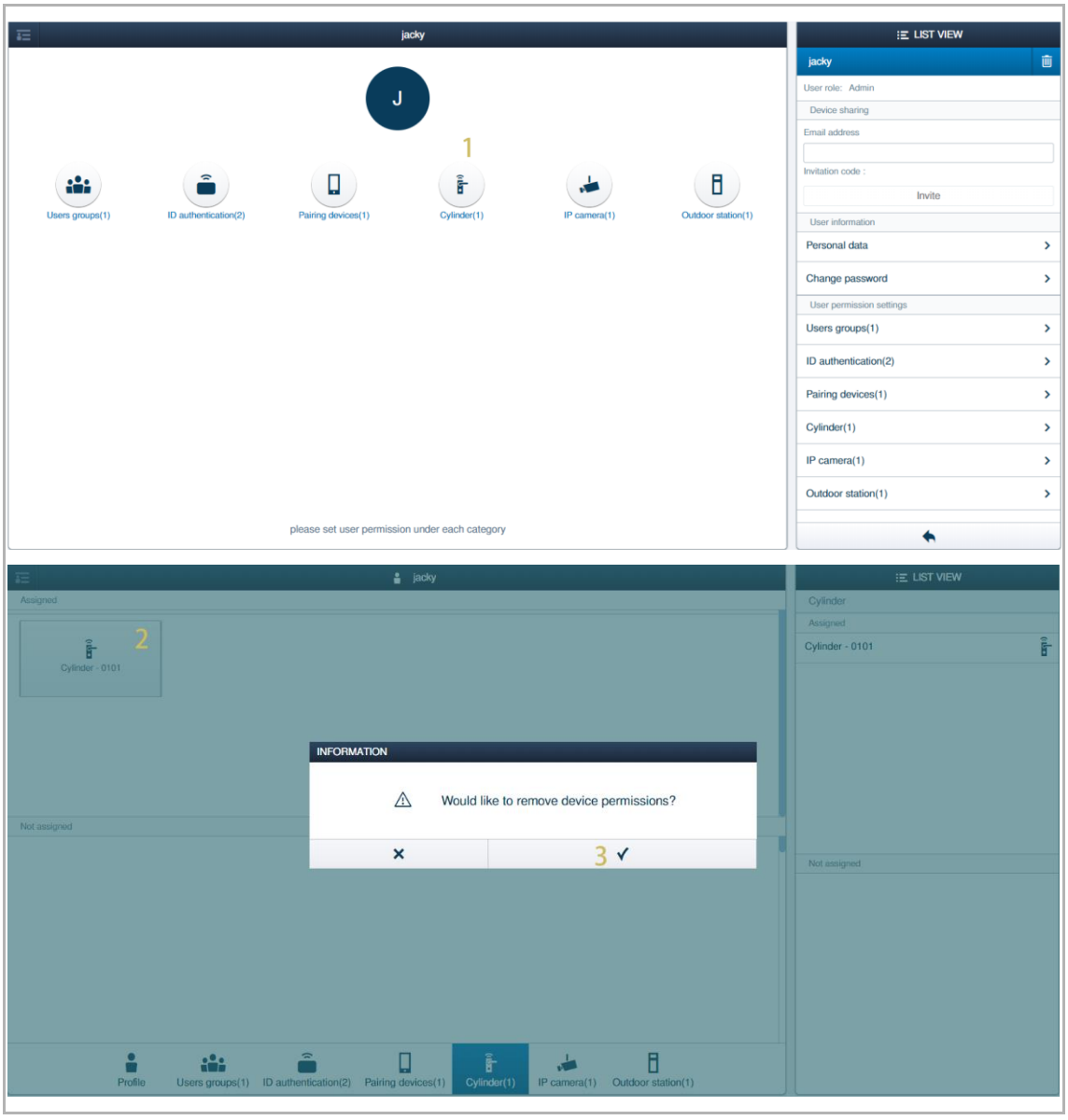
If you want the designated "Electronic locking cylinder" to be unusable for a user, please follow the steps below:

[1] On the designated user screen, click "Cylinder".

[2] Click the designated "Electronic locking cylinder" on the "Assigned" section.

[3] Click " √ " to confirm.

Repeat steps from 2-3 to remove the "Electronic locking cylinders" one by one.



2. Removing the designated ID authentications from a user

If you want the designated ID authentications to be unusable for a user, please follow the steps below:

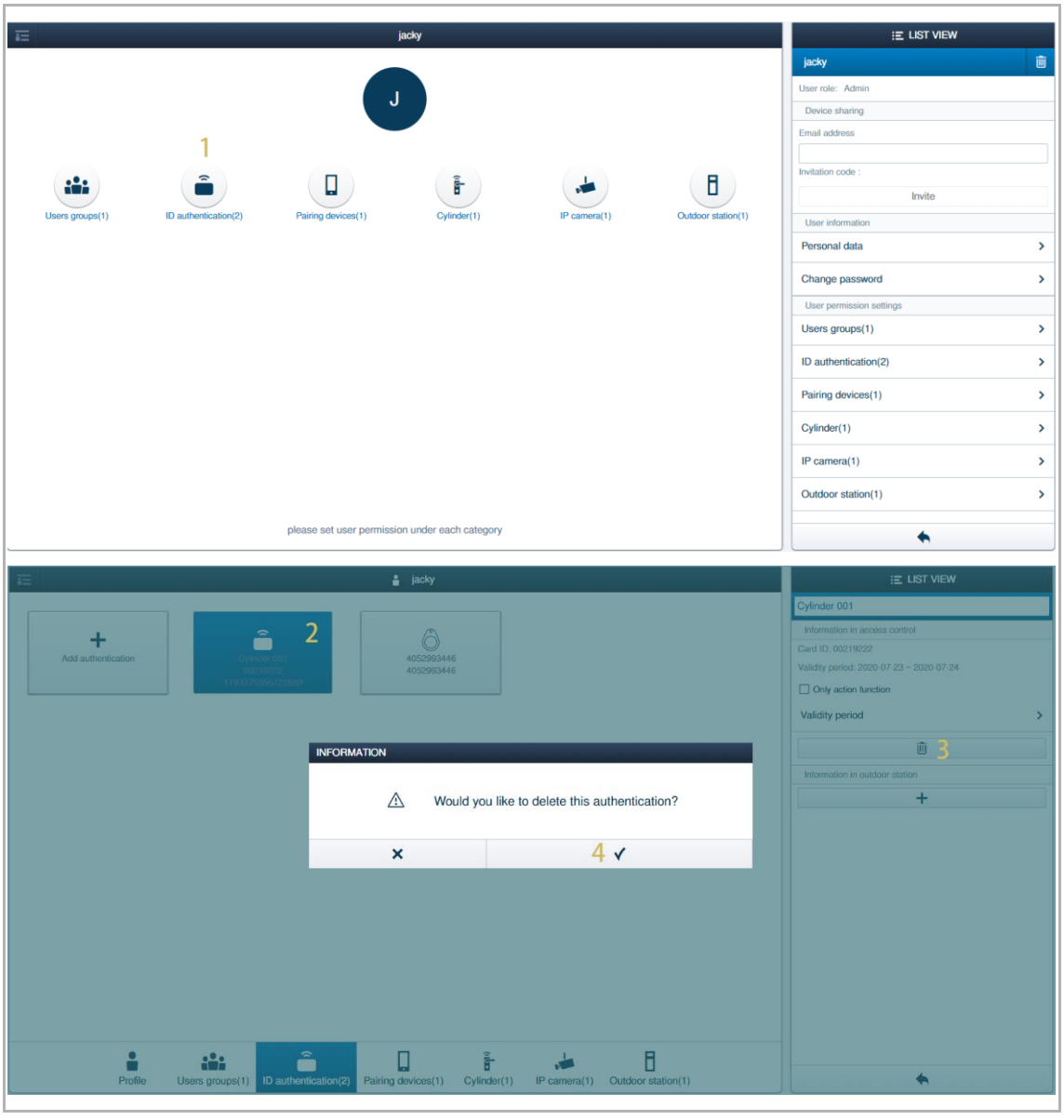
[1] On the designated user screen, click "ID authentication" to access the corresponding screen.

[2] Click the designated ID authentication.

[3] Click " " , if the card belongs to "Emergency card", please remove the emergency card first. see chapter 10.5.4 “Managing the emergency cards“ on page 220.

[4] Click " √ " to confirm.

Repeat steps from 2-4 to remove the ID authentications one by one.



10.10.2 Removing the permissions for the users in a group

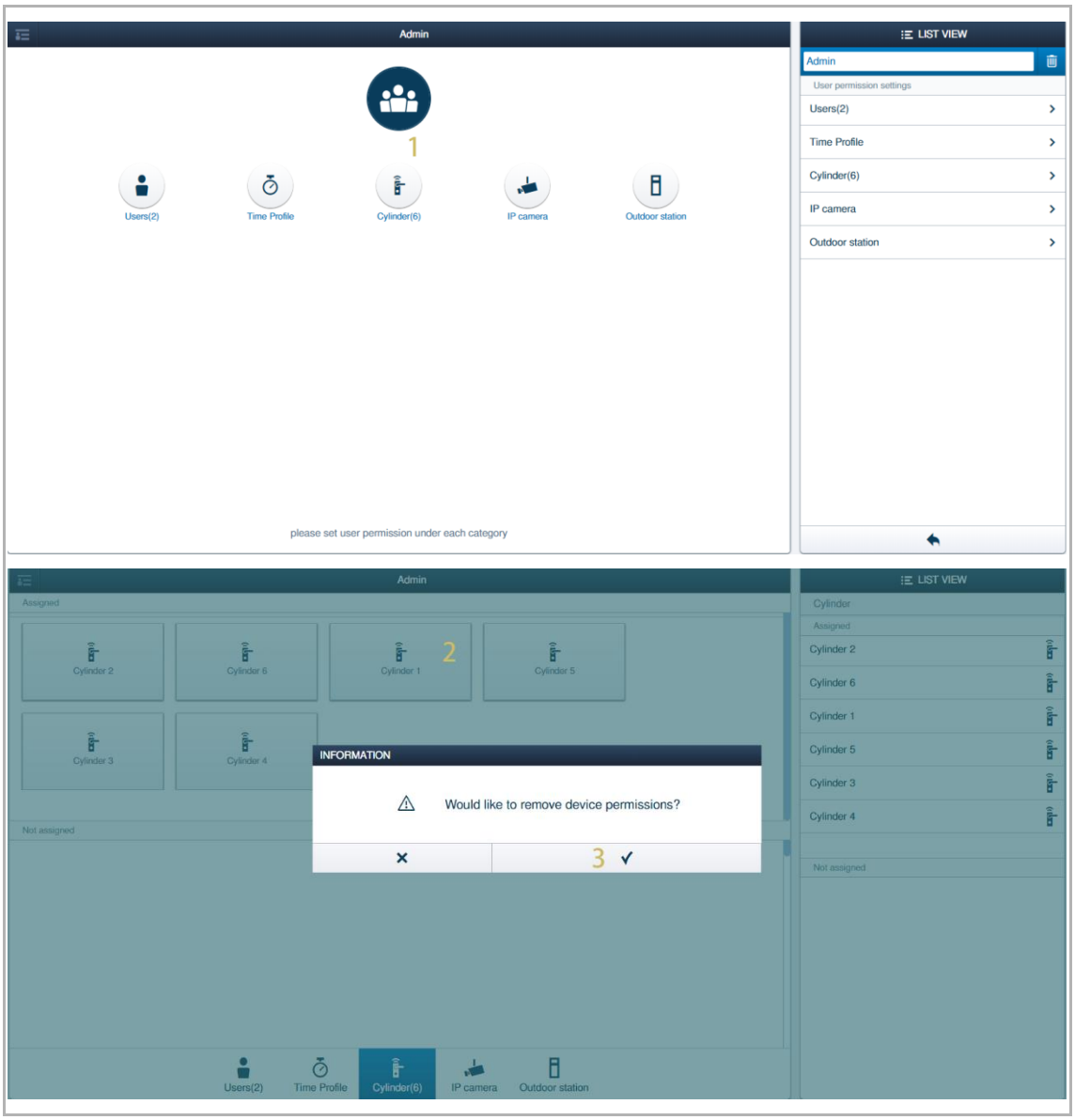
1. Removing the "Electronic locking cylinder" from a group

If you want the designated "Electronic locking cylinder" to be unusable for all users in the group, please follow the steps below:

[1] On the designated group screen, click "Cylinder".

[2] Click the designated "Electronic locking cylinder" in the "Assigned" section.

[3] Click " √ " to confirm.



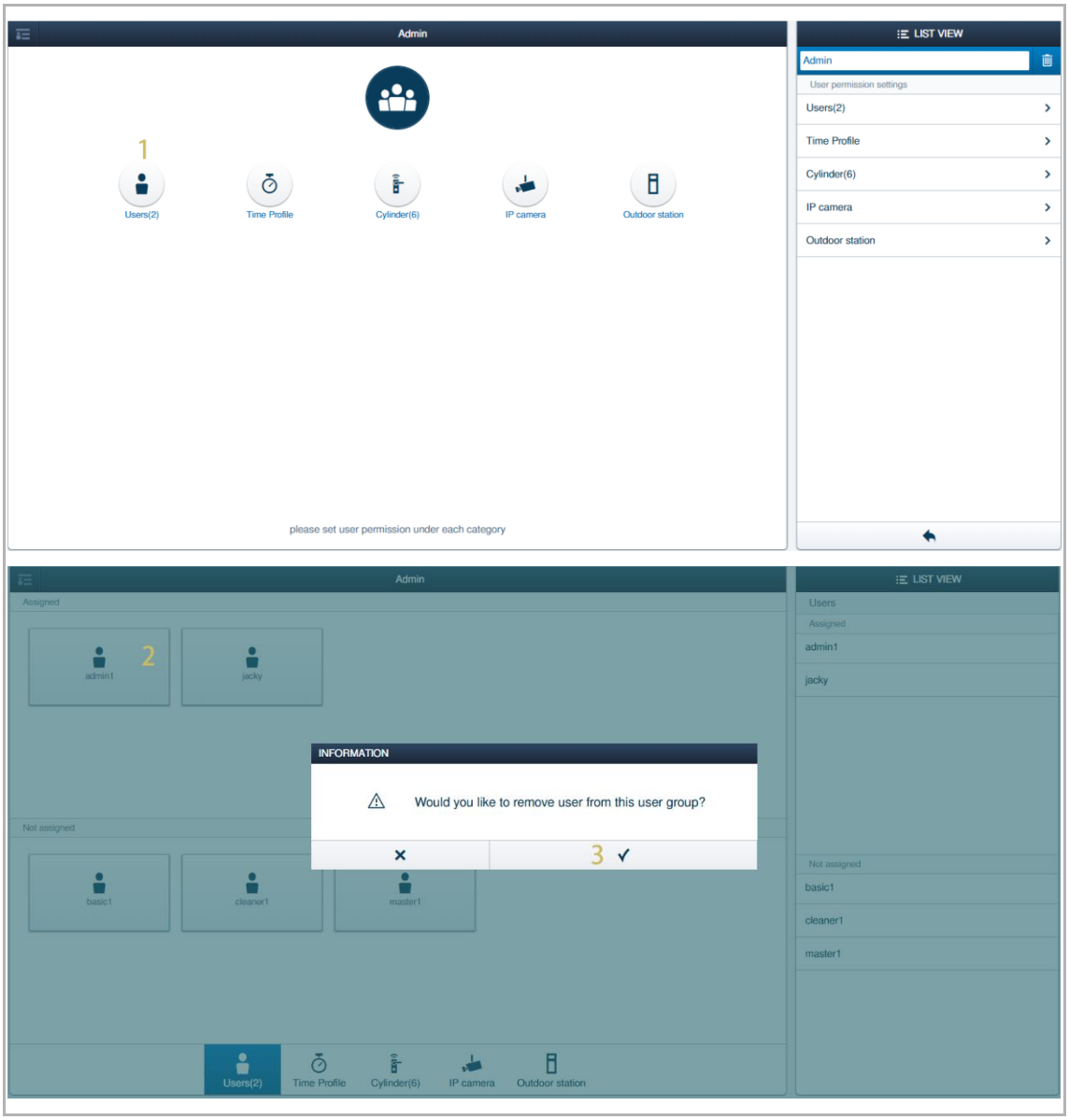
2. Removing designated users from the user group

If you want the "Electronic locking cylinder" to be unusable for some designated users in the group, please follow the steps below:

[1] On the designated group screen, click "User".

[2] Click the designated user on the "Assigned" section.

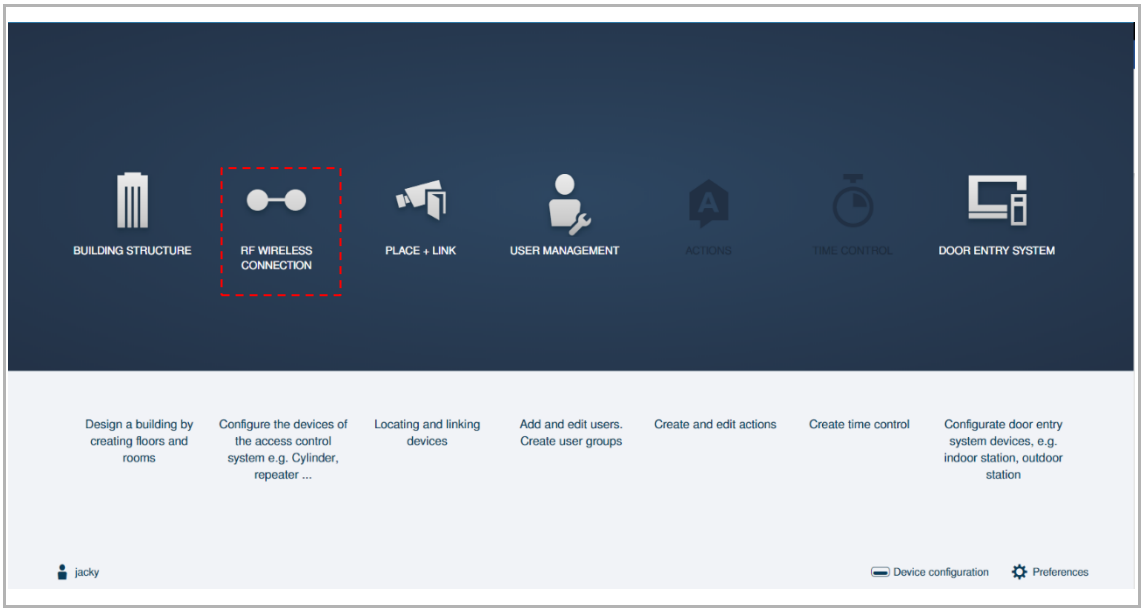
[3] Click " √ " to confirm.



10.11 Disconnecting the devices

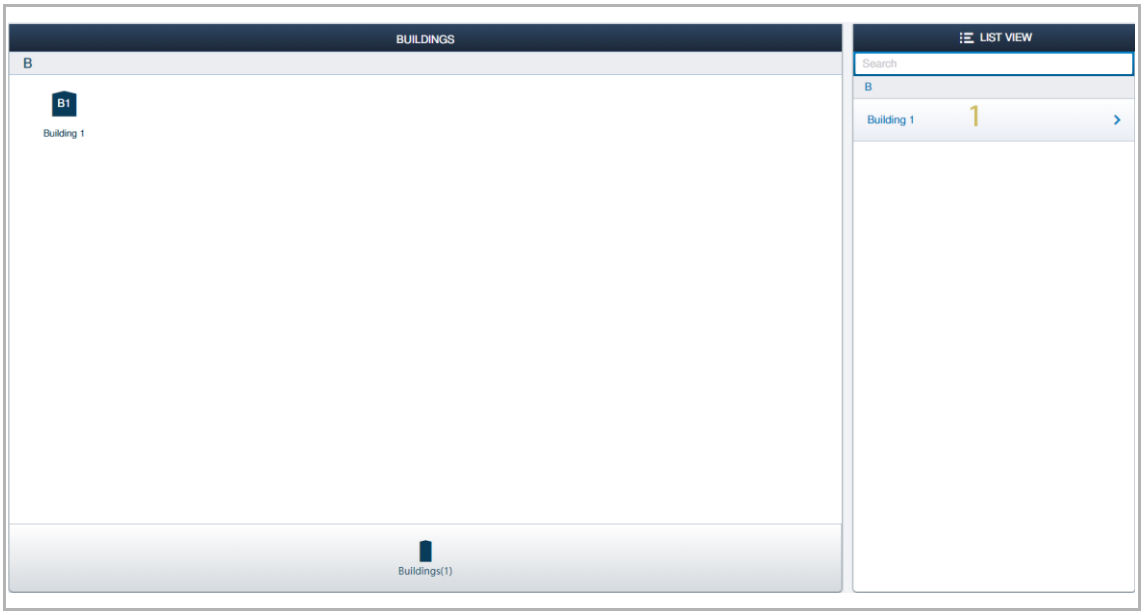
Accessing the RF connections screen

On the configuration screen, click "RF Wireless connection" to access the corresponding screen.

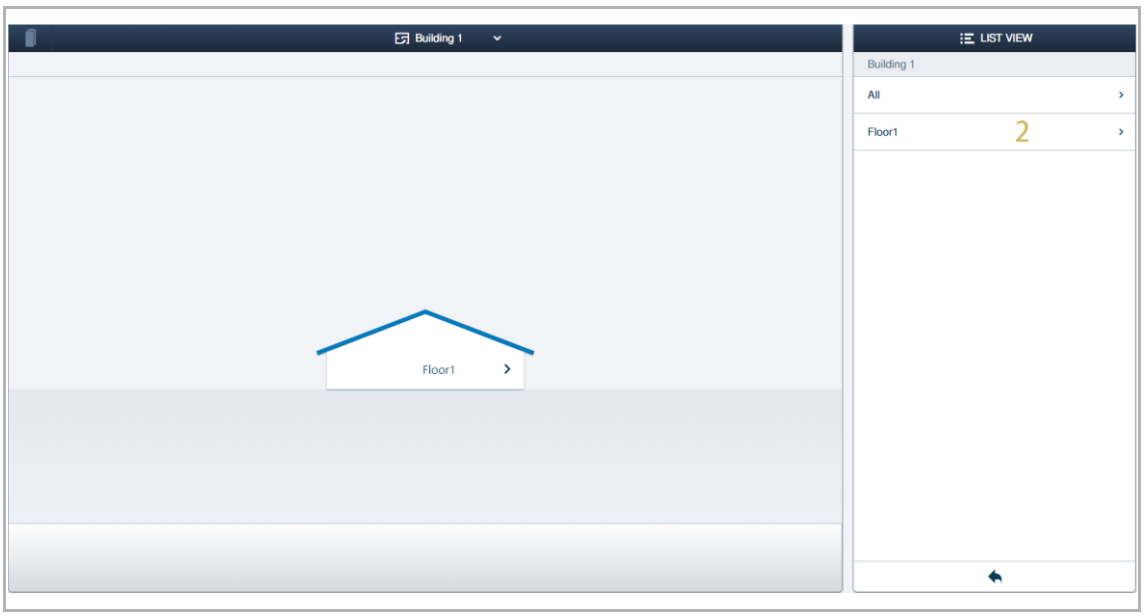


Please follow the steps below:

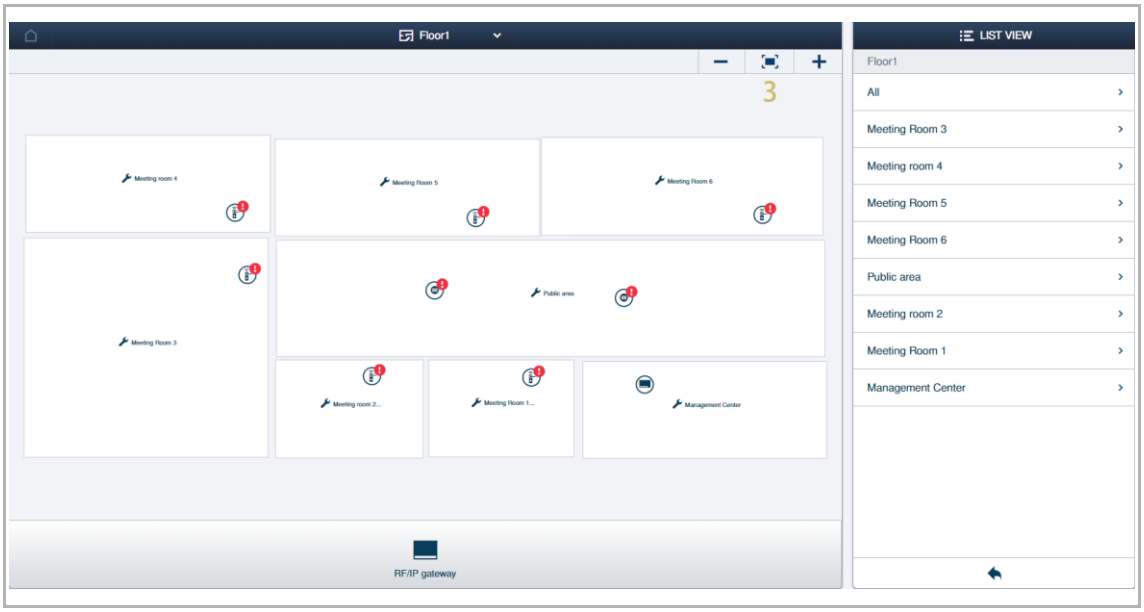
[1] On the "Buildings" screen, click the designated building (e.g. "Building 1" for demo case 1).



[2] Click the designated floor (e.g. "Floor 1" for demo case 1).



[3] Click " " to view all the devices on the floor screen, you can move the icons to a suitable postion by dragging them.



Disconnecting the AccessControl devices in a sequence

Please disconnect the AccessControl devices in a radio line according to the following sequence:

[1] Disconect the "Electronic locking cylinder" with its parent devices.

[2] Disconnect the "RF Repeater" with its parent devices.

10.11.1 Disconnecting "Electronic locking cylinders"

Attention!

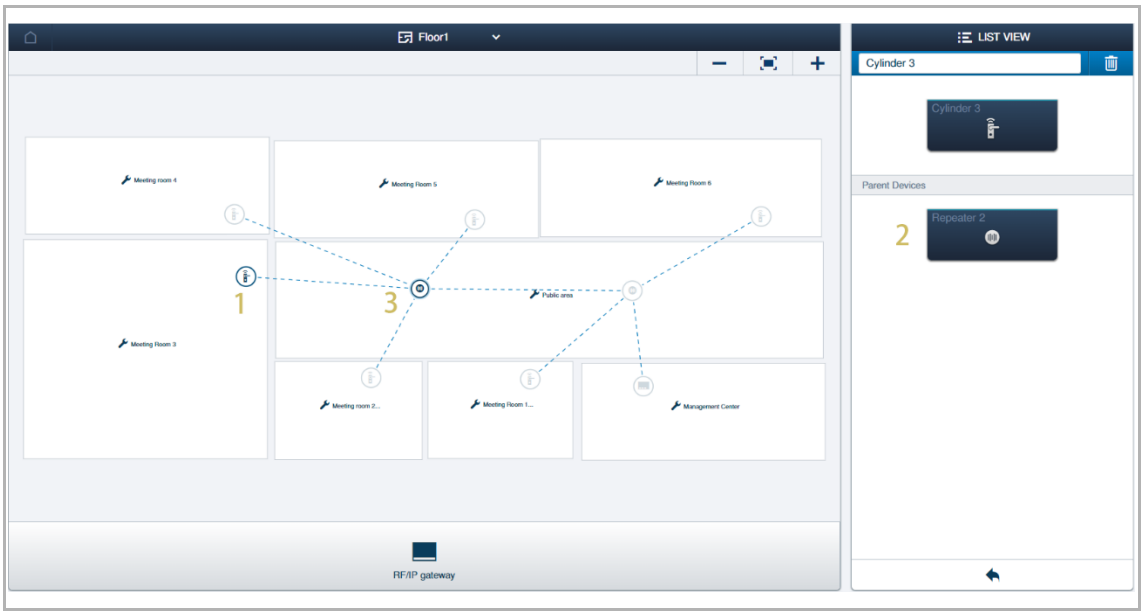
It is recommended the "Electronic locking cylinder" to be unpaired when online. If the "Electronic locking cylinder" is unpaired when online, it can be used normally in other system. If it is forcibly unpaired when offline, it can only be used in current system and cannot be used in other system. see chapter 10.4.3 “AccessControl device is offline“ on page 211.

Please follow the steps below:

[1] On the floor screen, click an "Electronic locking cylinder" (e.g. "Cylinder 3" for demo case 1).

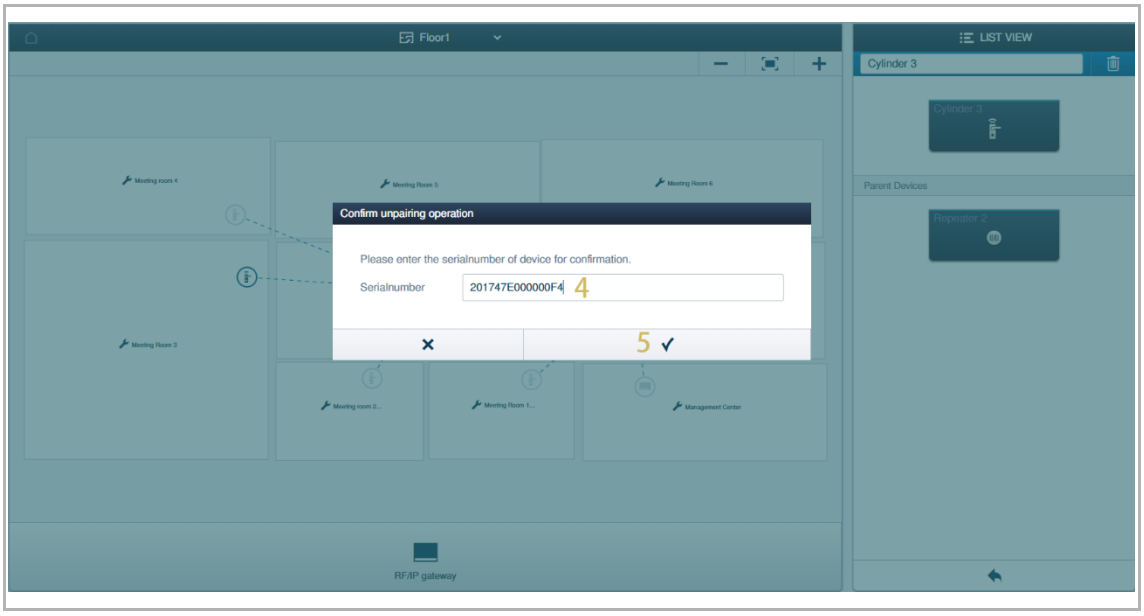
[2] Its parent device is displayed on the list.

[3] Click its parent device (e.g. "Repeater 2" for demo case 1).

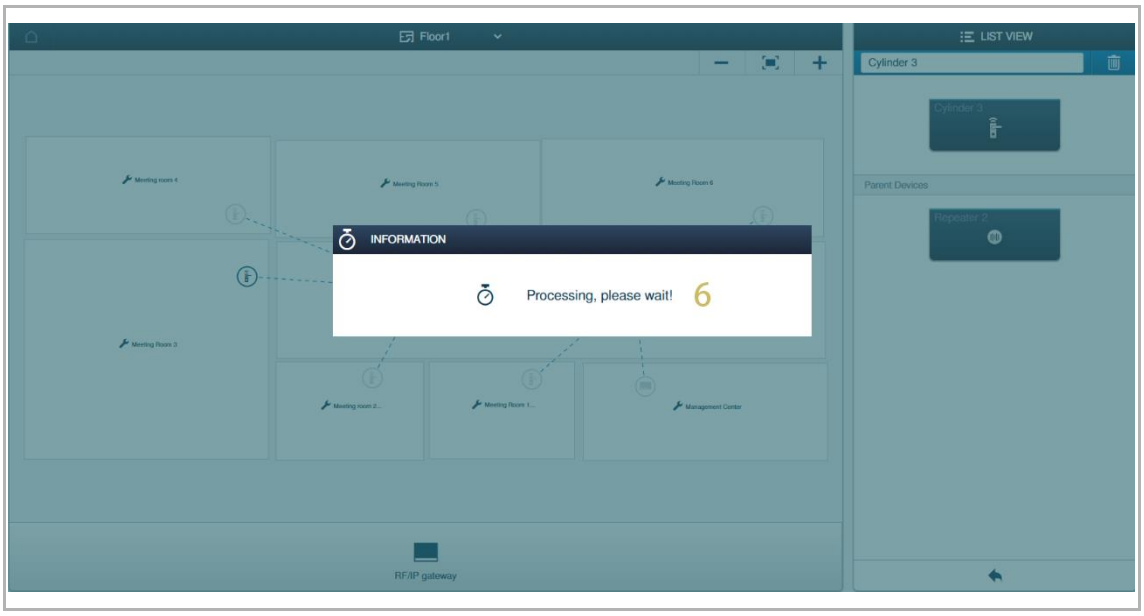


[4] Enter the serial number of the "Electronic locking cylinder".

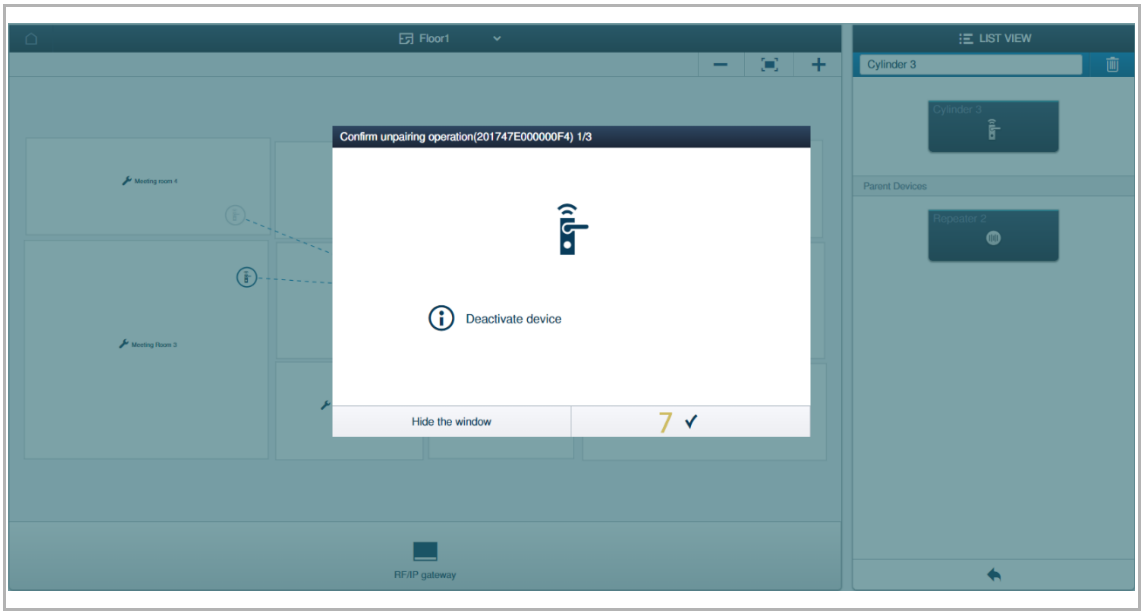
[5] Click " √ " to confirm.



[6] Wait for the pairing process.

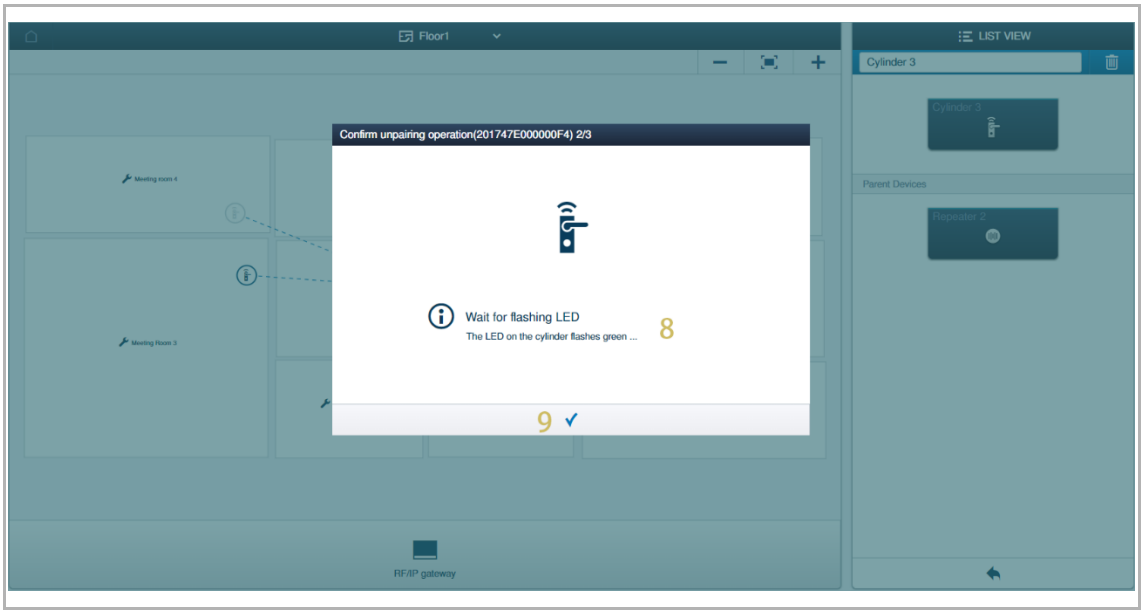


[7] Click " √ " to continue.



[8] Wait for the LED on the "Electronic locking cylinder" to flash green or sound a beep.

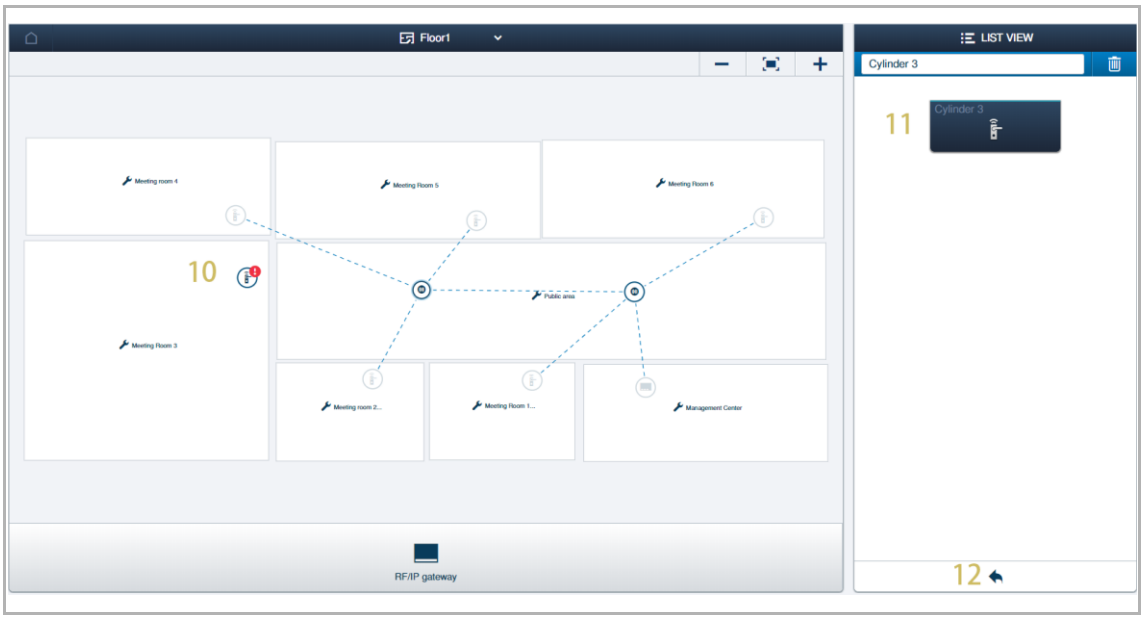
[9] Click " √ " to continue.



[10]No dashed line is displayed between the two devices.

[11]No parent device is displayed on the list.

[12]Click " " to turn back to the floor screen.



10.11.2 Disconnecting "RF Repeaters"

Attention!

The "RF Repeater" needs to be restore to factory default settings before being use in other system by holding the reset button for 3 seconds. see chapter 10.4.3 “AccessControl device is offline“ on page 211.

Attention!

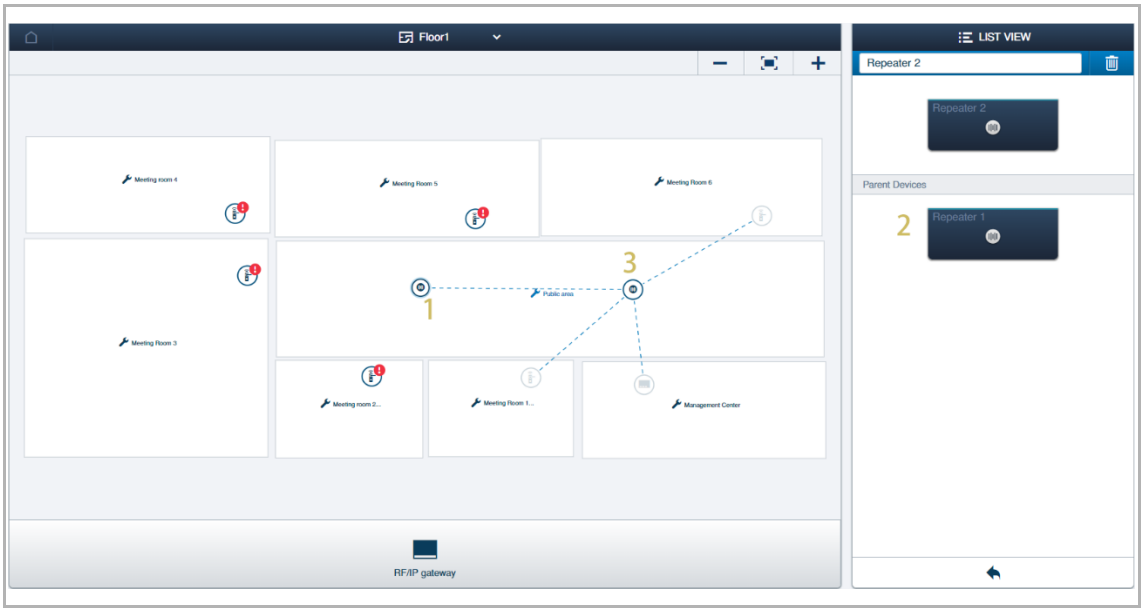
The "RF Repeater" to be unpaired cannot have slave devices!

Please follow the steps below:

[1] On the floor screen, click a "RF Repeater" (e.g. "Repeater 2" for demo case 1).

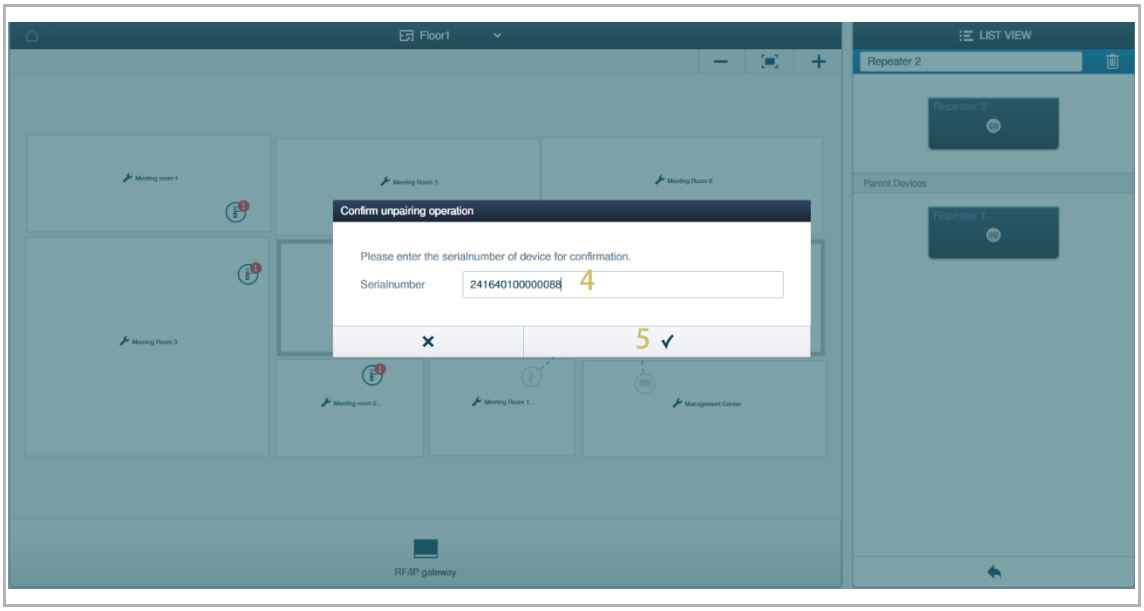
[2] Its parent device is displayed on the list.

[3] Click its parent device (e.g. "Repeater 1" fore demo case 1).

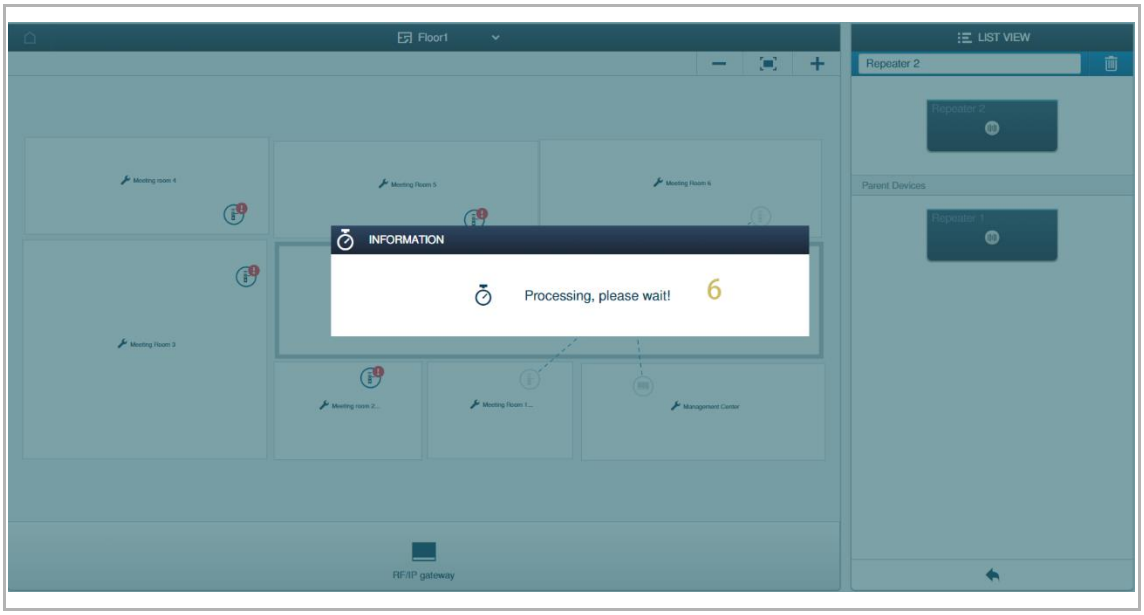


[4] Enter the serial number of the "RF Repeater" (e.g. "Repeater 2" for demo case 1).

[5] Click " √ " to confirm.



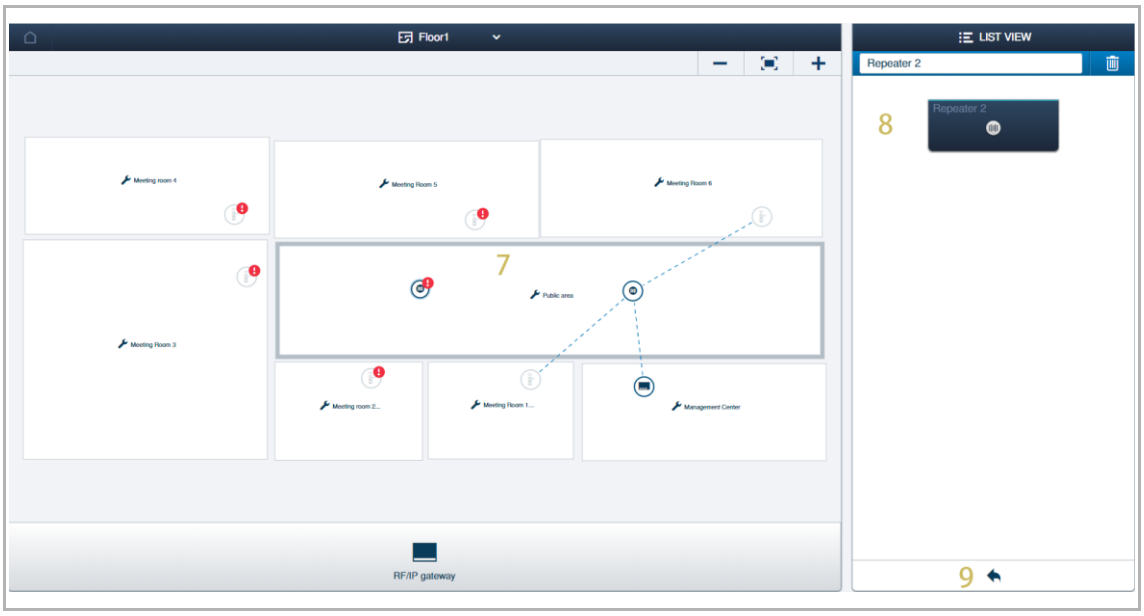
[6] Wait for the pairing process.



[7] No dashed line is displayed between the two devices.

[8] No parent device is displayed on the list.

[9] Click " " to turn back to the floor screen.



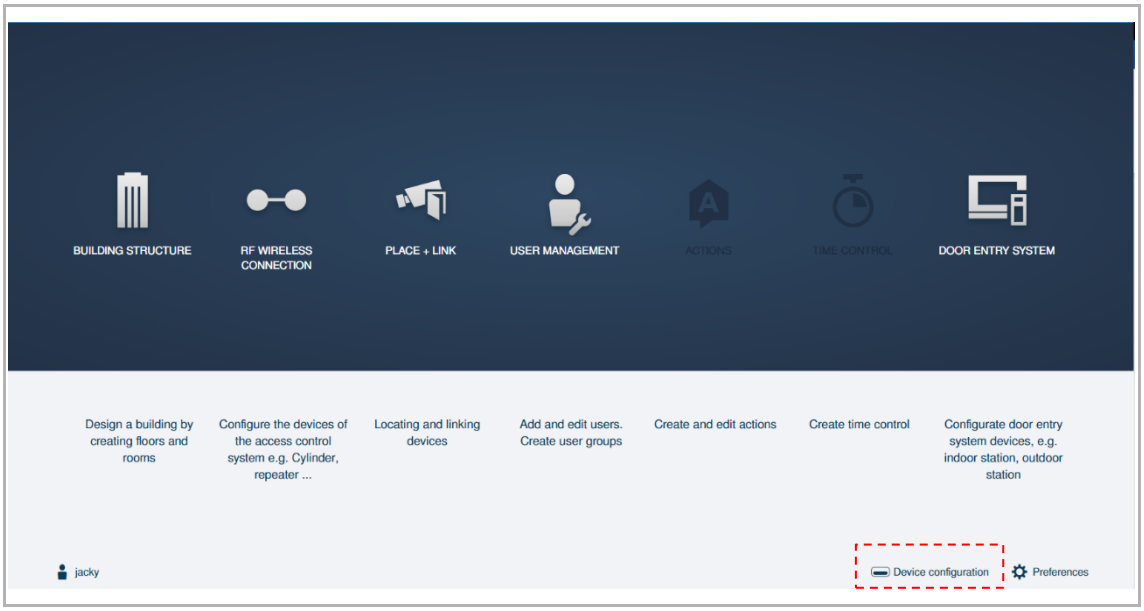
10.12 Removing the devices

Note

The AccessControl device cannot be deleted if it is paired. Please unpair it first.
see chapter 10.11 “Disconnecting the devices“ on page 259.

Accessin the "Device configuration" screen

On the configuration screen, click "Device configuration" to access the corresponding screen.



10.12.1 Removing "Electronic locking cylinders"

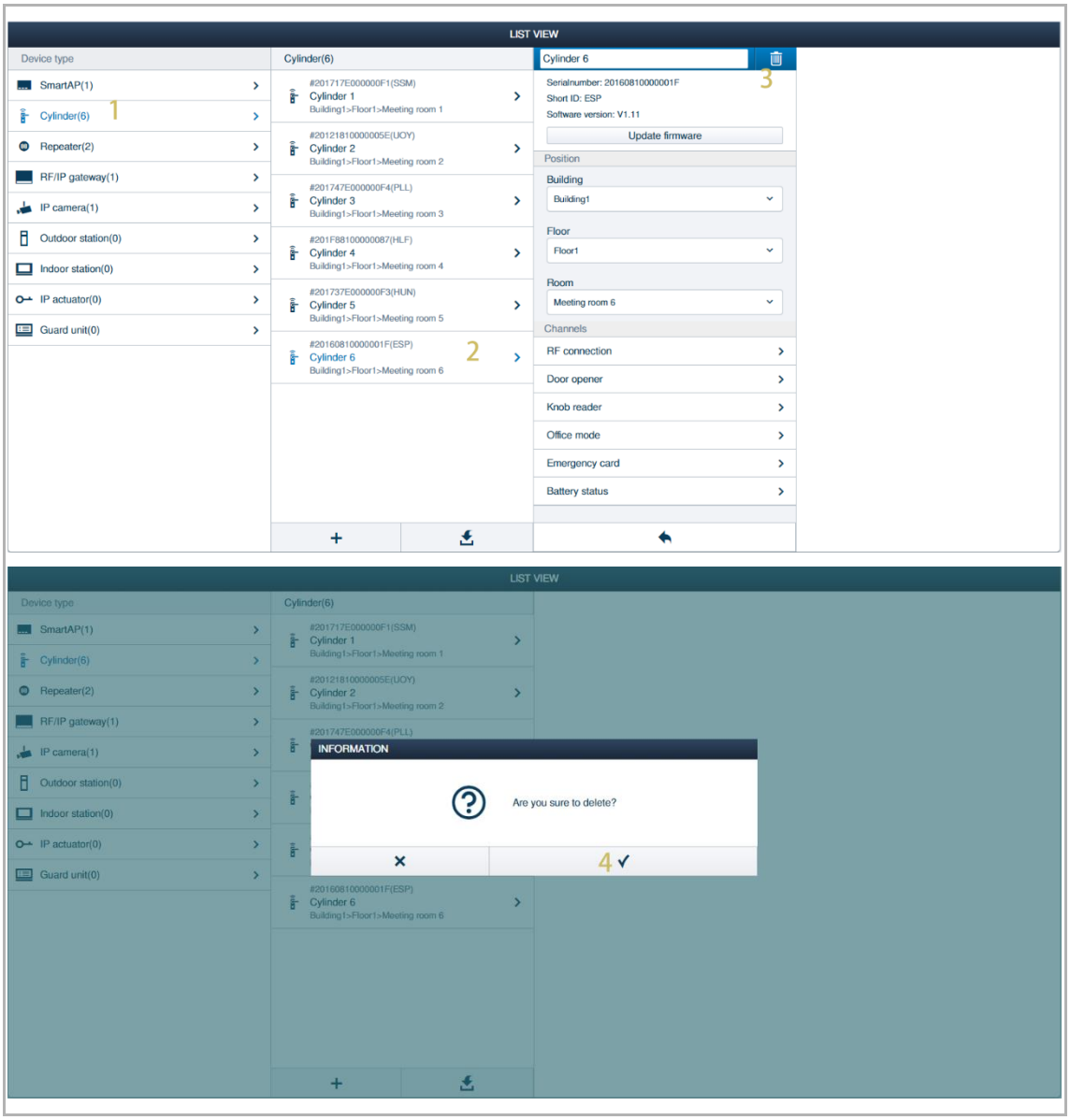
Please follow the steps below:

[1] On the "Device configuration" screen, click "Cylinder".

[2] Click the designated "Electronic locking cylinder" (e.g. "Cylinder 6").

[3] Click "  ".

[4] Click " √ " to confirm.



10.12.2 Removing "RF Repeaters"

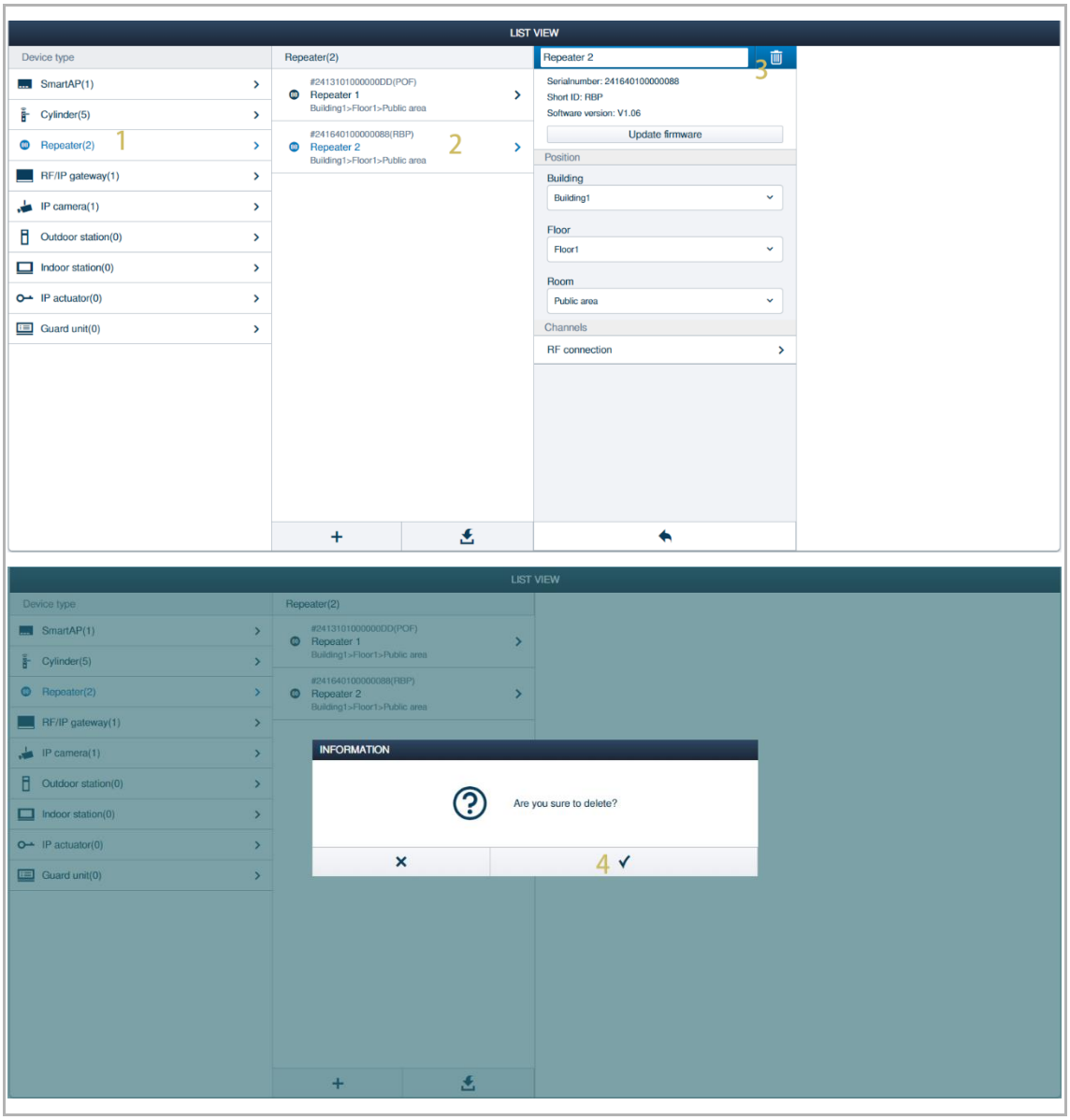
Please follow the steps below:

[1] On the "Device configuration" screen, click "Repeater".

[2] Click the designated "RF Repeater" (e.g. "Repeater 2").

[3] Click "  ".

[4] Click " √ " to confirm.



10.12.3 Removing "RF/IP Gateways"

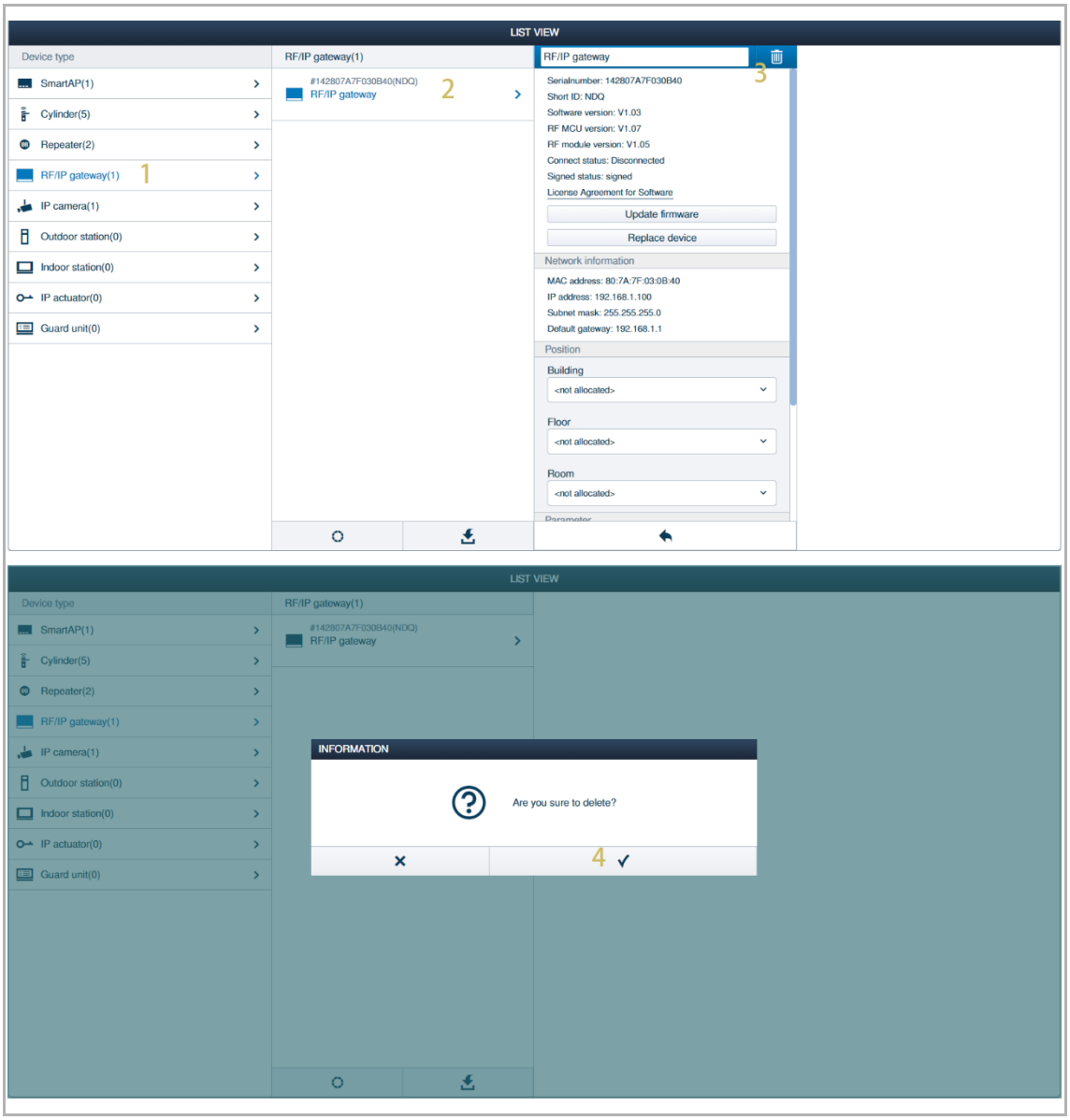
Please follow the steps below:

[1] On the "Device configuration" screen, click "RF/IP Gateway".

[2] Click the designated "RF/IP Gateway".

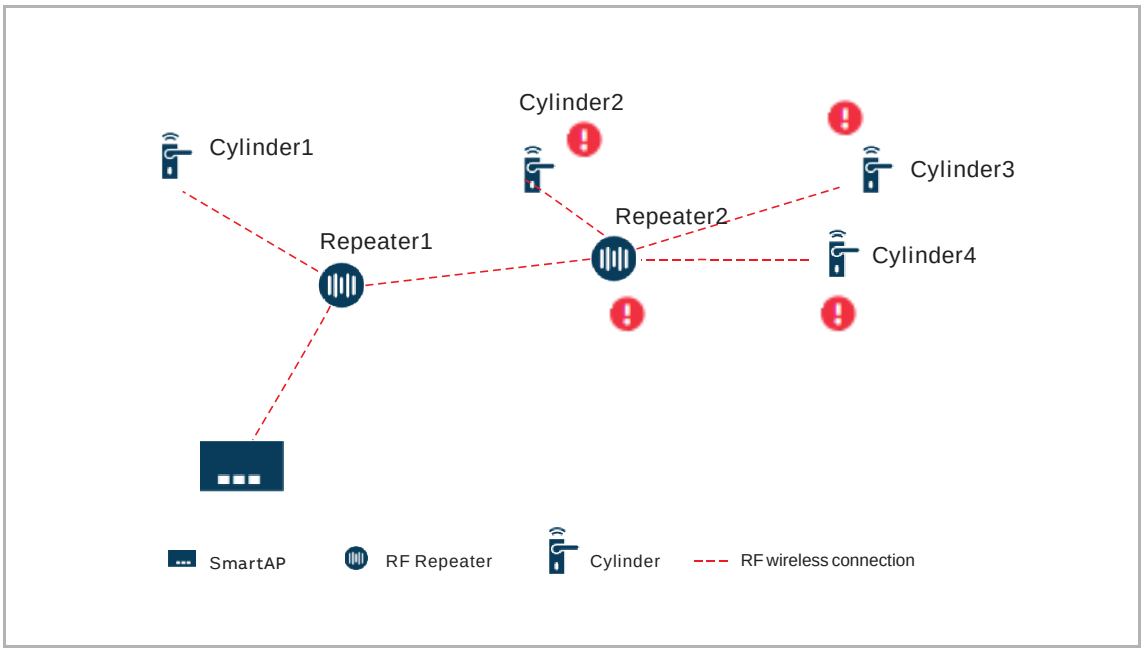
[3] Click " " ".

[4] Click " √ " to confirm.



10.13 Replacing the damaged "RF Repeater"

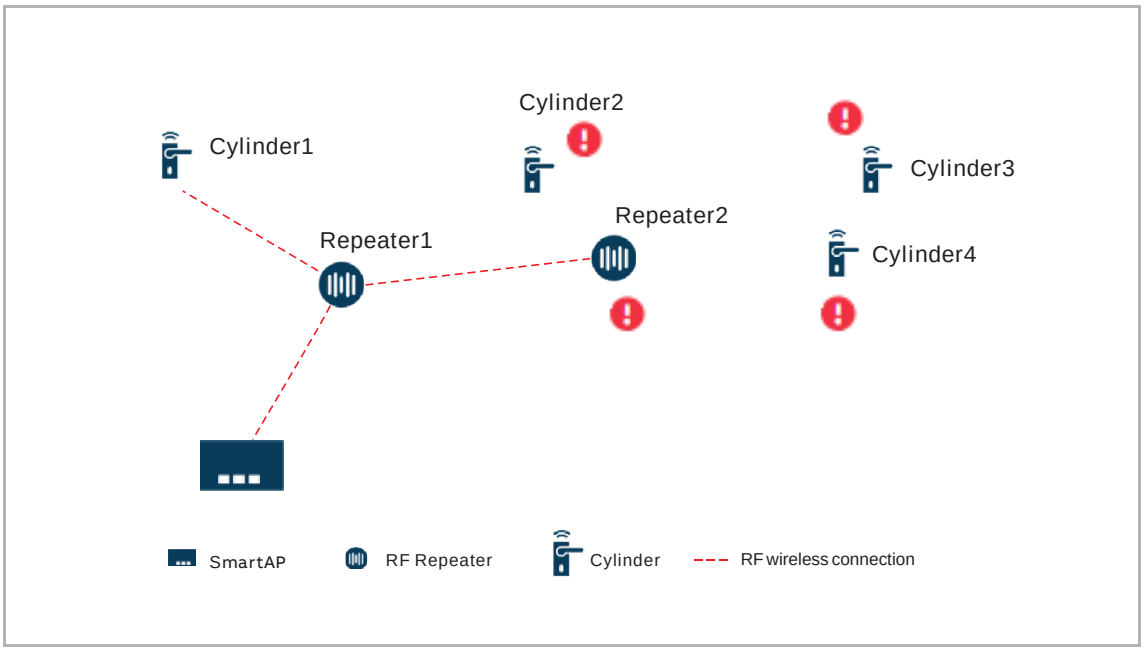
If a "RF Repeater" is damaged (e.g. "Repeater2" is damaged on the below diagram), all "RF Repeaters" and all "Electronic locking cylinders" paired to it will be offline. A new "RF Repeaters" (e.g. "Repeater3") needs to be used to replace the damaged "RF Repeaters".



Please follow the steps below:

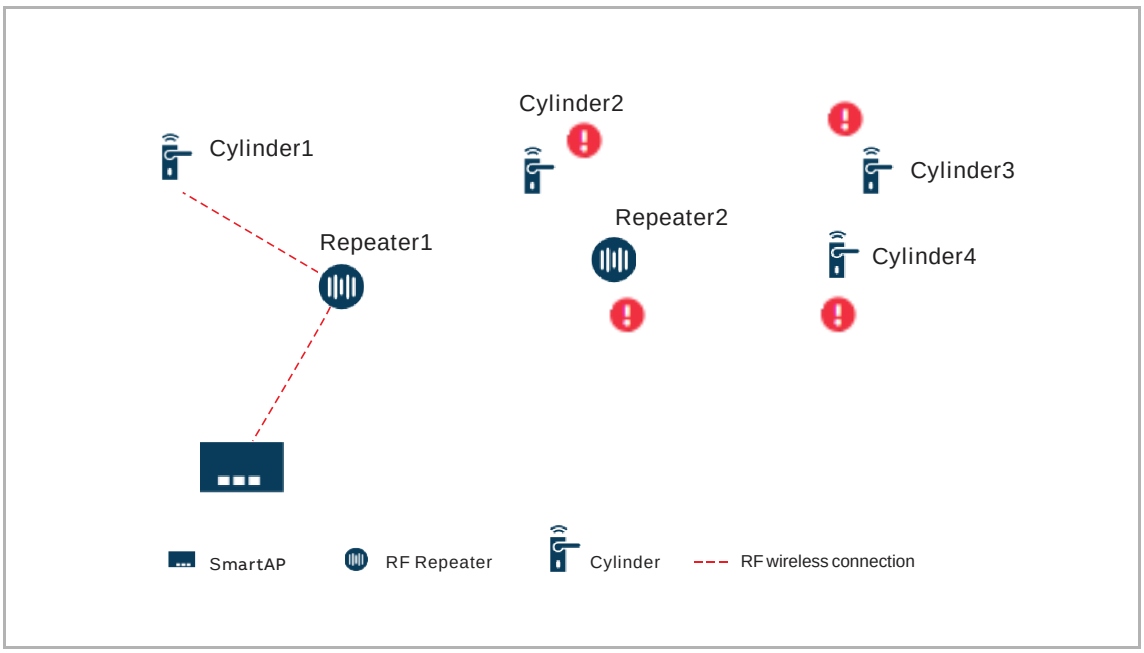
[1] Forcibly unpair the cylinders connected to the damaged "RF Repeater".

see chapter 10.11.1 “Disconnecting "Electronic locking cylinders"“ on page 261



[2] Forcibly unpair the damaged "RF Repeater" from its parent device.

see chapter 10.11.2 “Disconnecting "RF Repeaters"“ on page 265



[3] Remove the damaged "RF repeater" from the device list

see chapter 10.12.2 “Removing "RF Repeaters"“ on page 270

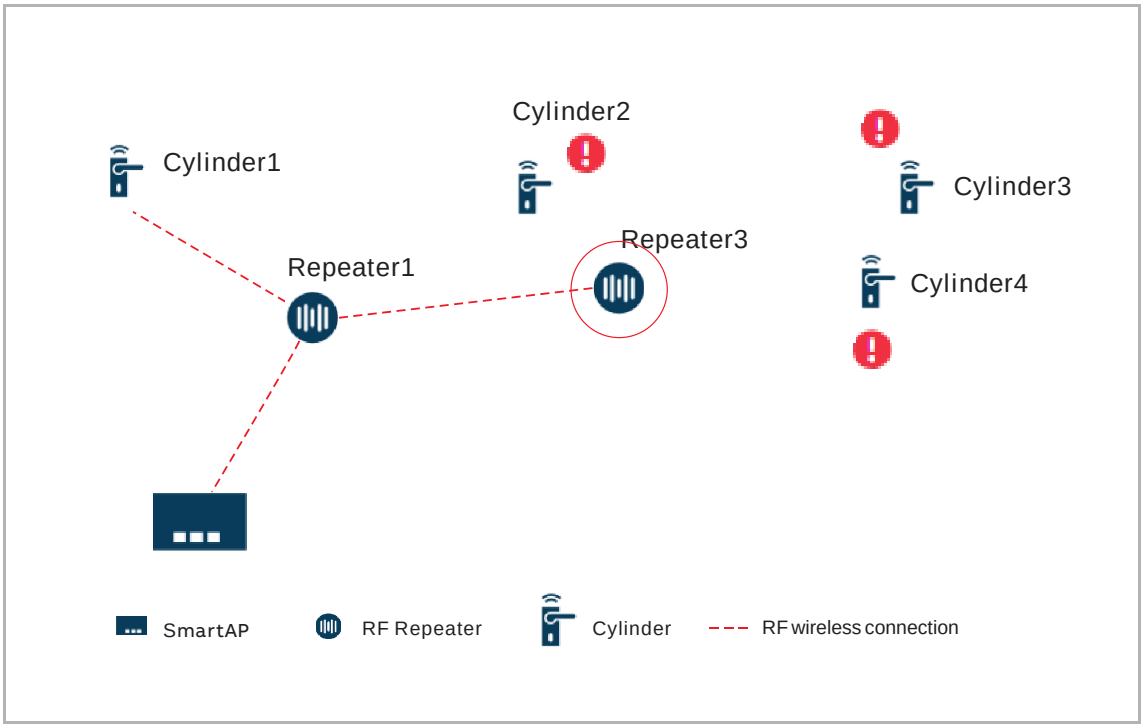
[4] Add a new "RF Repeater"

see chapter 10.3.3 “Adding and locating "RF Repeaters"“ on page 201

[5] Connect the new "RF Repeater" to its parent device

New "RF Repeater" should be restore to factory default settings (holding the reset button for 3 seconds and LED light red if success) before connecting.

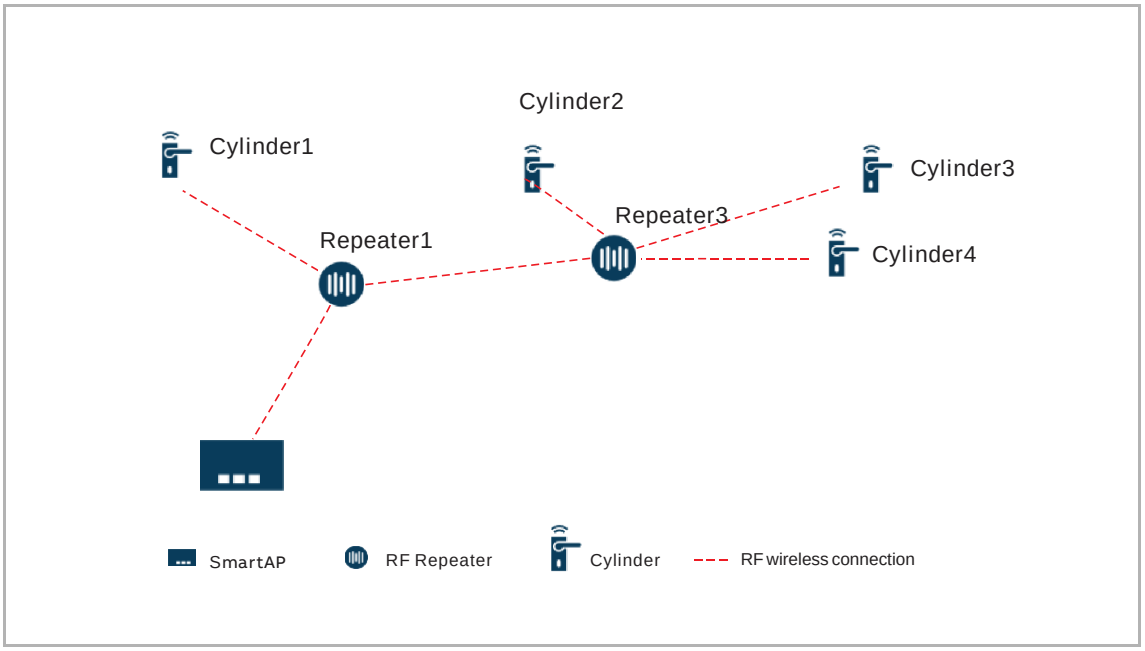
see chapter 10.4.1 “Connecting "RF Repeaters"“ on page 205



[6] Connect the "Electronic locking cylinders" to this new "RF Repeater"

The "Electronic locking cylinders" need to swipe the maintenance card during the process to connect to its parent device.

see chapter 10.4.2 “Connecting "Electronic locking cylinders"“ on page 207



10.14 Managing the link between the devices

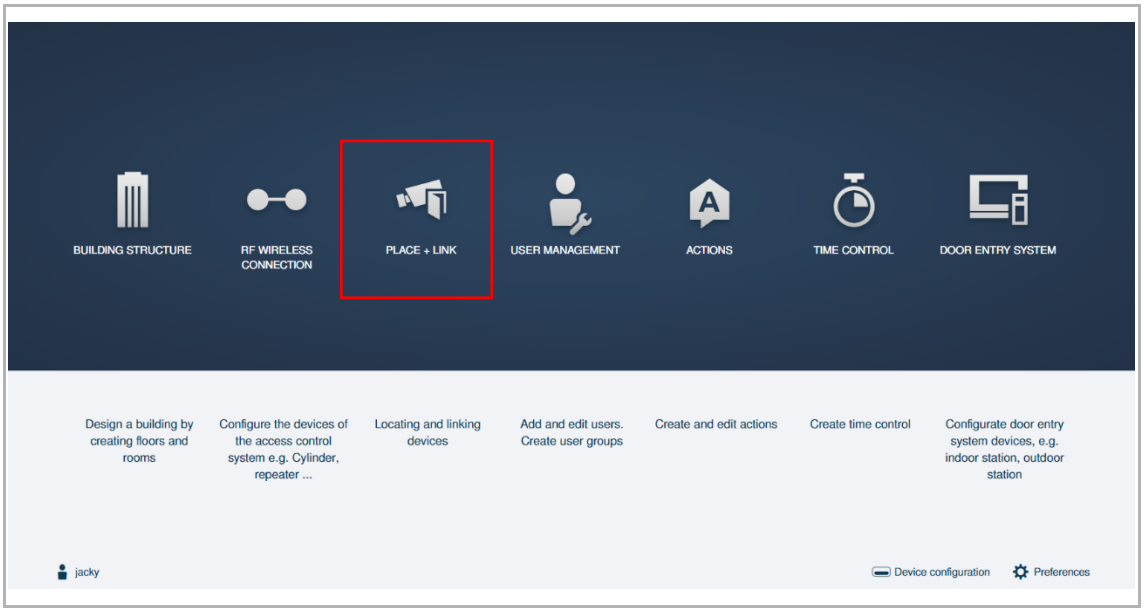
On "Smart Access Point", 2 AccessControl devices can be linked together. When one is triggered, the other can output an action.

Demo case

In this case, when the "Office mode" of the designated "Electronic locking cylinder" is activated, the doorbell of "Smart Access Point" rings.

Access the floor plan screen

On the configuration screen, click "Place + Link", "Building 1", "Floor 1" to access the floor plan screen.



10.14.1 Adding the link

Following operations are based on demo case. see chapter 10.1 “AccessControl topology“ on page 183.

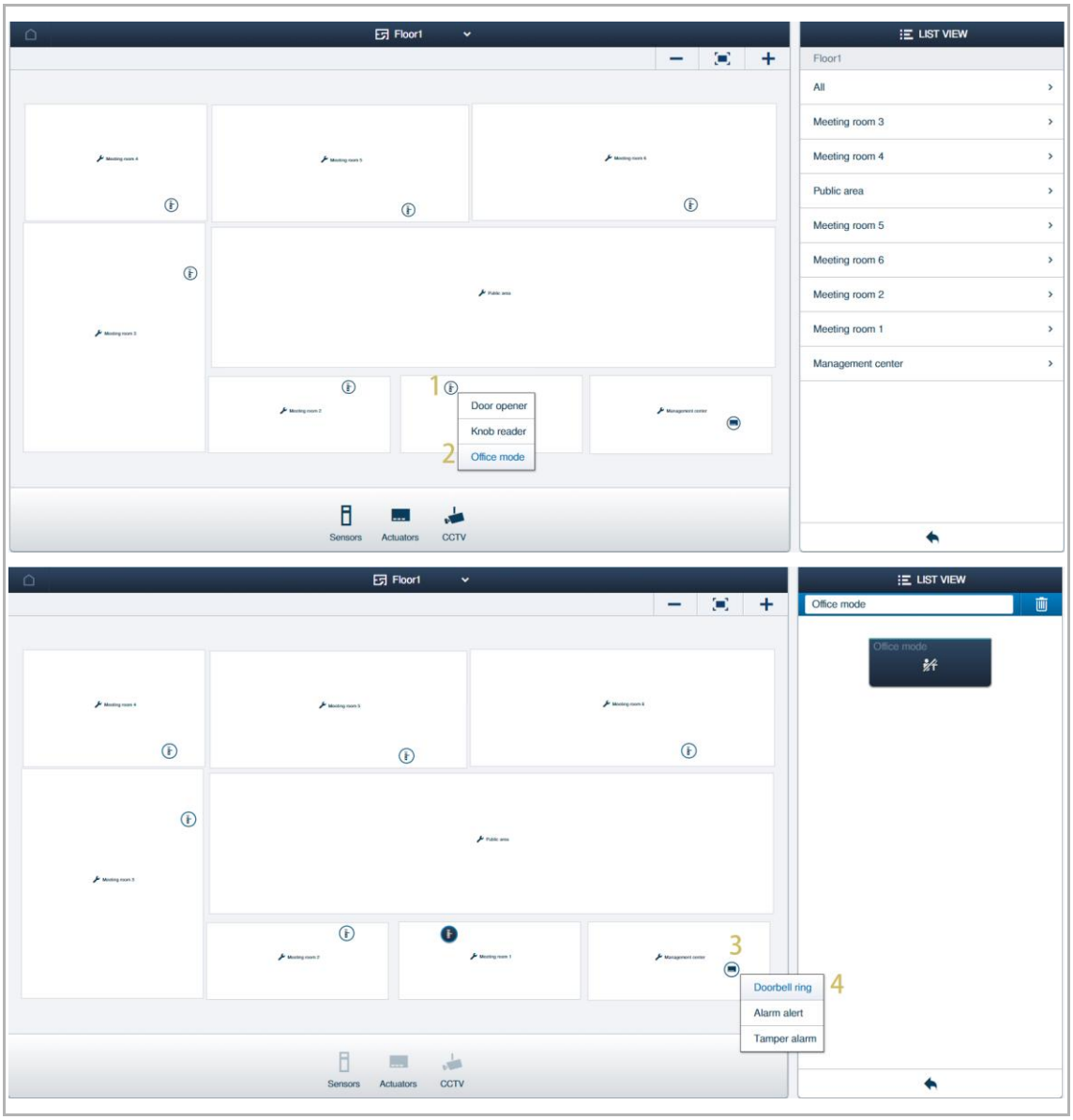
Please follow the steps below:

[1] On the floor plan screen, click the designated "Electronic locking cylinder".

[2] Click "Office mode".

[3] Click "Smart Access Point".

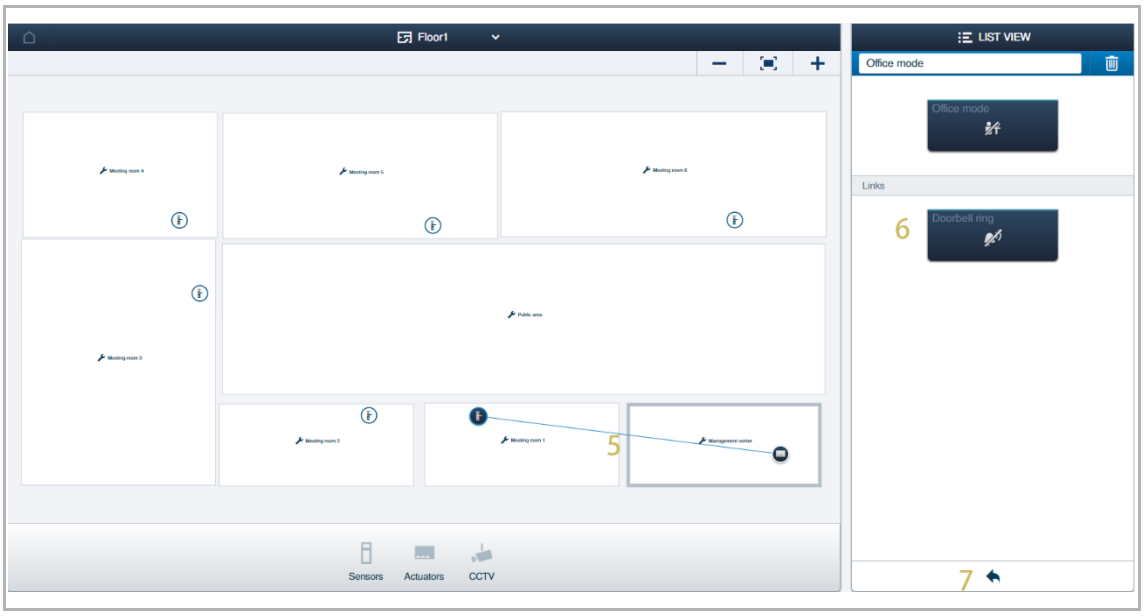
[4] Click "Doorbell ring".



[5] Pairing between the two devices is indicated by a line if successful.

[6] Linked device is displayed on the list.

[7] Click " " to turn back to the floor screen.



10.14.2 Managing the link

Please follow the steps below:

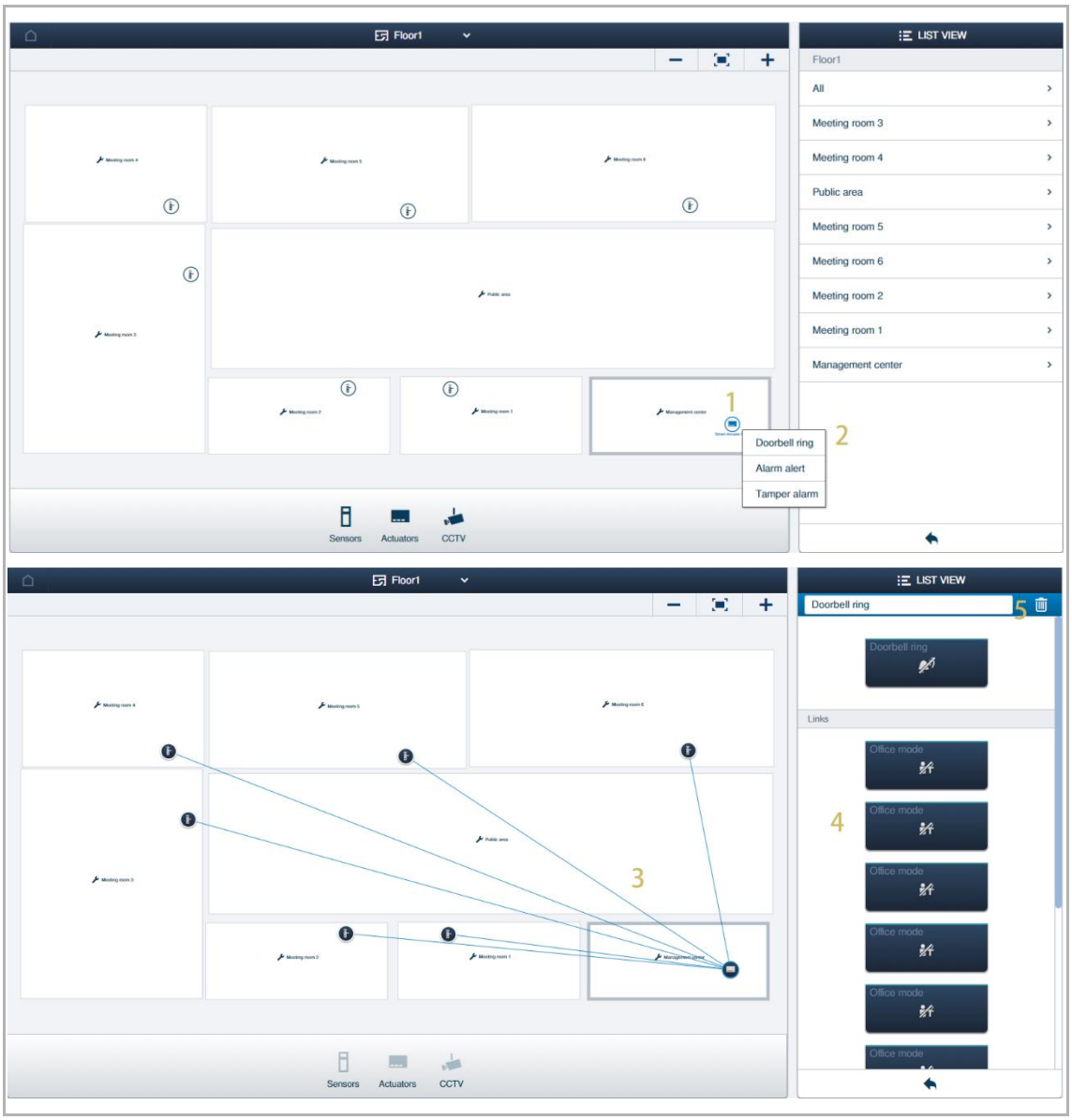
[1] On the floor plan screen, click "Smart Access Point".

[2] Click "Doorbell ring".

[3] The links are displayed on the floor plan.

[4] The linked devices are also displayed on the list.

[5] The channel cannot be removed if it has more than 2 links.



10.14.3 Removing the link

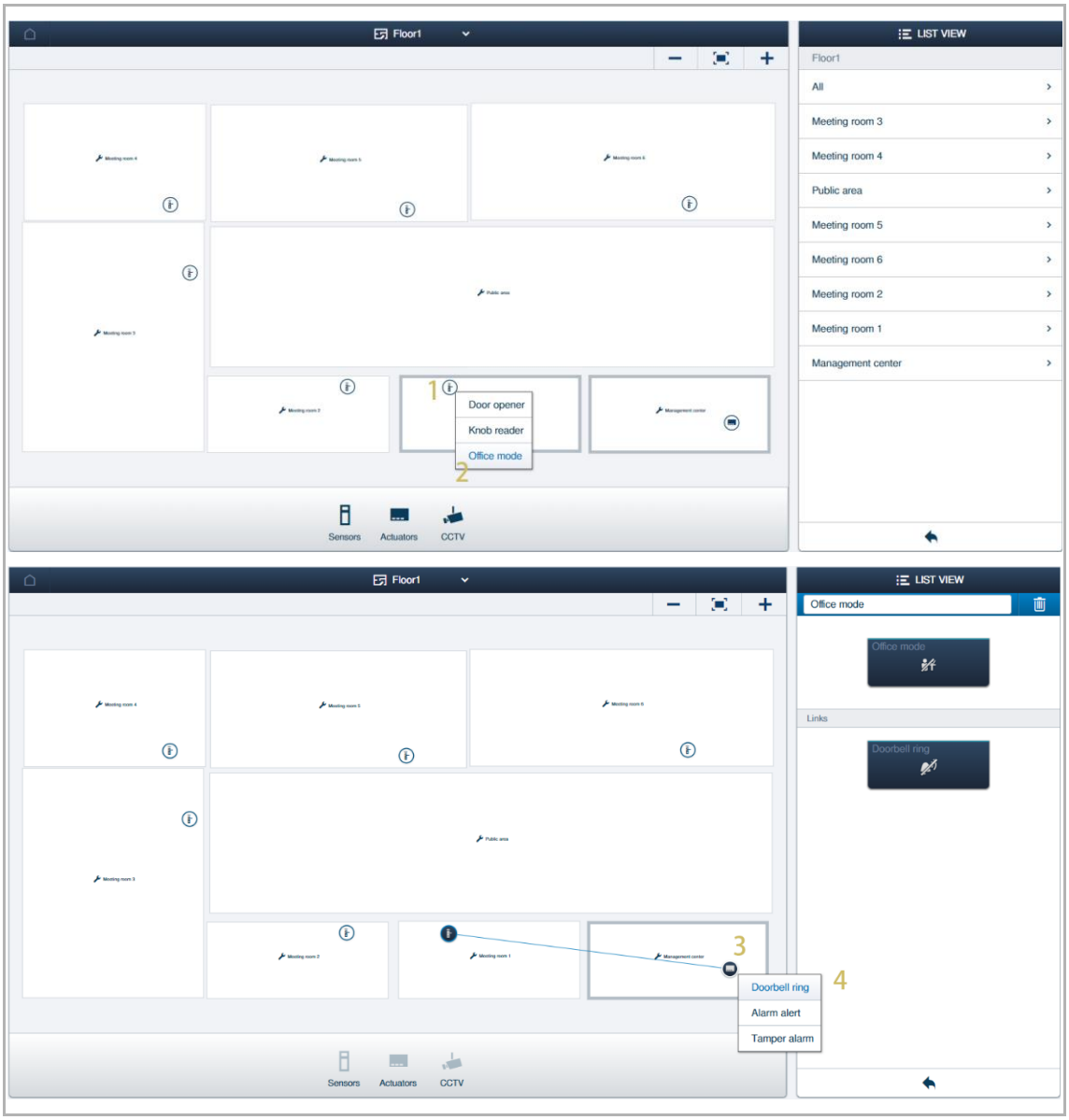
Please follow the steps below:

[1] On the floor plan screen, click the designated "Electronic locking cylinder".

[2] Click "Office mode".

[3] Click "Smart Access Point".

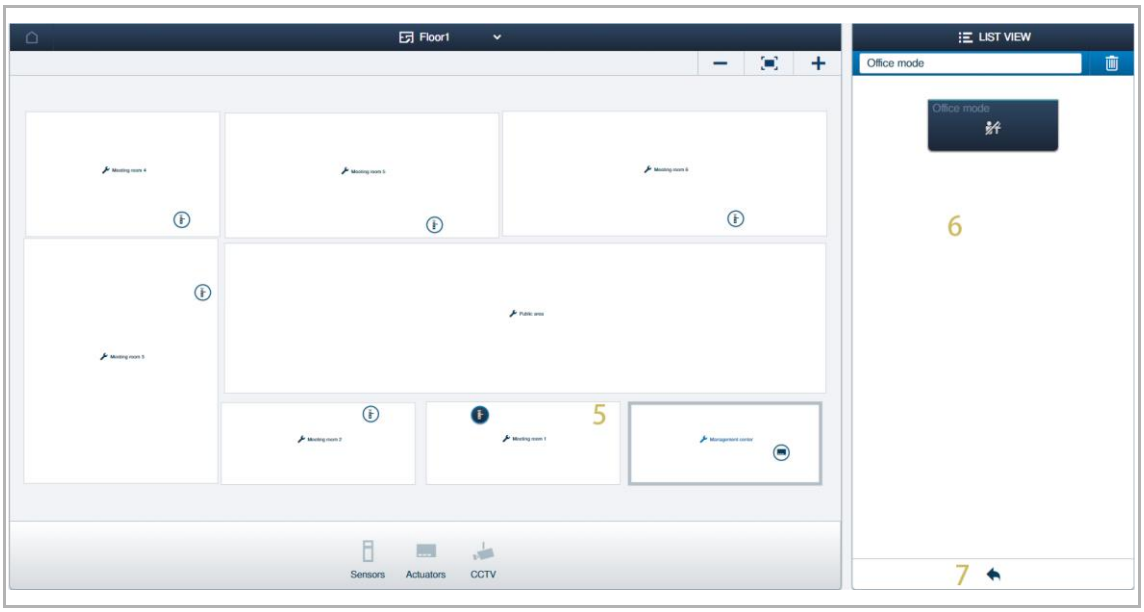
[4] Click "Doorbell ring".



[5] No link is displayed between the two devices if successful.

[6] No linked device is displayed on the list.

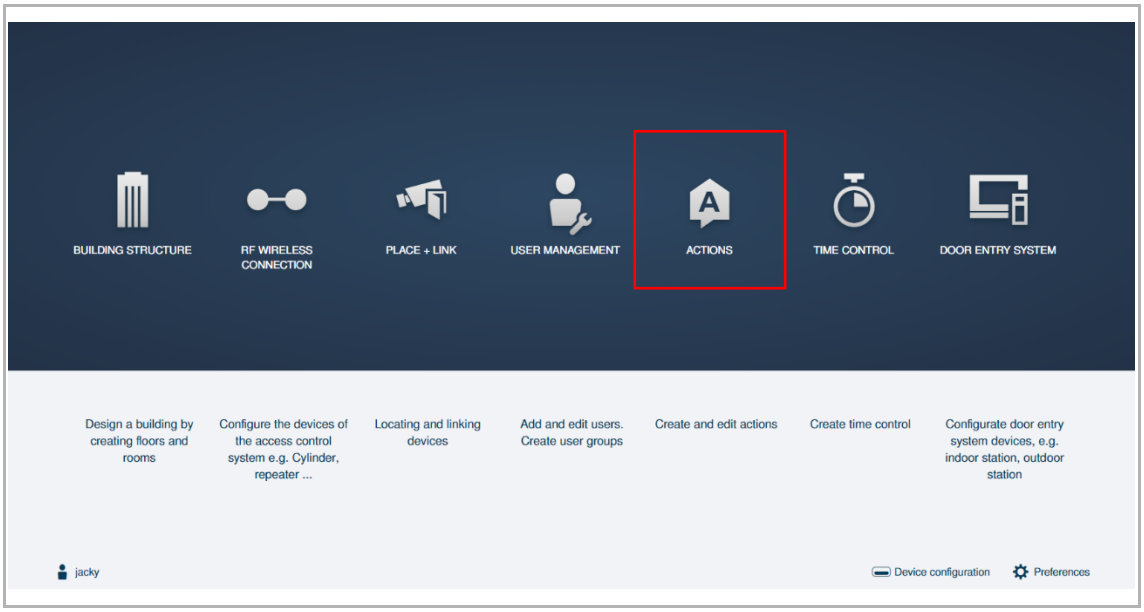
[7] Click " " to turn back to the floor screen.



11 Managing actions

Access the "Action" screen

On the configuration screen, click "Actions" to access the "Actions" screen.



Demo case

In this case, when the "Cylinder 1" is offline on the work time (e.g. AM 8~PM 5), "Smart Access Point" will receive and sound an alarm.

11.1 Adding an action

Following operations are based on demo case.

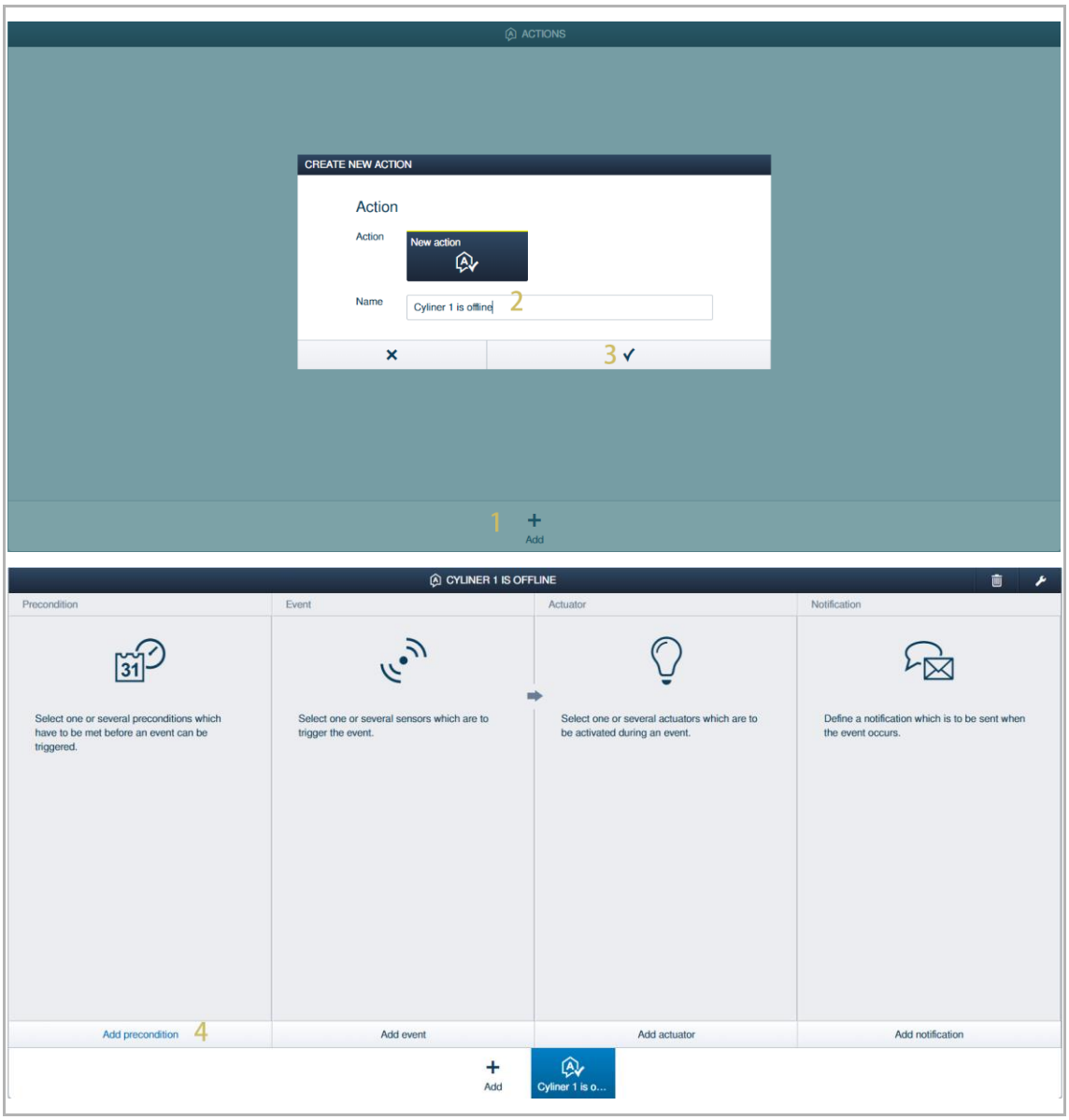
Please follow the steps below:

[1] On the "Actions" screen, click "+".

[2] Enter the name for the action.

[3] Click " √ " to save.

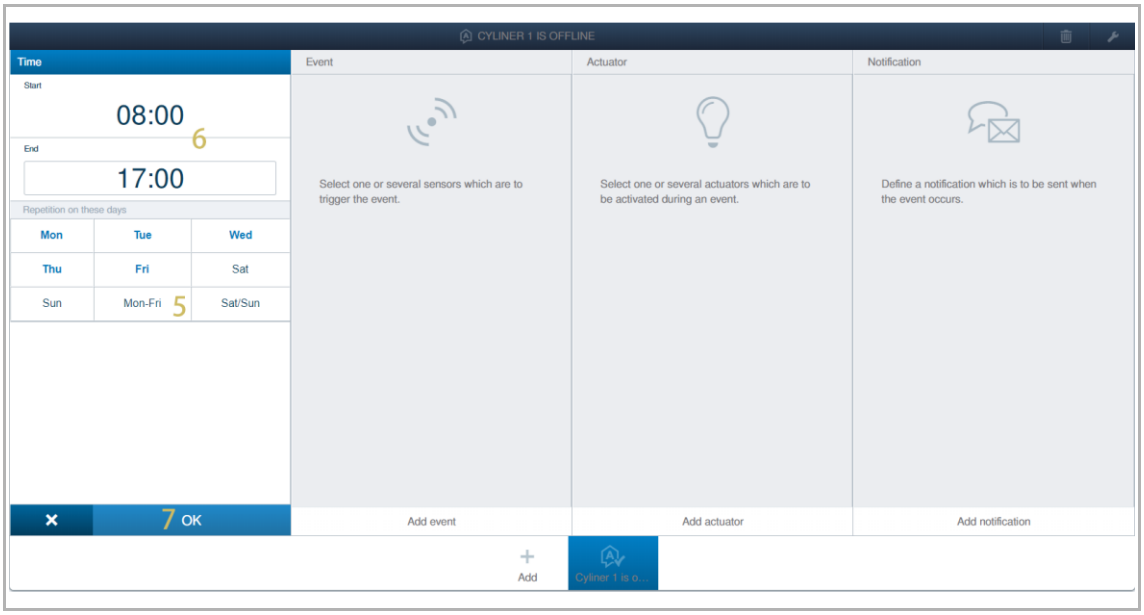
[4] On the designated action screen, click "Add precondition", followed by "Time".



[5] Click "Mon-Fri" to select the days from Monday to Friday.

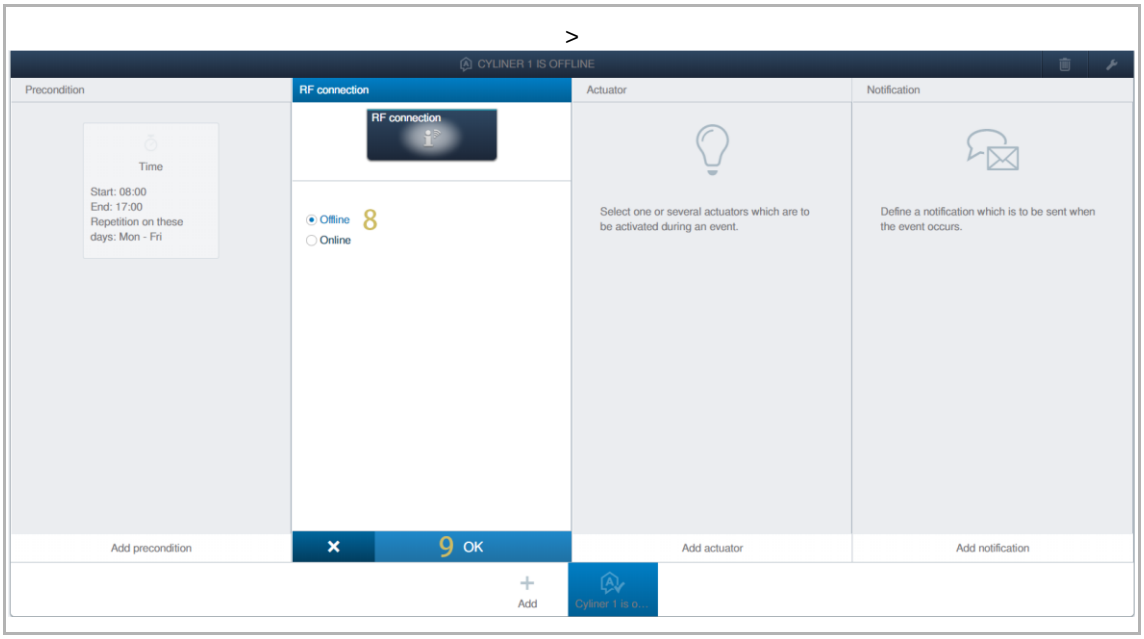
[6] Enter the start time and end time.

[7] Click "OK" to save.



[8] Click "Add event", followed by "Access control", "Cylinder 1", "RF connection", select "Offline".

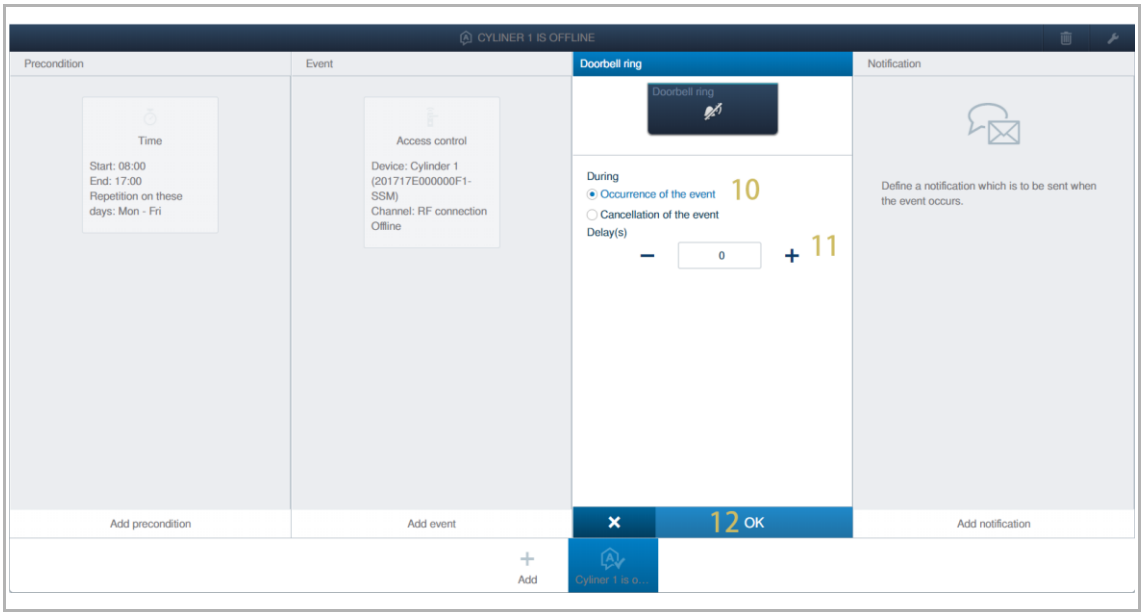
[9] Click "OK".



[10]Click "Add actuator", followed by "SmartAP", "Smart Access Point", "Doorbell ring", select "Occurrence of the event".

[11]Enter the delay time between when the actuator is activated and the event is triggered.

[12]Click "OK".



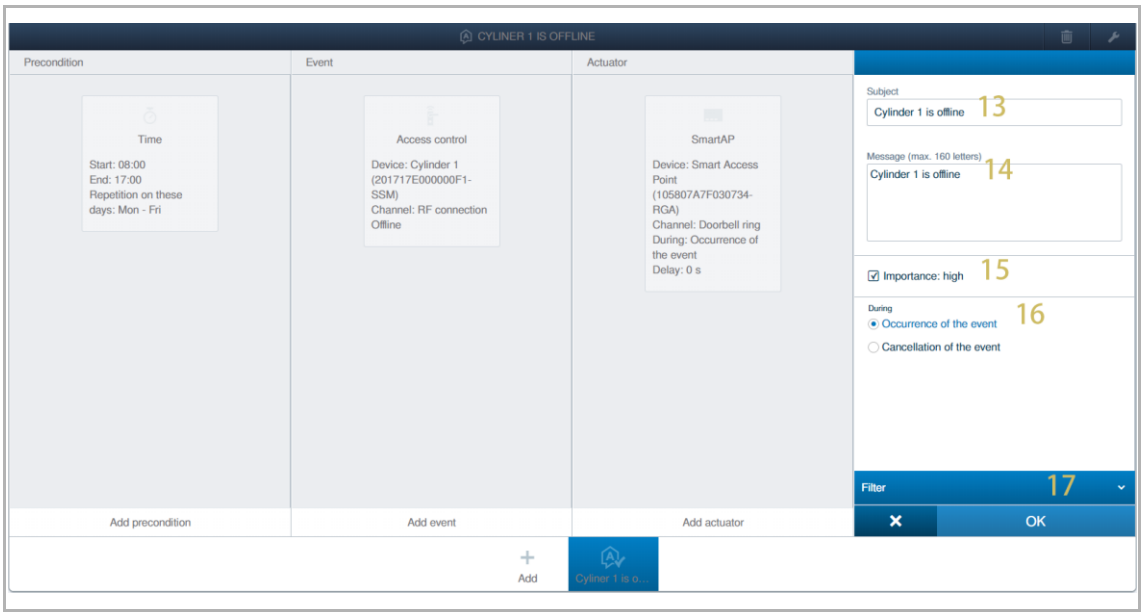
[13]Click "Add notification", enter the subject.

[14]Enter the description.

[15]If the check box "Importance: high" is activated, the message will received as an alarm, otherwise, the message will be received as a notice.

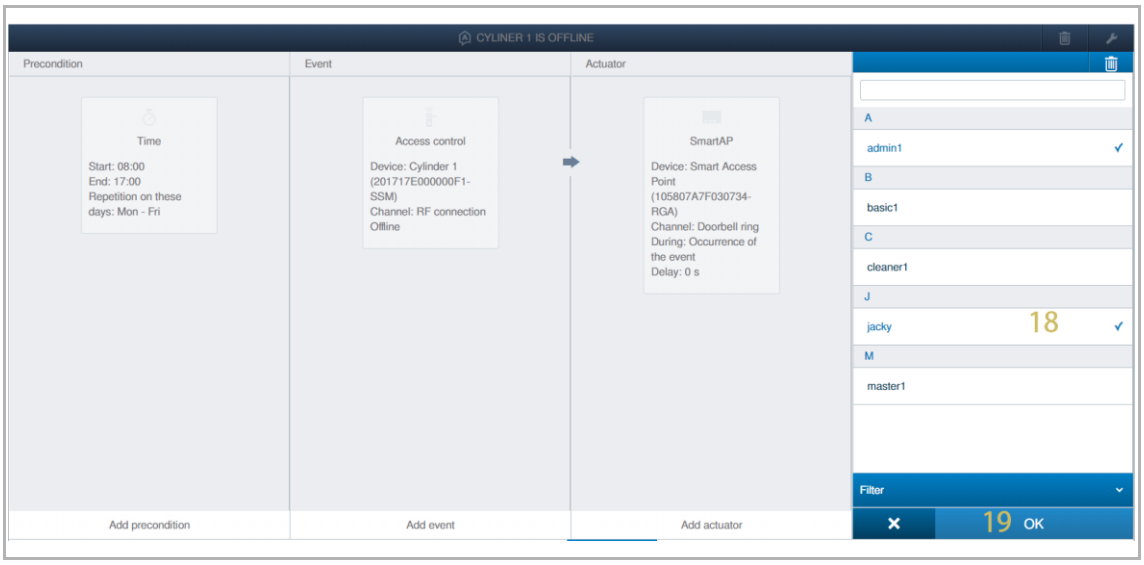
[16]Select "Occurrence of the event".

[17]Click "Filter".

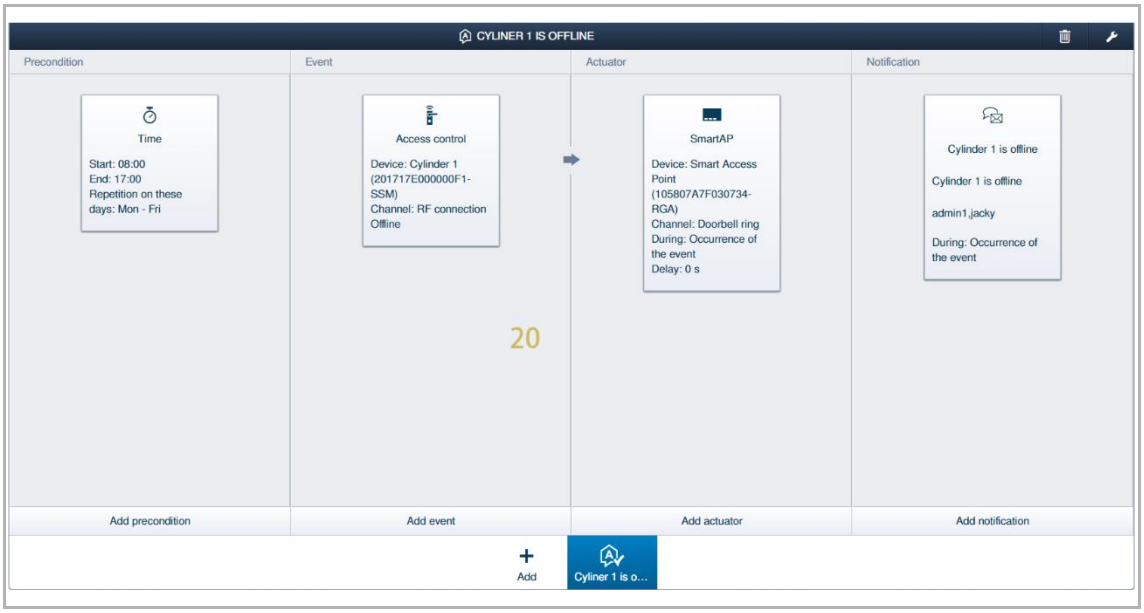


[18]Click to select the users.

[19]Click "OK" to save.



[20]The result is displayed on the screen.



11.2 Managing the action

Please follow the steps below:

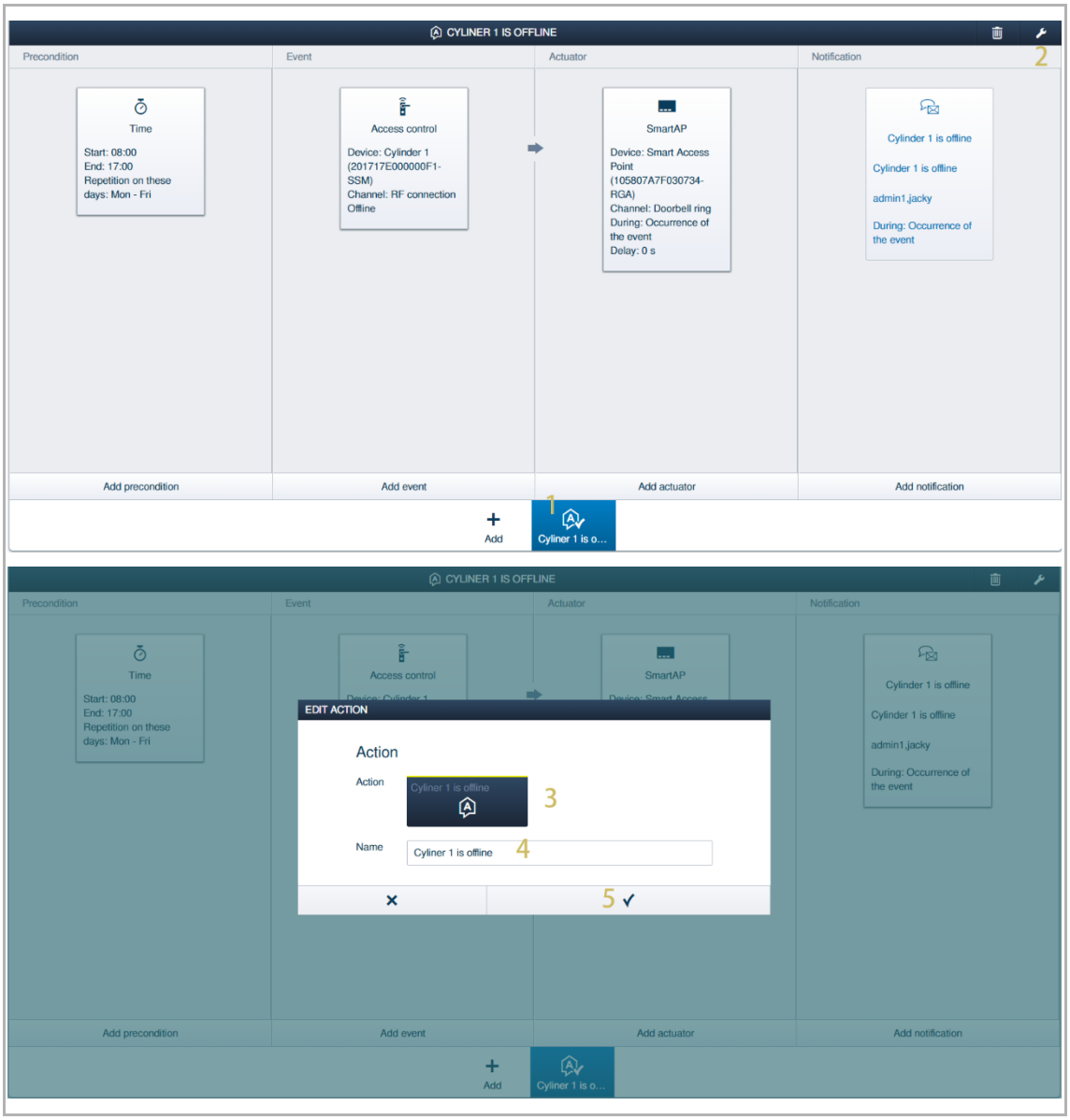
[1] On the "Actions" screen, click the designated action.

[2] Click " " ".

[3] Click the icon to disable or enable the action.

[4] Rename the action.

[5] Click "√" to save.



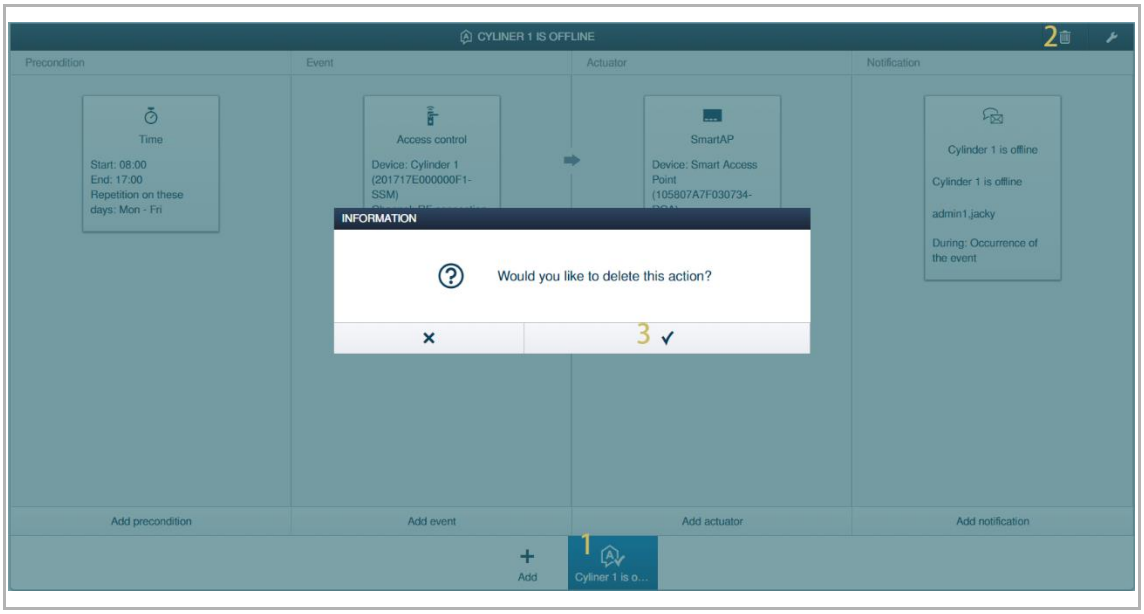
11.3 Removing the action

Please follow the steps below:

[1] On the "Actions" screen, click the designated action.

[2] Click " " ".

[3] Click "√" to save.



12 Cyber security

12.1 Disclaimer

D0401. "Smart Access Point" and D04031 "RF/IP Gateway" are designed to be connected and to communicate information and data via a network interface, which should be connected to a secure network. It is the customer's sole responsibility to provide and continuously ensure a secure connection between the product and customer's network or any other network (as the case may be) and to establish and maintain appropriate measures (including as but not limited to the installation of firewalls, application of authentication measures, encryption of data, installation of antivirus programs, etc.) to protect the D0401. "Smart Access Point" and D04031 "RF/IP Gateway", the network, its system and interfaces against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. Busch-Jaeger Ltd and its affiliates are not liable for damages and/or losses related to such security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information.

Although Busch-Jaeger provides functionality testing on the products and updates that we release, you should institute your own testing program for any product updates or other major system updates (to include but not limited to code changes, configuration file changes, third party software updates or patches, hardware change out, etc.) to ensure that the security measures that you have implemented have not been compromised and system functionality in your environment is as expected.

12.2 Performance and service and network performance

D0401. "Smart Access Point" network performance

Type	Value
Ethernet	100 Mbps (148,800 packets/s)
ARP	21 Mbps (31,250 packets/s)
ICMP	20 Mbps (29,800 packets/s)
IP	10 Mbps (14,880 packets/sec)

D0401. "Smart Access Point" Port and service

Port	Service	Purpose
53	TCP	DNS
53	UDP	DNS
80	TCP	HTTP web service
443	TCP	HTTPS web service
1883	TCP	MQTT server
1900	UDP	UPnP service
3344	UDP	Private Protocol Transmission
5061	UDP	SIP server
5070	UDP	SIP server
5070	TCP	SIP server
5222	TCP	Service for XMPP client
5280	TCP	Service for XMPP HTTP administrator service
5281	TCP	Service for XMPP HTTPS administrator service
7000	TCP	Private protocol service
7777	TCP	Private protocol service
7777	UDP	Private protocol service
8883	TCP	MQTT service
8884	TCP	MQTT server
8887	TCP	Used for upgrading process
10700	TCP	Private protocol service (TLS)
10777	TCP	Private protocol service (TLS)
31002	UDP	Searched for & managed PC client tools
49152	TCP	UPnP

D04031 "RF/IP Gateway" network performance

Type	Value
Ethernet	100 Mbps (148,800 packets/s)
ARP	1 Mbps (1,448 packets/s)
ICMP	1 Mbps (1,448 packets/s)
IP	1 Mbps (1,448 packets/s)

D04031 "RF/IP Gateway" Port and service

Port	Service	Purpose
8883	TCP	MQTT client
3344	UDP	Private Protocol Transmission

12.3 Deployment guideline

Please do not install D0401. "Smart Access Point" within a public place and ensure that physical access to the devices is granted only to trusted person.

D0401"Smart Access Point" is not recommended to use HTTP (unencrypted data transfer) outside of secure, private networks. Please use HTTPS (encrypted data transfer) when communicating over a public network. Please note that using HTTPS will result in a warning. This is due to technical reasons.

During commissioning, the "Electronic locking cylinders" and "RF Repeaters" need to be added one by one following the "Smart Access Point" commissioning process; it is essential that the observed indications for "Electronic locking cylinders" and "RF Repeaters" should be confirmed correctly.

D04031 "RF/IP Gateway" is the gateway for the TCP/IP network and the RF network; it needs to pair to "Smart Access Point" for its functions. No sensitive data related to privacy is stored on "RF/IP Gateway".

If the reset option is activated, the D04031."RF/IP Gateway" can be unpaired from "Smart Access Point" by pressing and holding the reset button on the device. If installed in the public area, it is recommended to deactivate the reset option.

The configuration data need to be backed up manually after every Access control system topology change, so that the backup configuration can be restored to "Smart Access Point" in case of misconfiguration.

12.4 Upgrading

The firmware can be uploaded by the webpage; a signature file also requires to be updated together with the firmware file, which is used to verify the authentication and integrity of firmware.

If internet services are available, D0401. "Smart Access Point" will connect to the myBUSCH-JAEGER server to obtain the new firmware automatically but needs to be confirmed by the end user every time. Also, for security purposes, D0401. "Smart Access Point" will automatically download the respective signature file and firstly verify the authentication and integrity of firmware before updating.

12.5 Backup/restore

Some device configurations can be downloaded locally by webpage, the password is needed to encrypt the exported configuration data, the configurations include,

- "Smart Access Point" configuration parameters
- User data
- Device data including Access control system device, Door Entry System devices and VideoControl system device

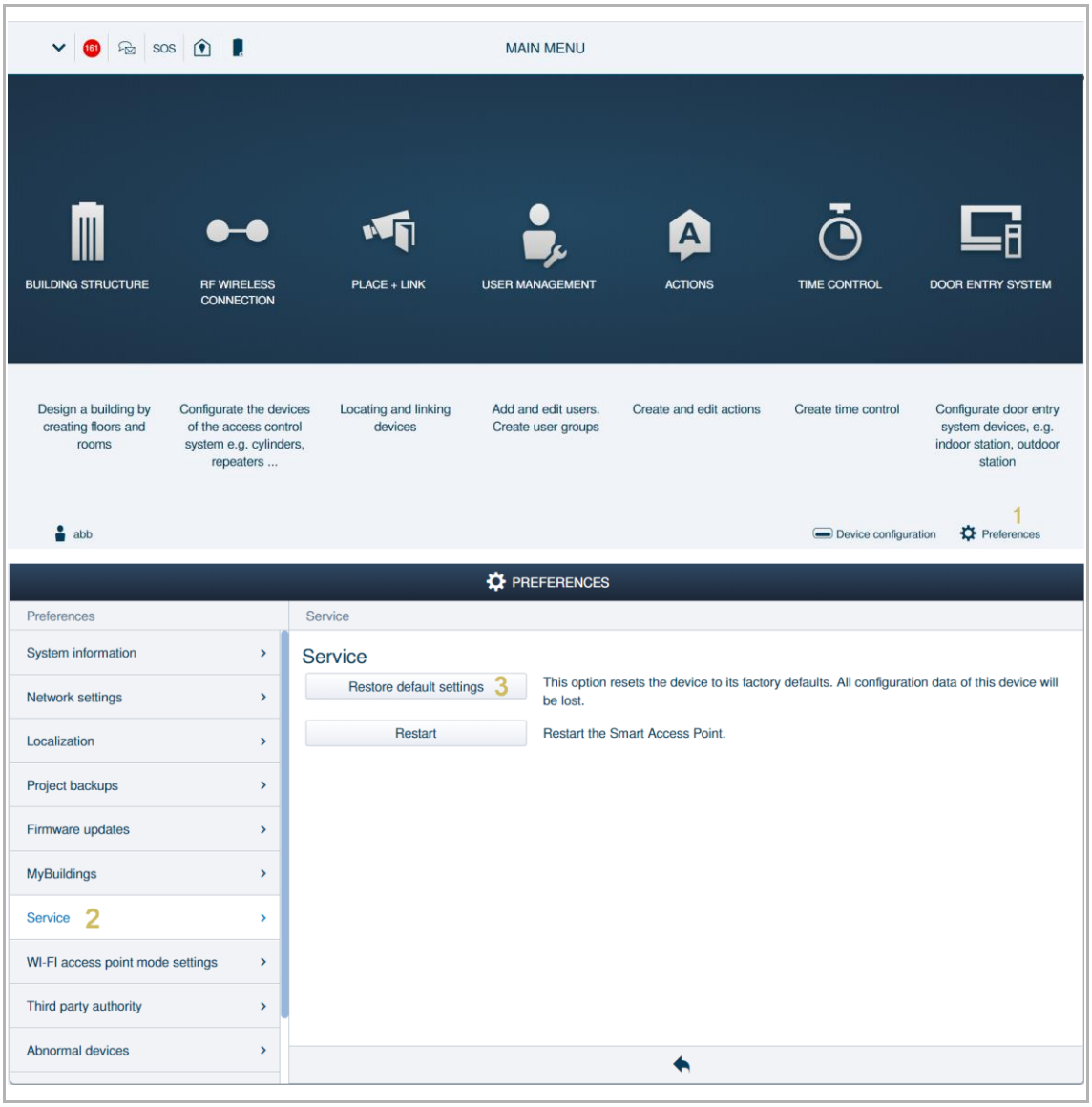
When restoring from the backup configured, the exported file needs to be updated to the device by webpage, and the respective password used when exporting the configuration is needed.

12.6 Data purging

In the case of quitting the working system (e.g. replaced by another device, re-install in another system…), all the data stored in the device need to be purged using the "Restore default setting" on the webpage as shown below.

Log in to the web page using an admin user account.

On the configuration screen, follow the steps below:



The data stored in the D04031."RF/IP Gateway" can be purged via the webpage of "Smart Access Point", or via the reset button if the reset option is activated.

12.7 Malware prevention solution

These devices are not susceptible to malware, because custom code cannot be executed on the system.

The only way to update the software is by firmware updating. Only firmware signed by Busch-Jaeger can be accepted.

12.8 Default passwords and user accounts

In the factory defaults, D0401. "Smart Access Point" has the following passwords or user accounts:

- The password for Wi-Fi Access Point
- The user account for the initial commissioning

All the default passwords and user accounts given must be changed during the initial commissioning process.

In the factory defaults, the D04031 "RF/IP Gateway" does not have a default password.

The communication key between D04031 "RF/IP Gateway" and RF module can be changed when the D04031 "RF/IP Gateway" is reset to the defaults.

The communication key and the key pairs used in TLS is stored with flash encryption, and the encryption key is stored in ROM of MCU, which cannot be read out.

12.9 Password rule

The password for all user accounts need to fulfil the following rules:

- Minimum 8 characters
- Must include at least three of these four types: lowercase letters, uppercase letters, digits, symbols
- Accepted characters: a-z, A-Z, 0-9, space and symbols !"#/()=?@${[]}\,.-_<>|;:'*^~+

12.10 Logging

The device has a logging system which can log some events, which contains,

- Changing settings
- Adding/changing/removing other devices
- Adding/changing/removing user accounts (including information and access rights)
- Updating/patching software firmware
- Accessing to devices, such as unlock, record, snapshot, etc.
- Security attacks, such as tamper alarm, multiple login error, disconnect BLE module from SmartAP.

The following information and events from devices in Access control system for the logging purpose.

Device	Information for events
"RF Repeater"	Loss connection with SmartAP event
"Electronic locking cylinder"	Battery status Loss connection from system event Unlock event Battery low event Swipe Card event
"RF/IP Gateway"	Loss connection with SmartAP event

Every piece of log information contains the time, event source, behaviour and signature.

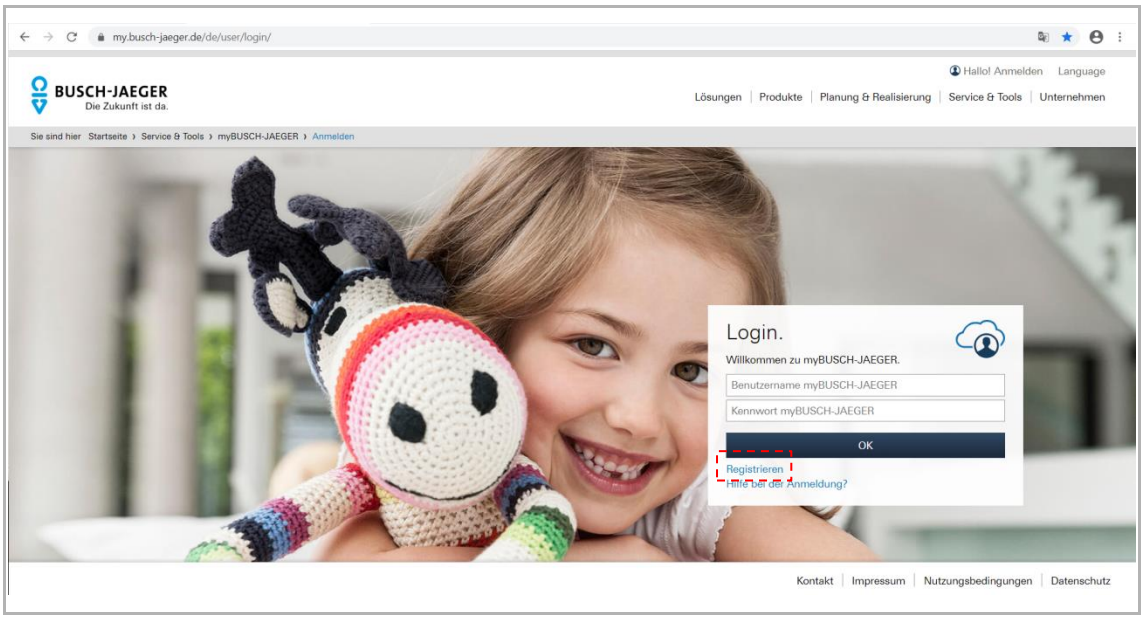
The device will automatically generate logs and store them when the above events occur.

The admin user can log into the webpage, then switch to the notification center to manage the logs.

13 Appendix

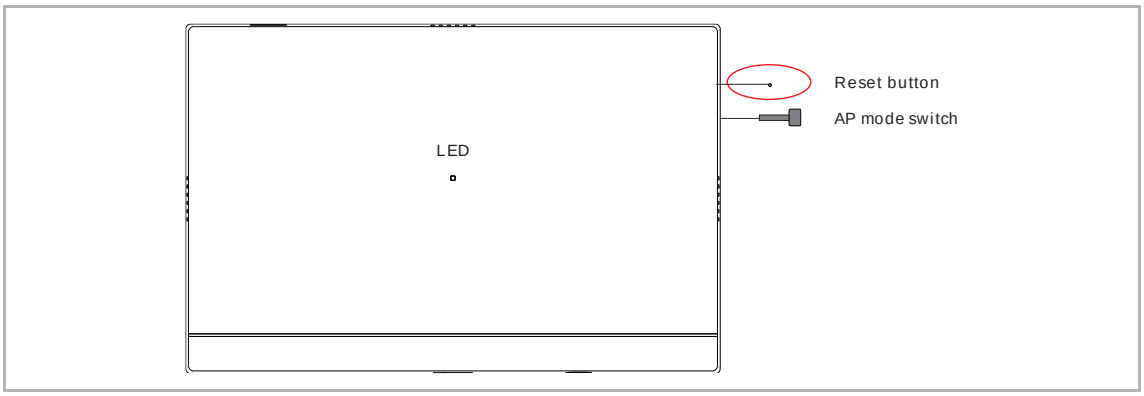
13.1 Registering an account on the myBUSCH-JAEGER portal

Access the link: https://my.busch-jaeger.de/en/user/login/, and click "Register". Fill in the form as required to register an account. Then activate the user account when you receive the email sent from the myBUSCH-JAEGER portal.



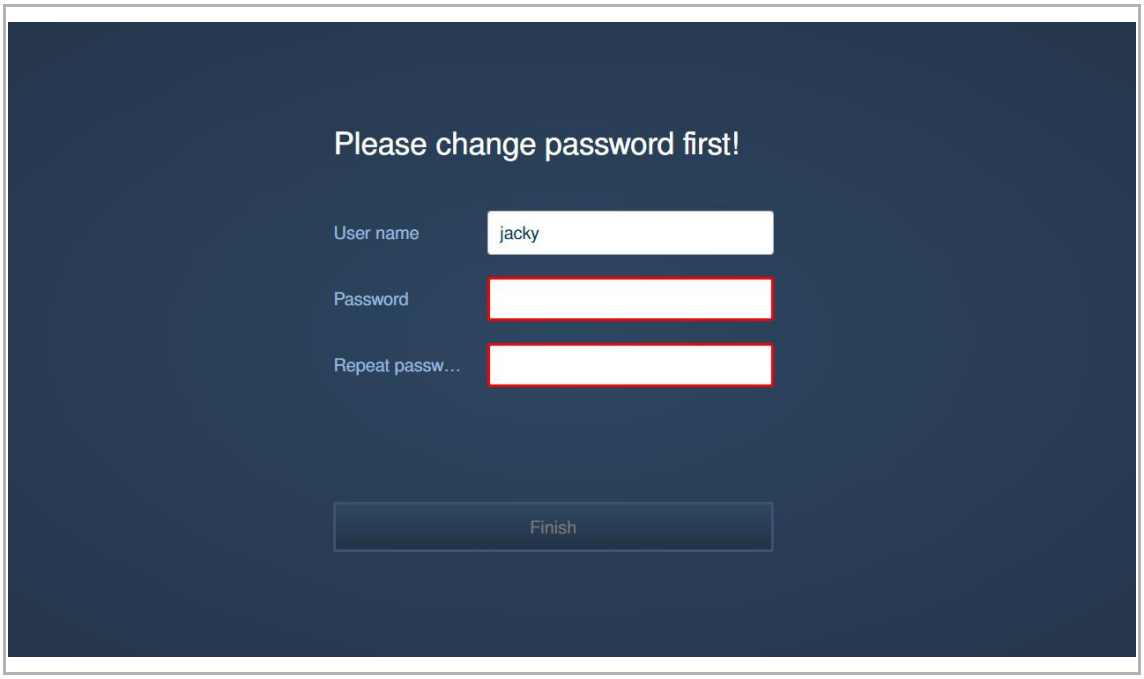
13.2 Resetting the password for the primary admin

Press and hold the reset button for 10 s.



1. Reset option = Without MyBuildings account

If the reset option is set to " Without MyBuildings account" in the initial setup, you can change the password for the primary admin directly by entering a new password twice.

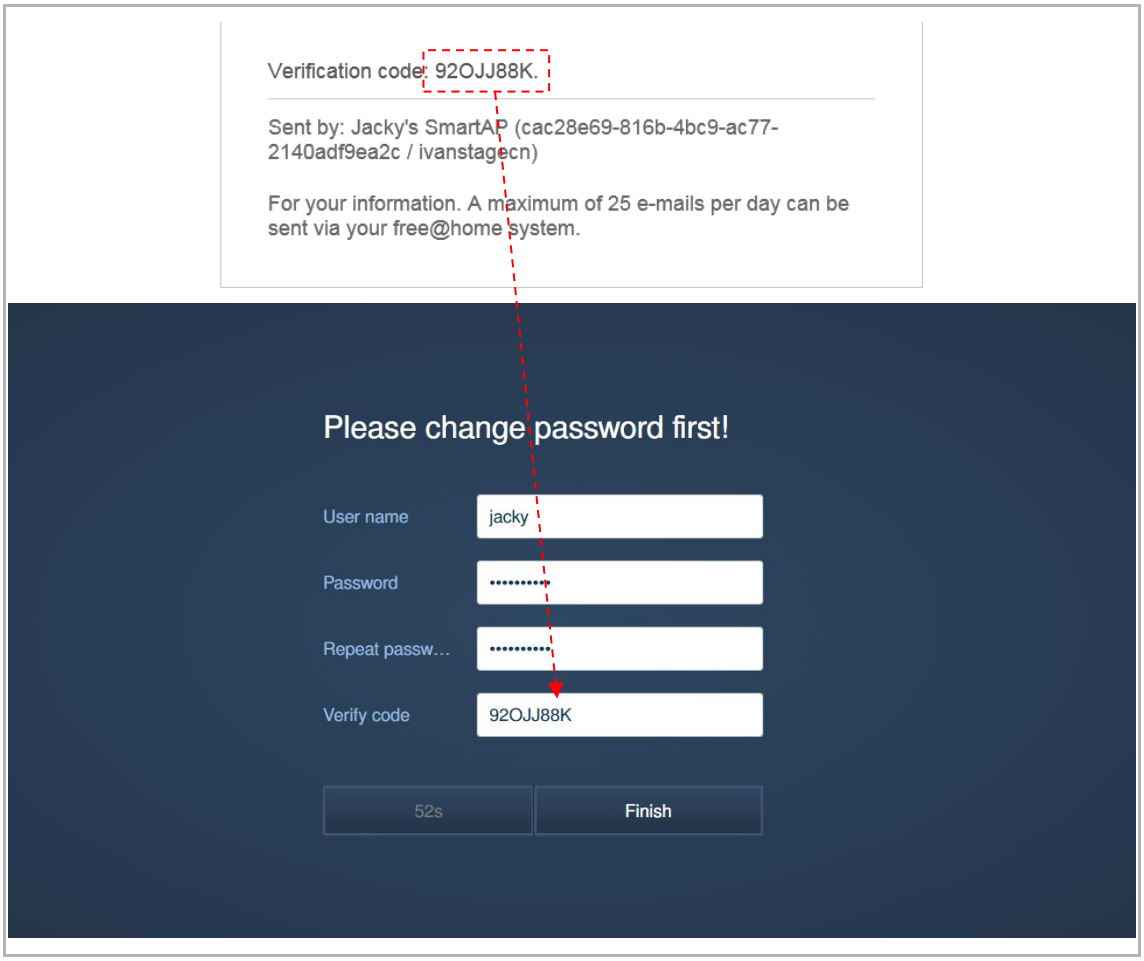


2. Reset option = With MyBuildings account

If the reset option is set to "With MyBuildings account" in the initial setup, besides entering a new password twice, a verification code is also needed.

Note

If you have set an email to receive the verification code in the initial setup, you can obtain the verification code sent by email.



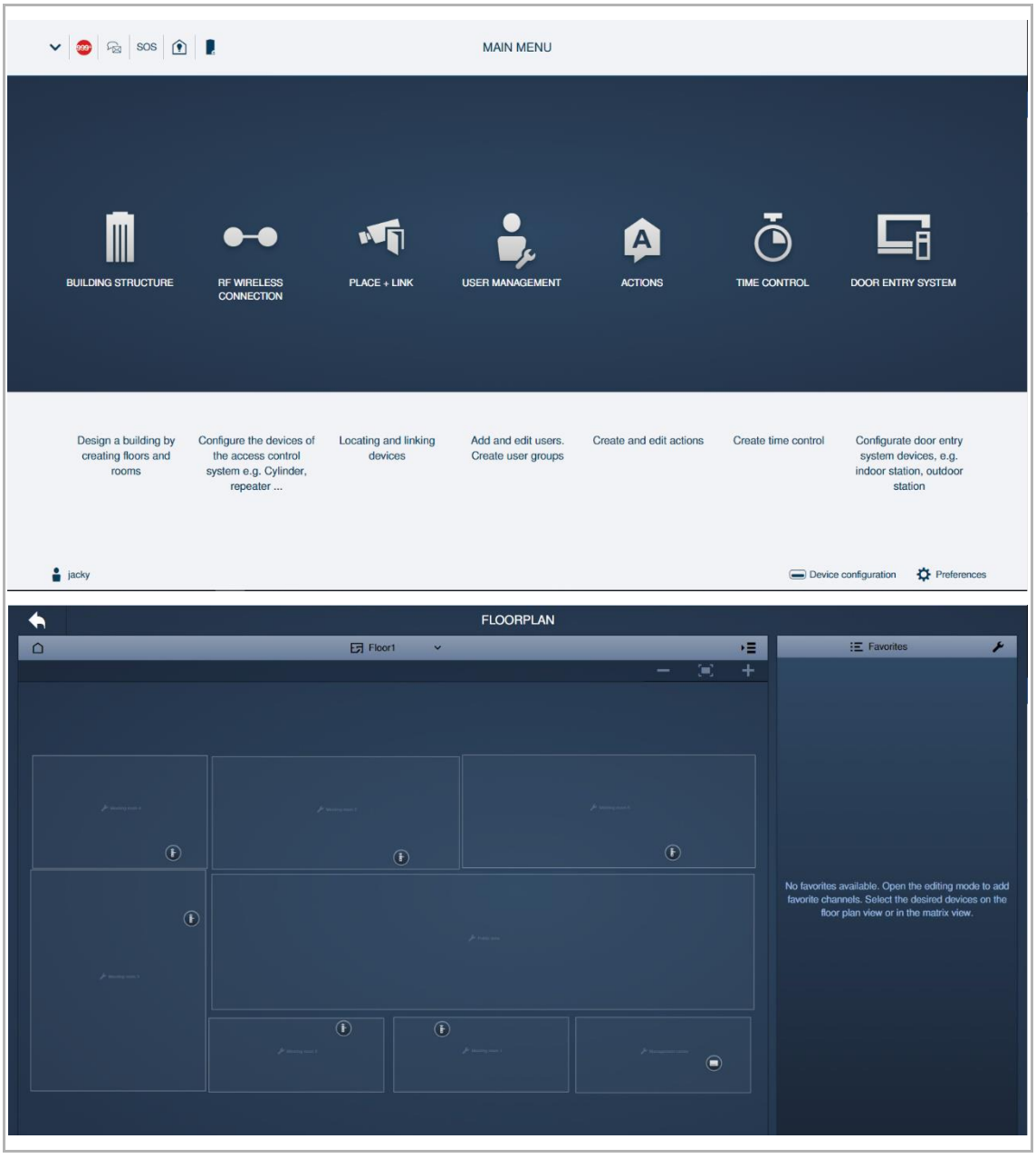
13.3 User management

13.3.1 User roles

There are 4 optional user roles supported by "Smart Access Point".

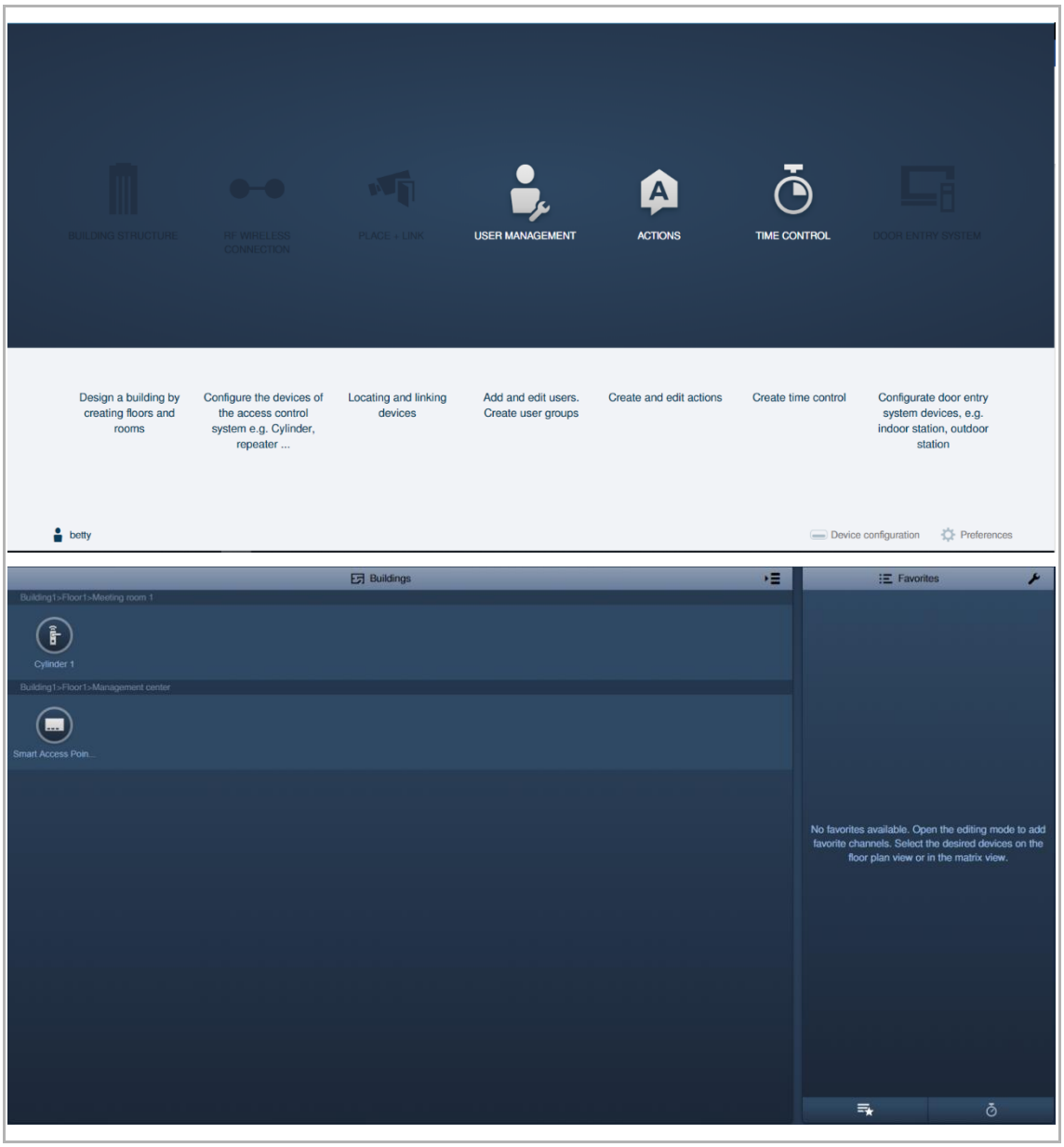
1. Admin users

- The primary admin user is created only during the initial setup. The other admin users can be created by the primary admin user or other admin users. see chapter 8.3 “Initial setup“ on page 26.
- Admin users can manage other admin users, master users, basic users and 3rd party users.
- Admin users can operate all of the functions on the configuration screen.
- Admin users can operate all of the functions on the control screen.



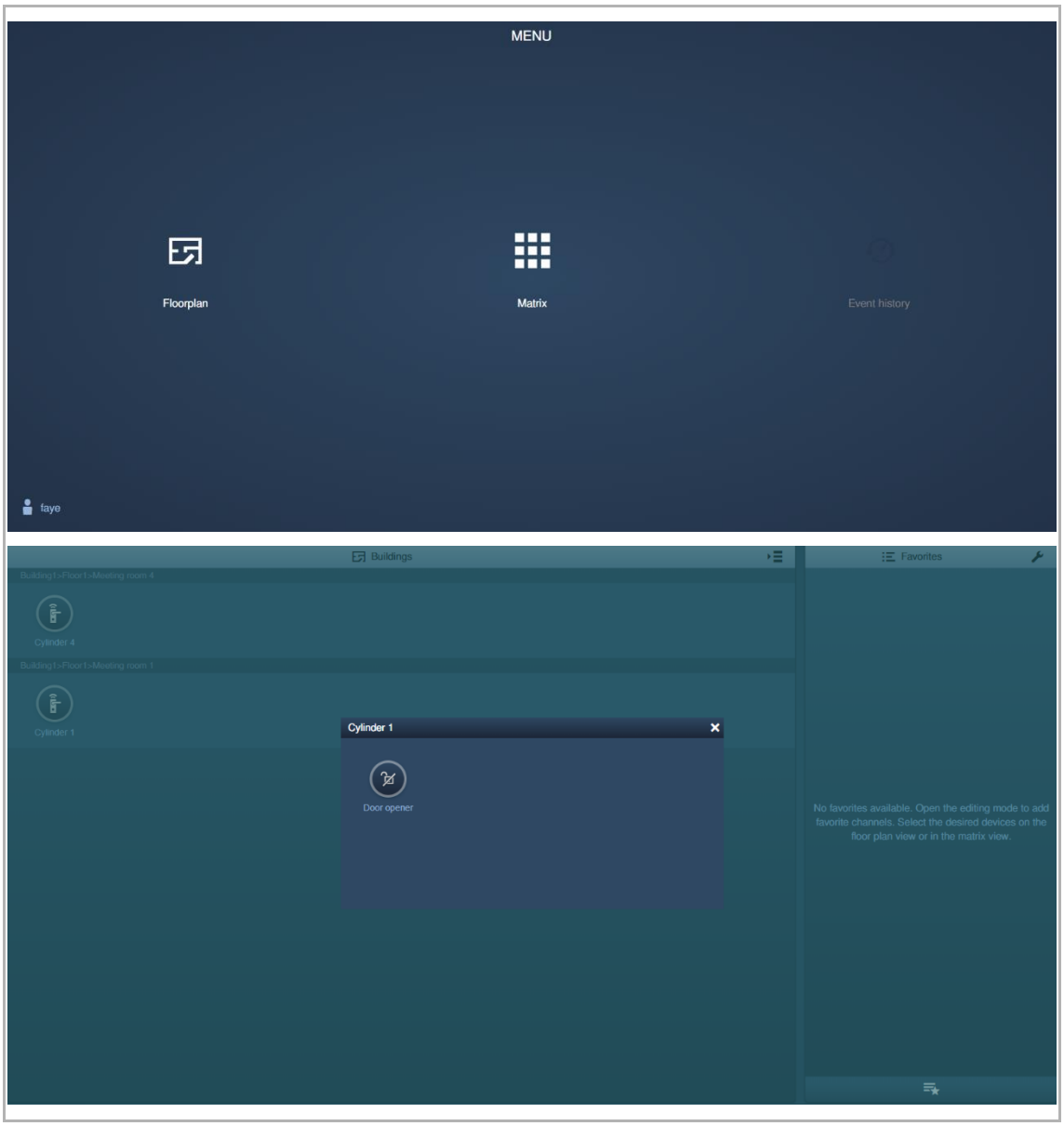
2. Master users

- Master users can be created by admin users or other master users.
- Master users can manage other master users, basic users and 3rd party users.
- Master users can operate some of the functions on the configuration screen.
- Master users can operate "Smart Access Point" and the "Electronic locking cylinder" assigned to him.



3. Basic users

- Basic users can be created by admin users and master users.
- Basic users can operate only the "Electronic locking cylinder" assigned to them.
- Basic user cannot access the "Event history" screen.



4. 3rd party users

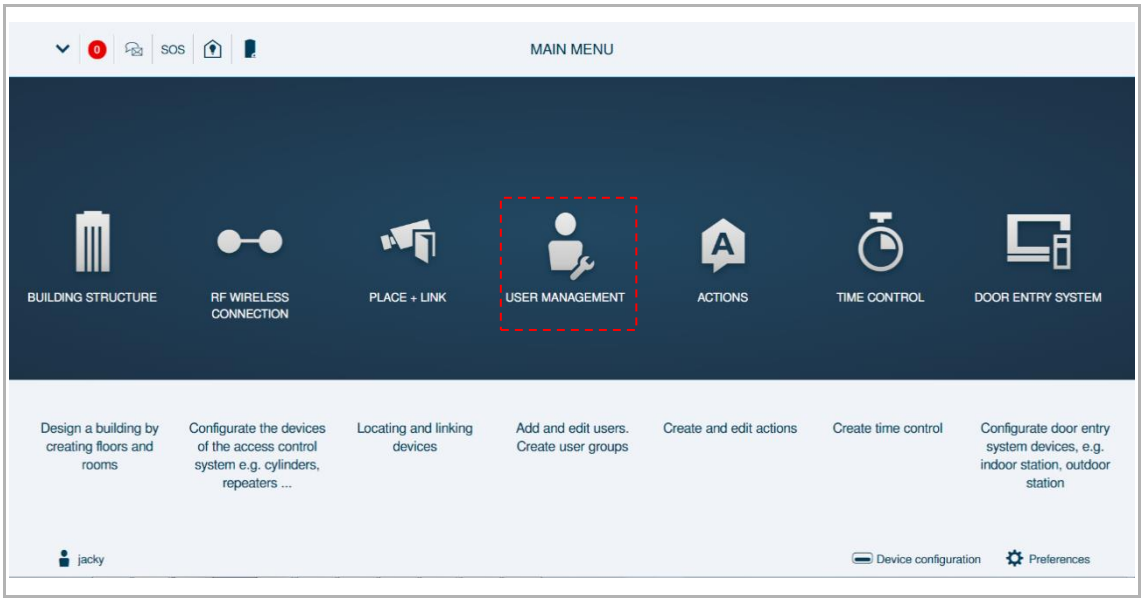
- 3rd party users can be created by admin users and master users.
- 3rd party users can operate only the "Electronic locking cylinders" assigned to them during the specified duration.

13.3.2 Adding users

Note
Up to 2000 users can be supported by a "Smart Access Point".

Accessing the "Users" screen

On the configuration screen, click "User management" to access the "Users" screen.

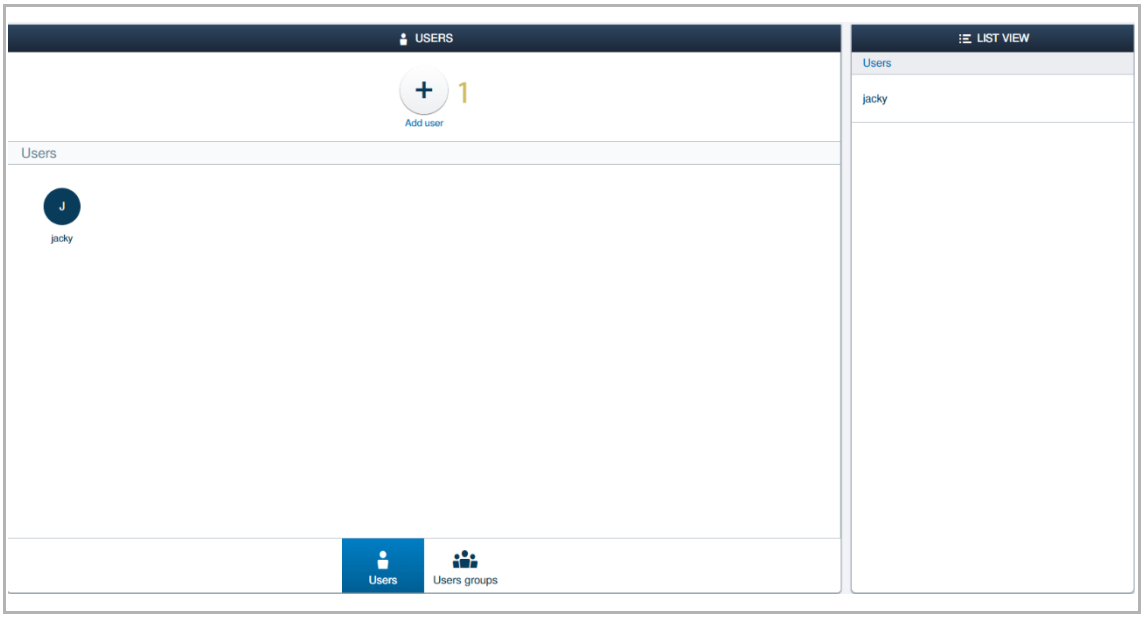


Adding users

1. Adding admin users

Please follow the steps below:

[1] On the "Users" screen, click "Add user".



[2] Enter the username, this username could not be the same to exist username.

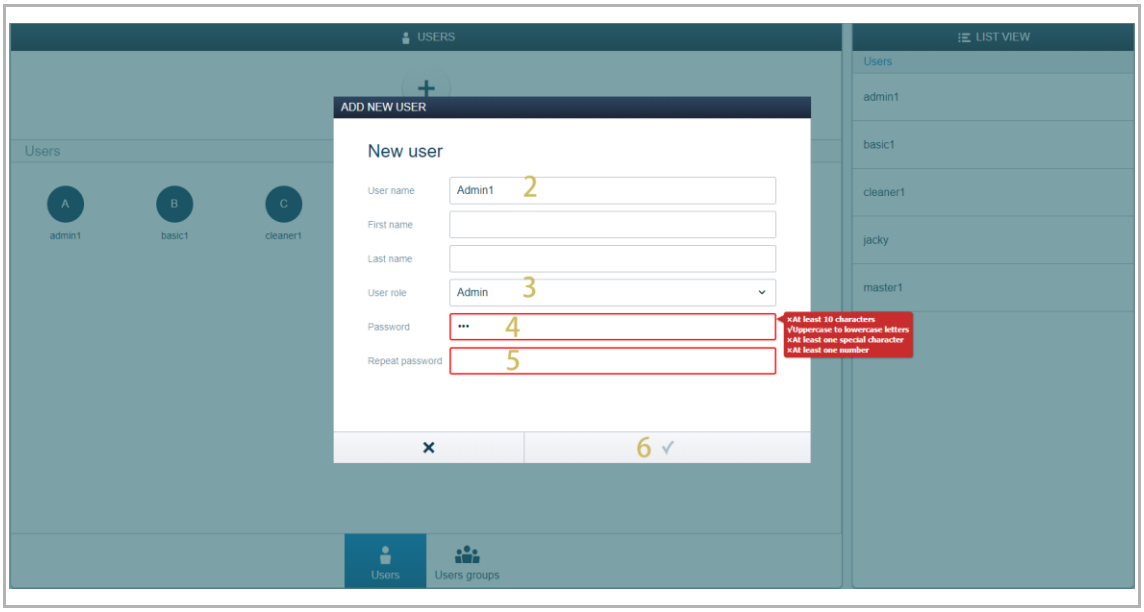
[3] Select "Admin" from the drop-down list.

[4] Enter the password according to the password rules displayed on the screen.

[5] Enter the password again

[6] Click "OK" to save.

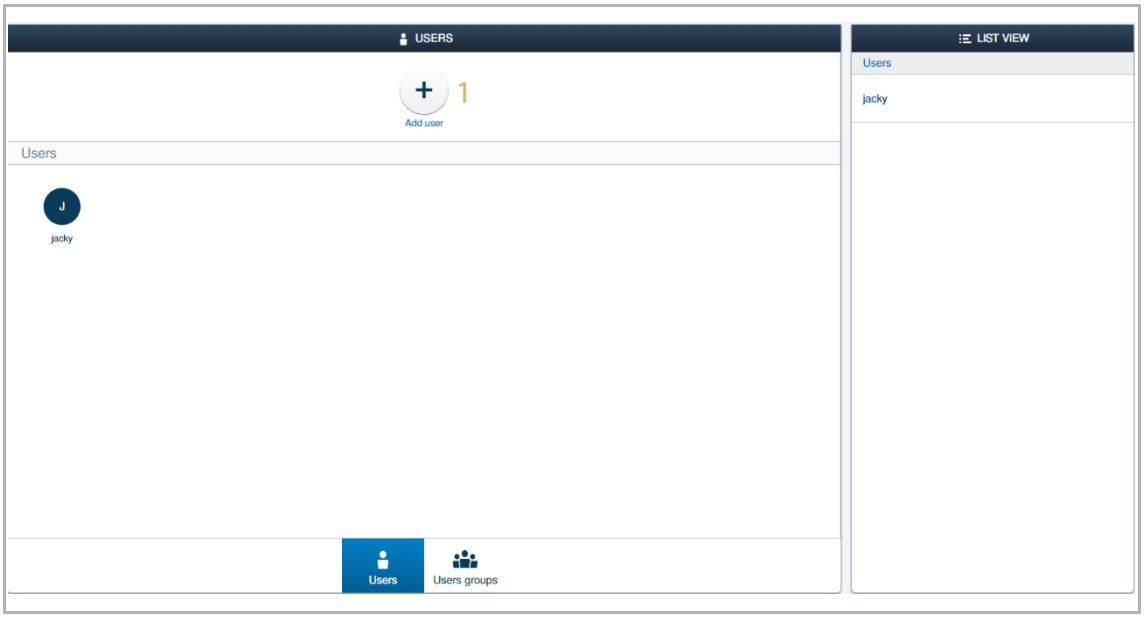
Repeat steps 1-6 to add admin users.



2. Adding master users

Please follow the steps below:

[1] On the "Users" screen, click "Add user".



[2] Enter the username, this username could not be the same to exist username.

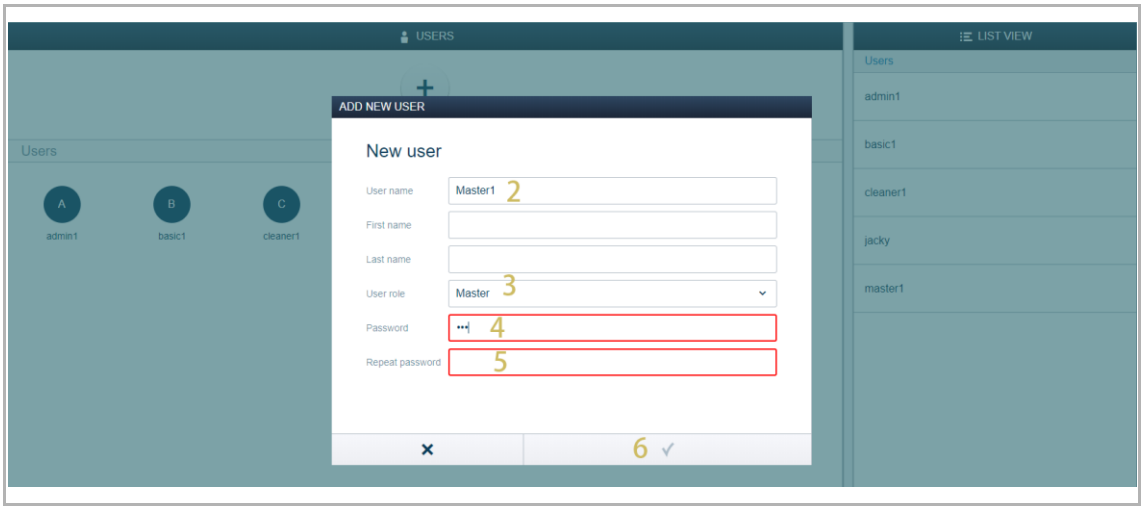
[3] Select "Master" from the drop-down list.

[4] Enter the password according to the password rules displayed on the screen.

[5] Enter the password again.

[6] Click "OK" to save.

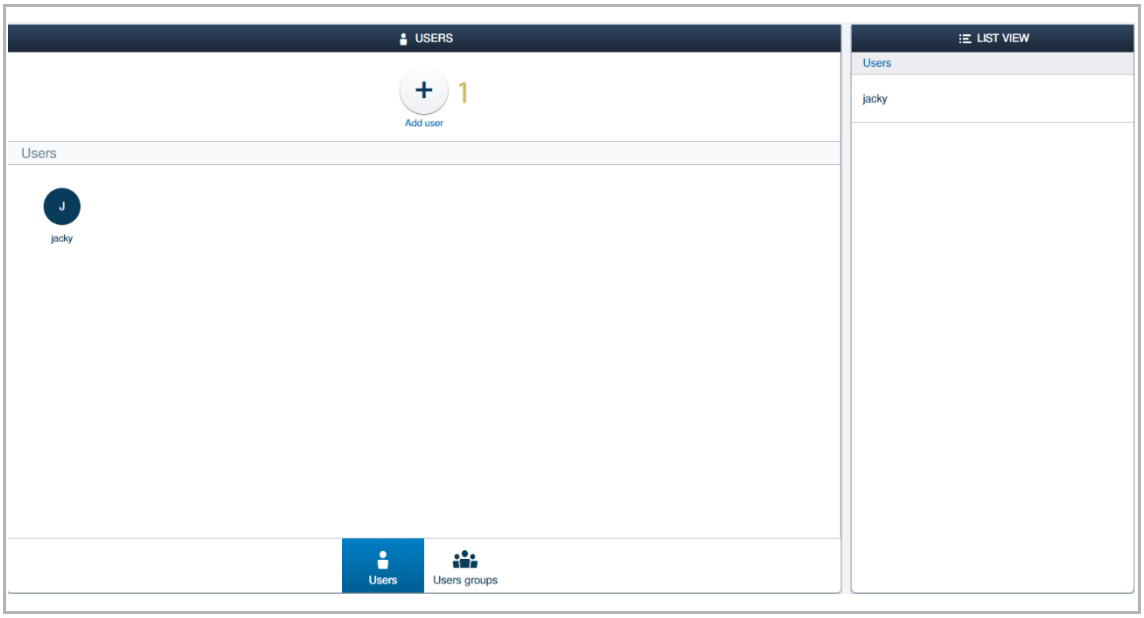
Repeat steps 1-6 to add master users.



3. Adding basic users

Please follow the steps below:

[1] On the "Users" screen, click "Add user".



[2] Enter the username, this username cannot be the same as the existing username.

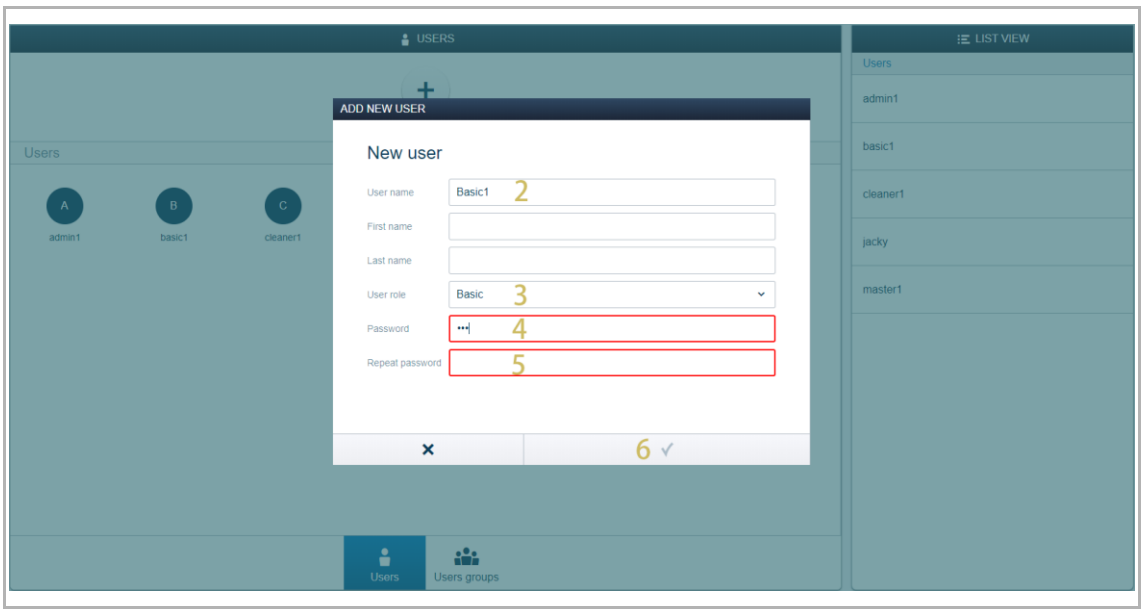
[3] Select "Basic" from the drop-down list.

[4] Enter the password according to the password rules displayed on the screen.

[5] Enter the password again.

[6] Click "OK" to save.

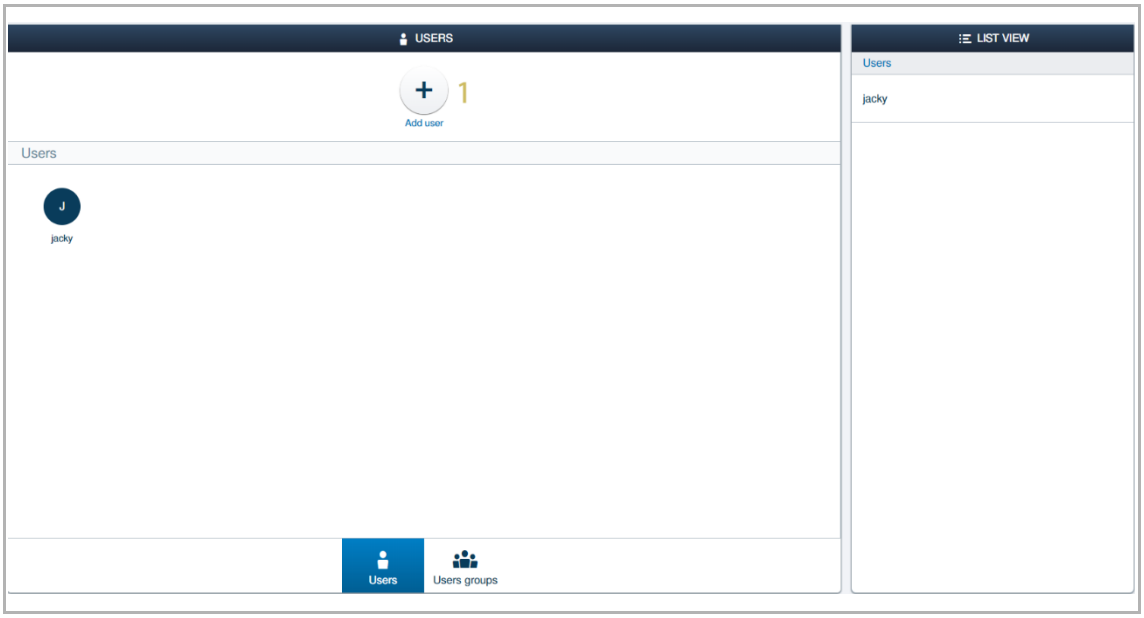
Repeat steps 1-6 to add basic users.



4. Adding 3rd users

Please follow the steps below:

[1] On the "Users" screen, click "Add user".



[2] Enter the username, this username cannot be the same as the existing username.

[3] Select "3rd party" from the drop-down list.

[4] Enter the password according to the password rules displayed on the screen.

[5] Enter the password again.

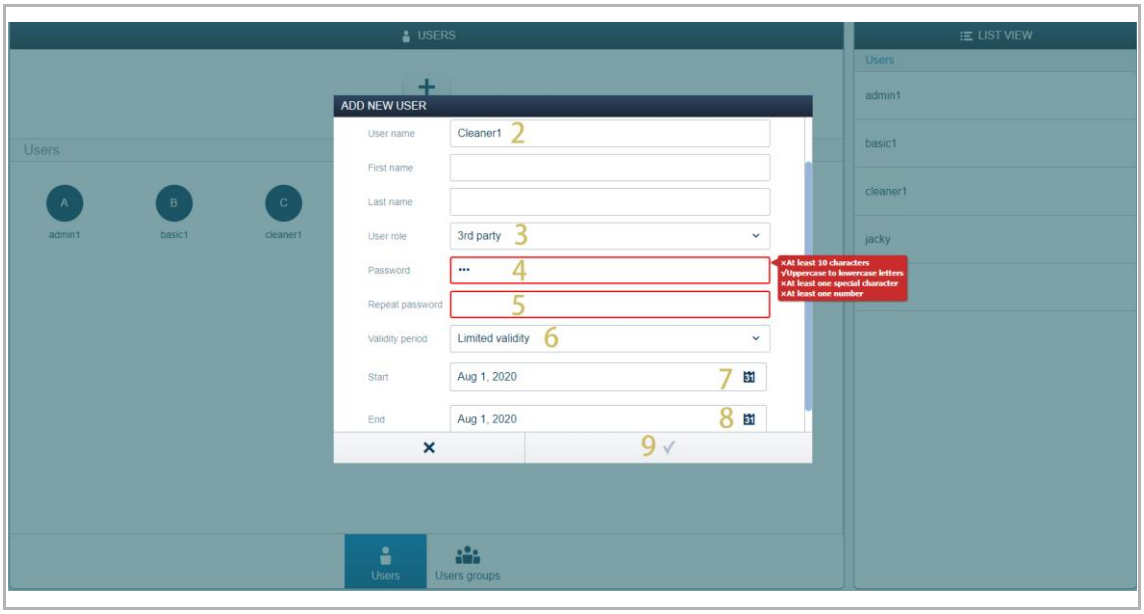
[6] Select "Limited validity" from the drop-down list.

[7] Set the start date via clicking " 31 ".

[8] Set the end date via clicking " 31 ".

[9] Click "OK" to save.

Repeat steps 1-9 to add 3rd party users.



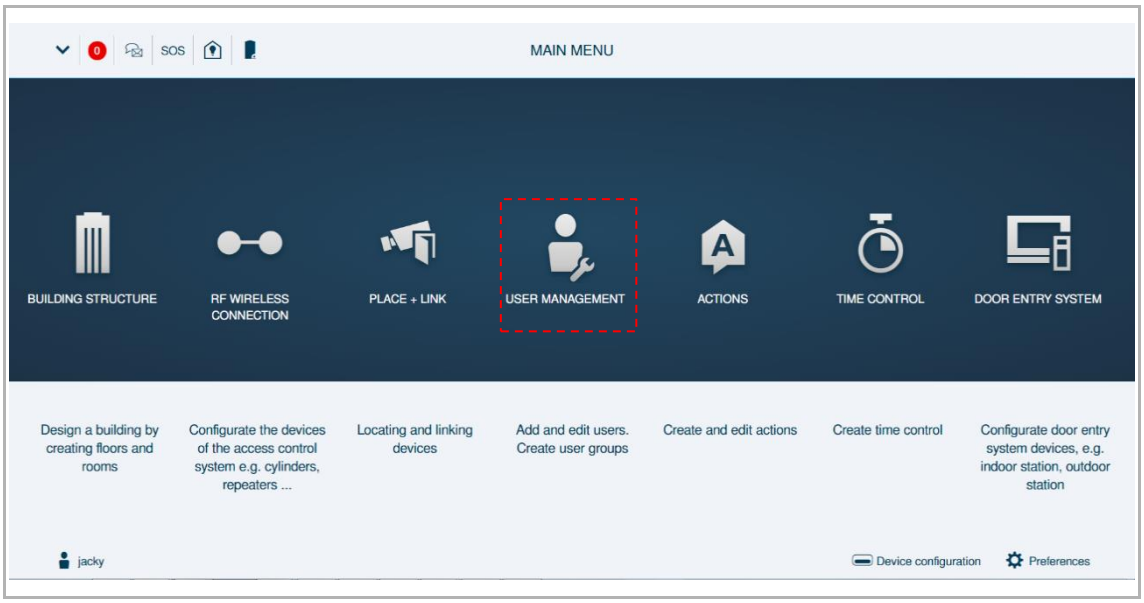
13.3.3 Adding user groups

Note

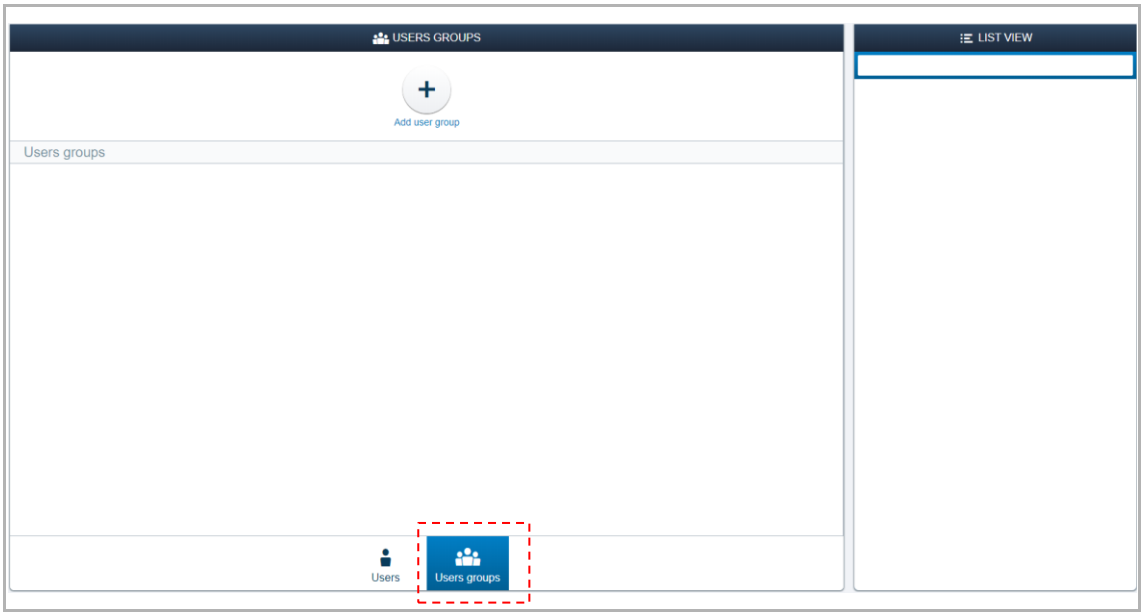
User group is a collection of the users. All the users in the group have the same permission for the devices. All the users in the group change permissions automatically when some permissions are changed.

Accessing the "User groups" screen

On the configuration screen, click "User management" to access the "Users" screen.



On the "Users" screen, click "User groups" to access the "User groups" screen.



Adding user groups

Please follow the steps below:

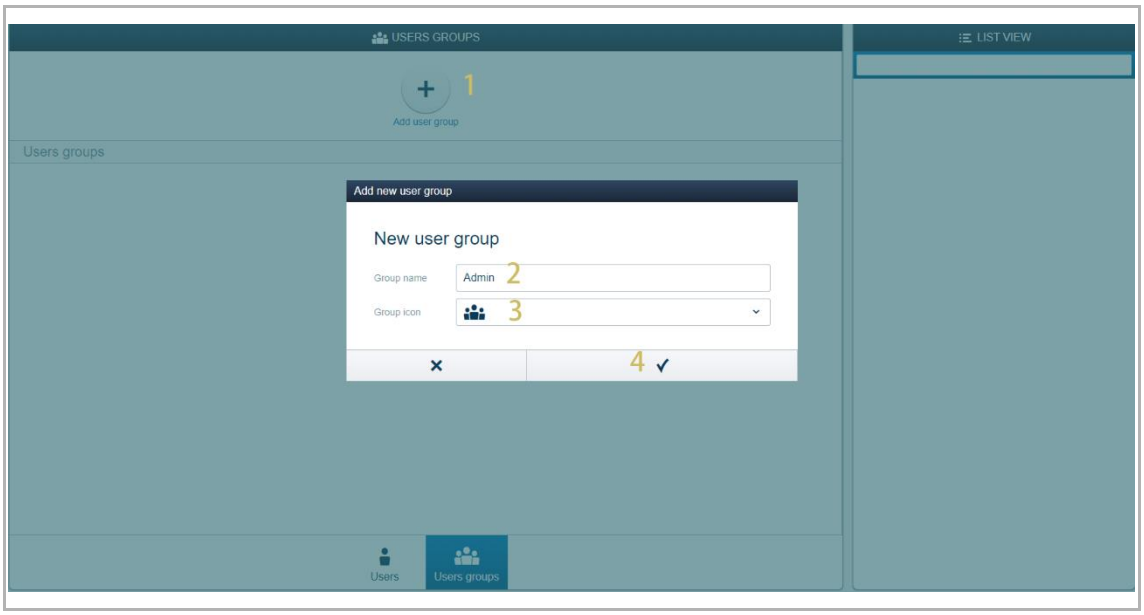
[1] On the "User groups", click "Add user group".

[2] Enter the group name.

[3] Select a group icon from the drop-down list.

[4] Click " √ " to save.

Repeat steps from 1-4 to add user groups.

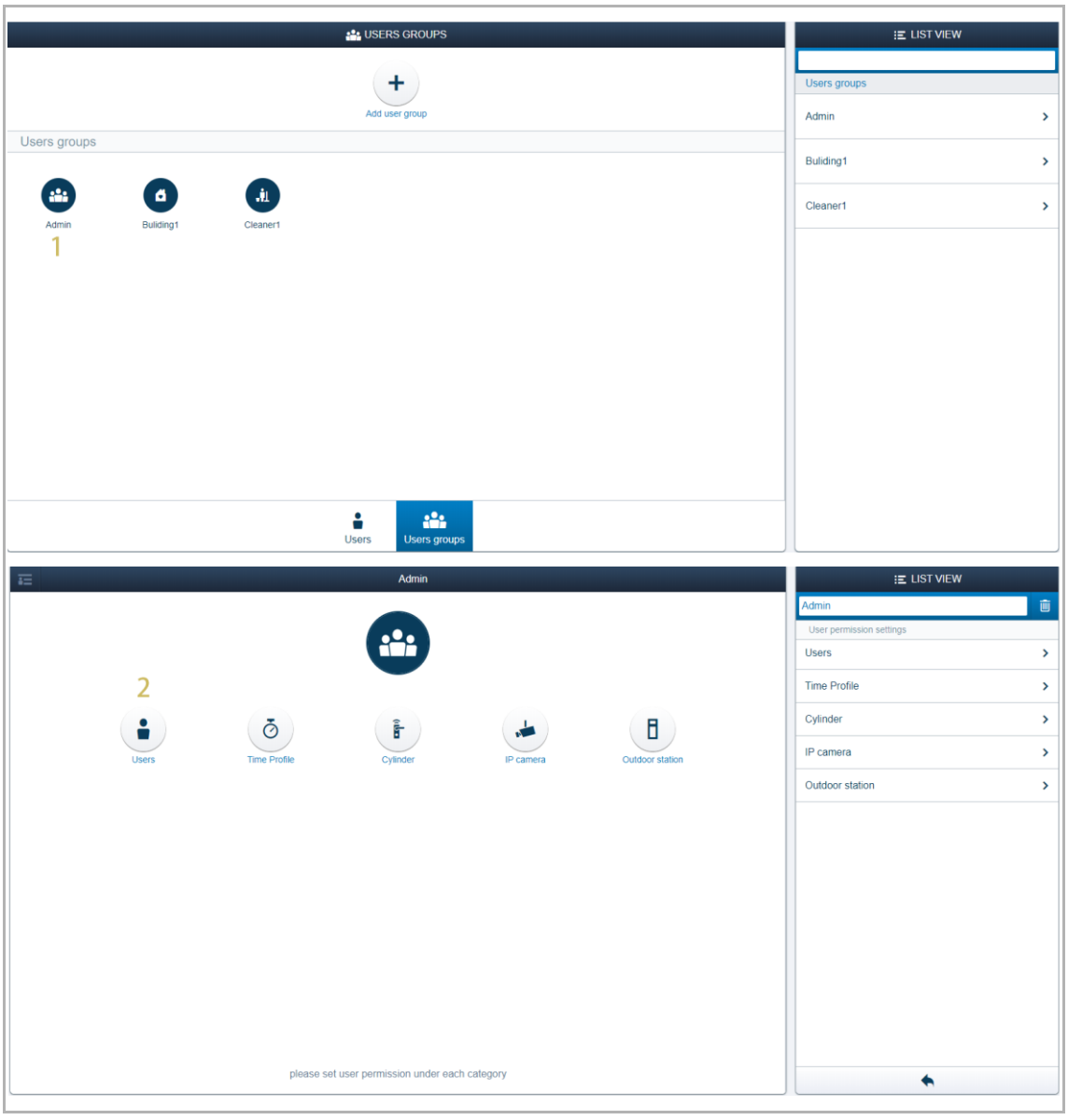


13.3.4 Assigning the users to a user group

Please follow the steps below:

[1] On the "User groups" screen, click a user group.

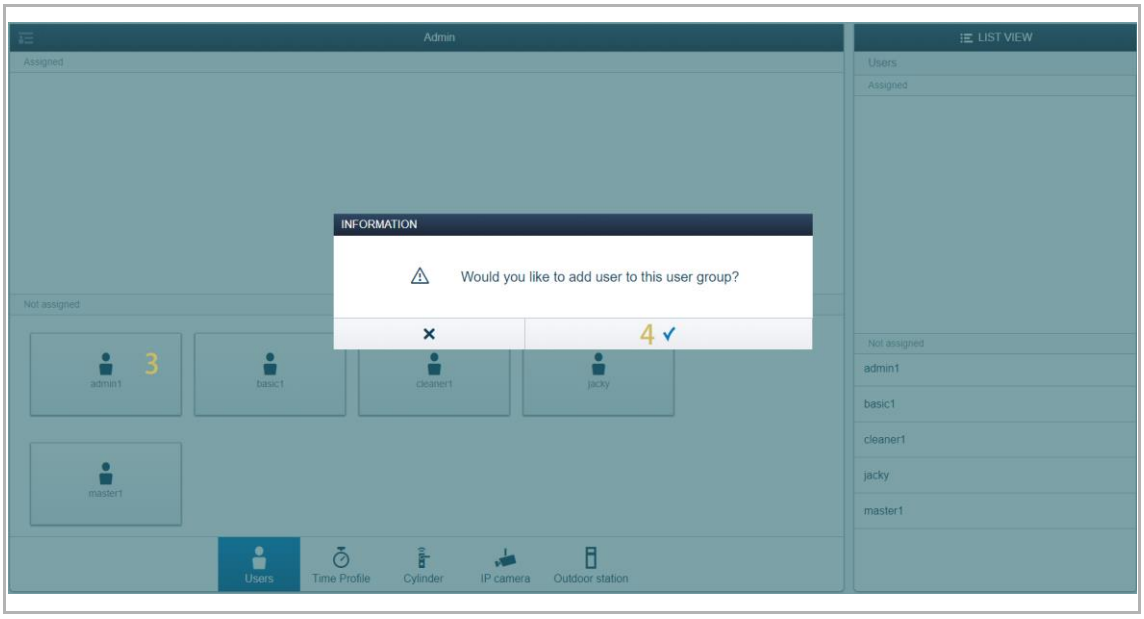
[2] Click "Users".



[3] On the designated user group screen, click the designated user on the "Not assigned" section.

[4] Click " √ " to confirm.

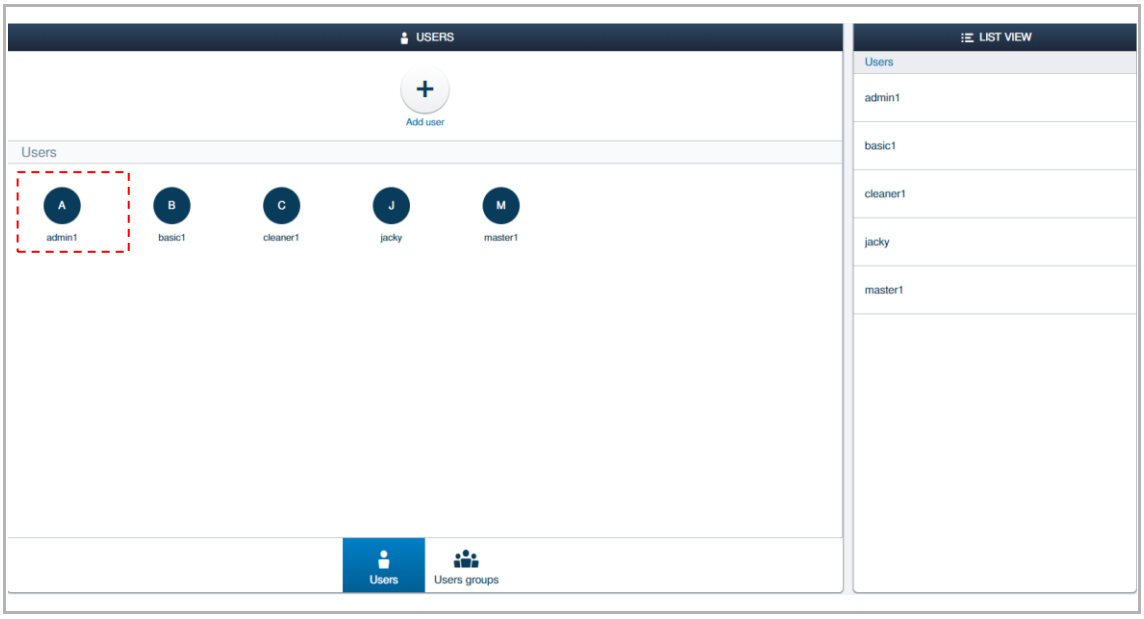
Repeat steps 3-4 to assign the designated users to a user group.



13.3.5 Configuring a user

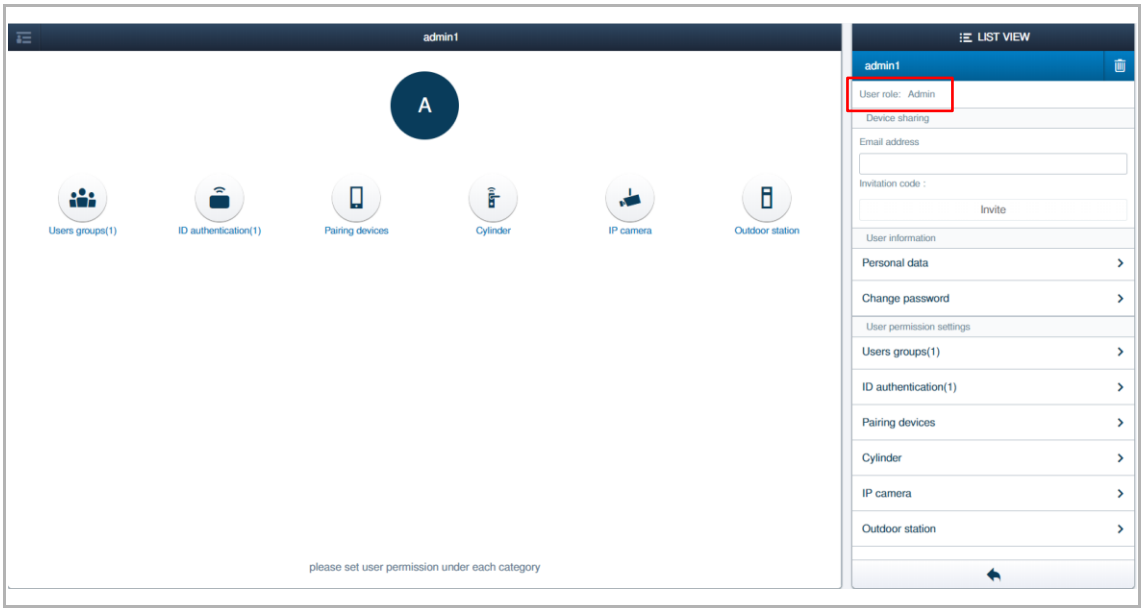
Accessing the designated user screen

On the "Users" screen, click the designated user to access the designated user screen.



1. View the user role

On the designated user screen, the user role can be viewed on the screen.



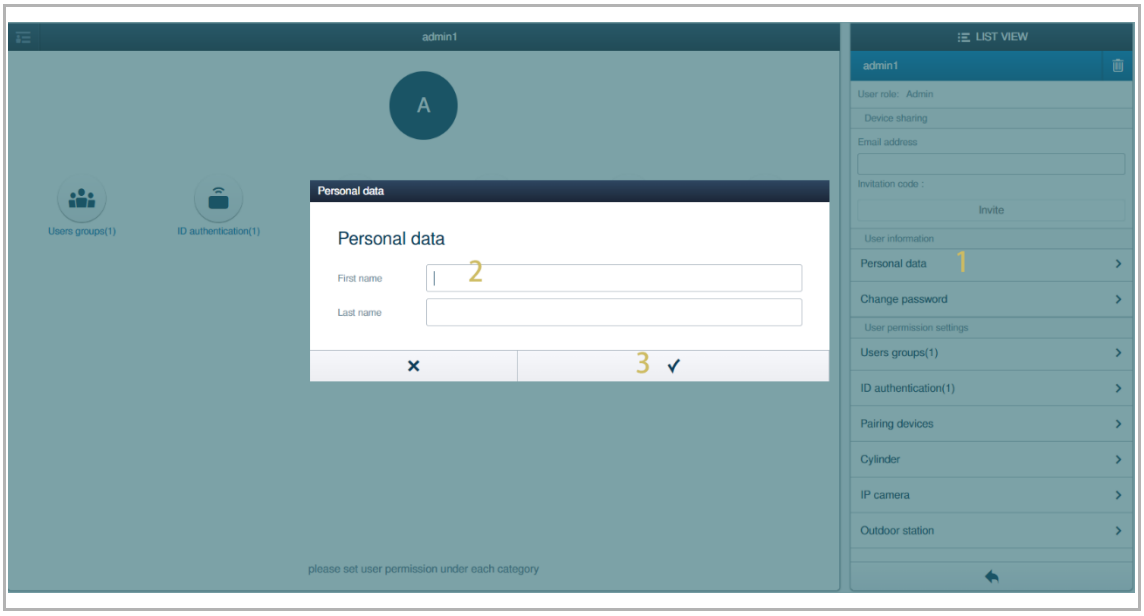
2. Changing the user name

On the designated user screen, follow the steps below:

[1] Click "Personal data".

[2] Enter the first name and the last name.

[3] Click " √ " to save.



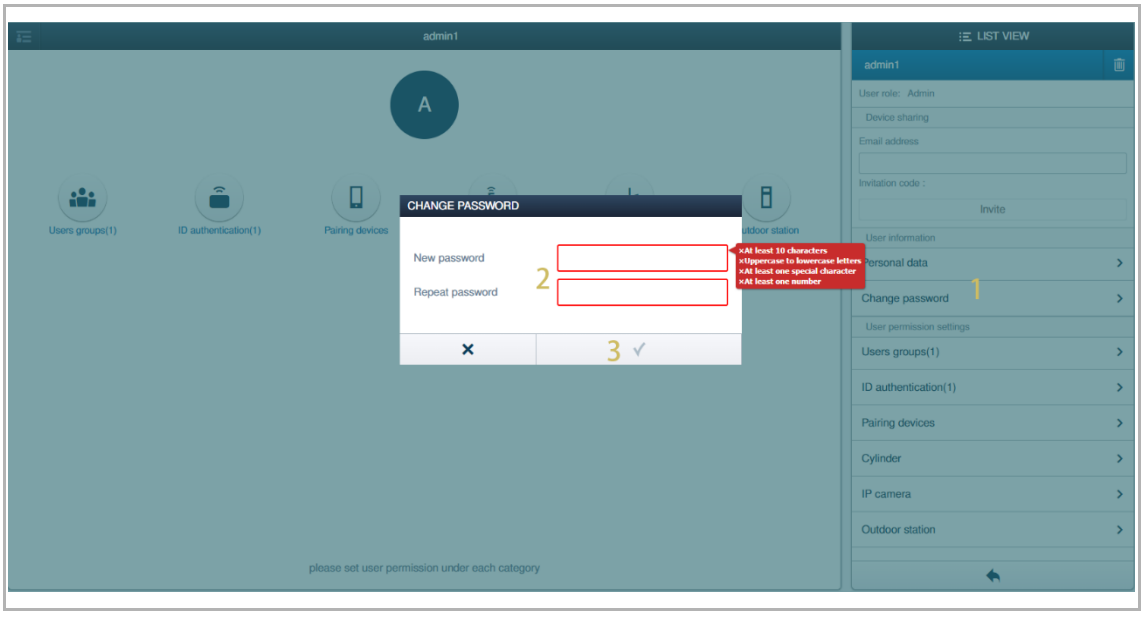
3. Changing the password

On the designated user screen, follow the steps below:

[1] Click "Change password".

[2] Enter the password twice according to the password rule displayed on the screen.

[3] Click " √ " to save.



4. Changing the validity period

Note
It is only applicable to 3rd party user.

On the designated user screen, follow the steps below:

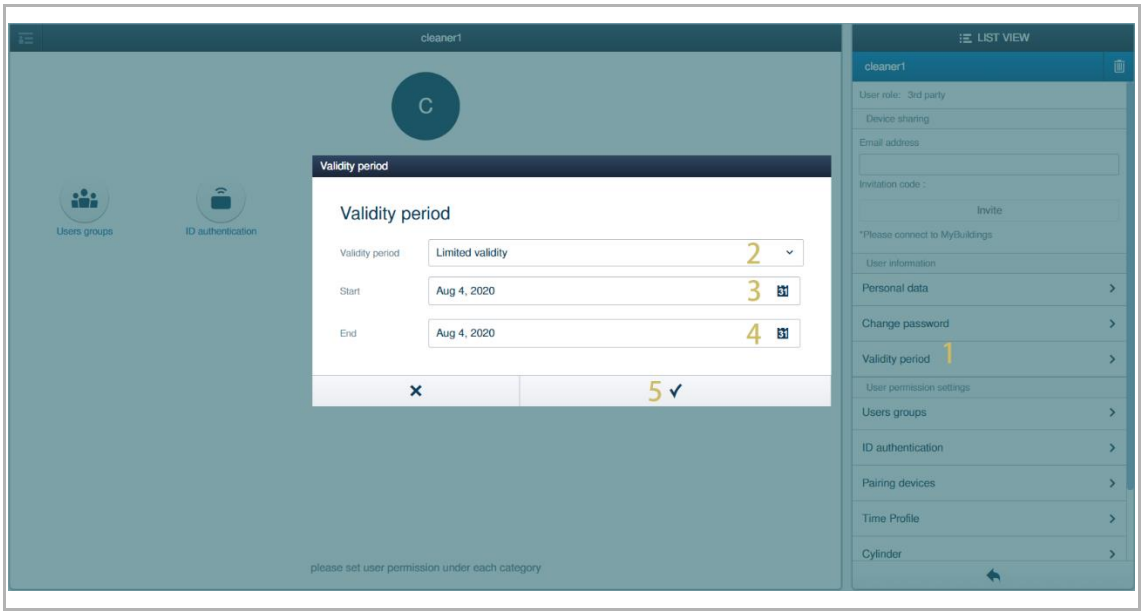
[1] Click "Validity period".

[2] Select "Limited validity" from the drop-down list.

[3] Set the start date via clicking " 31 ".

[4] Set the end date via clicking " 31 ".

[5] Click "OK" to save.

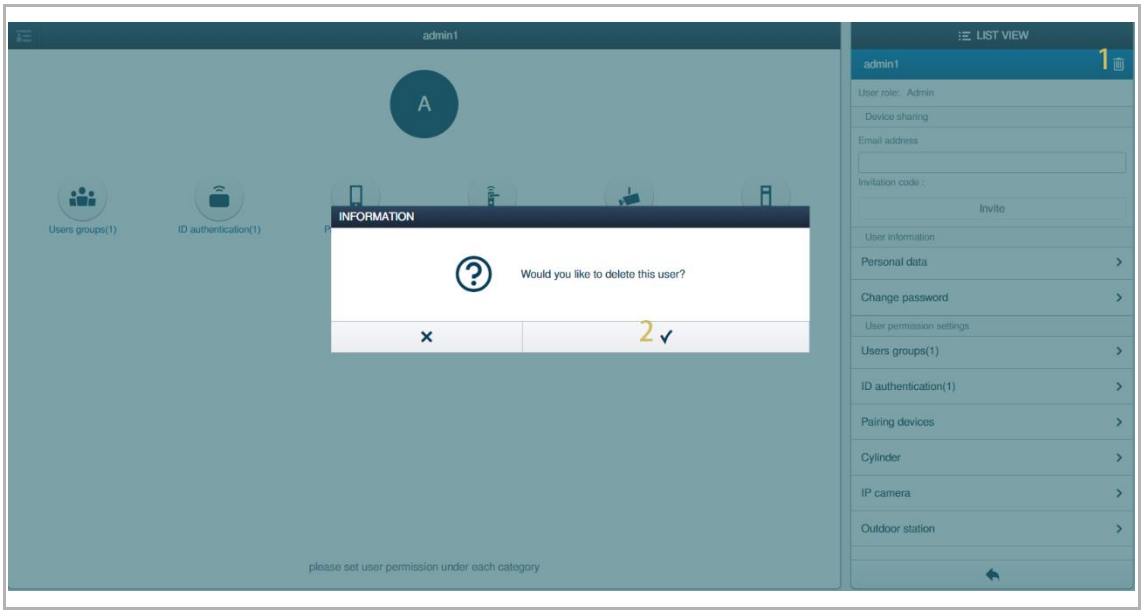


5. Removing a user

On the designated user screen, follow the steps below:

[1] Click "  ".

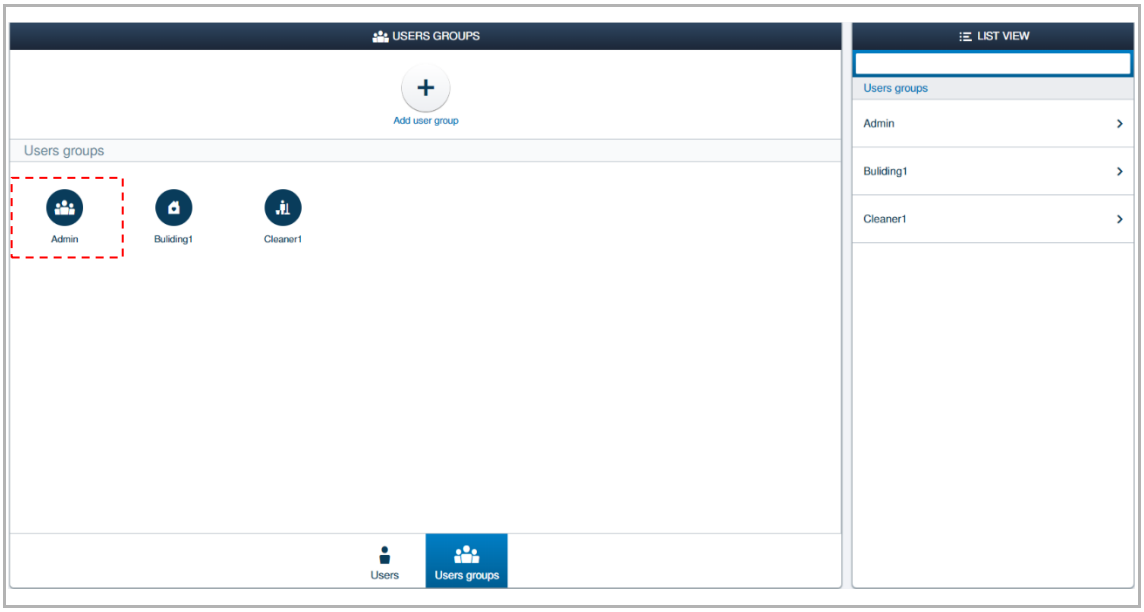
[2] Click " √ " to save.



13.3.6 Configuring a user group

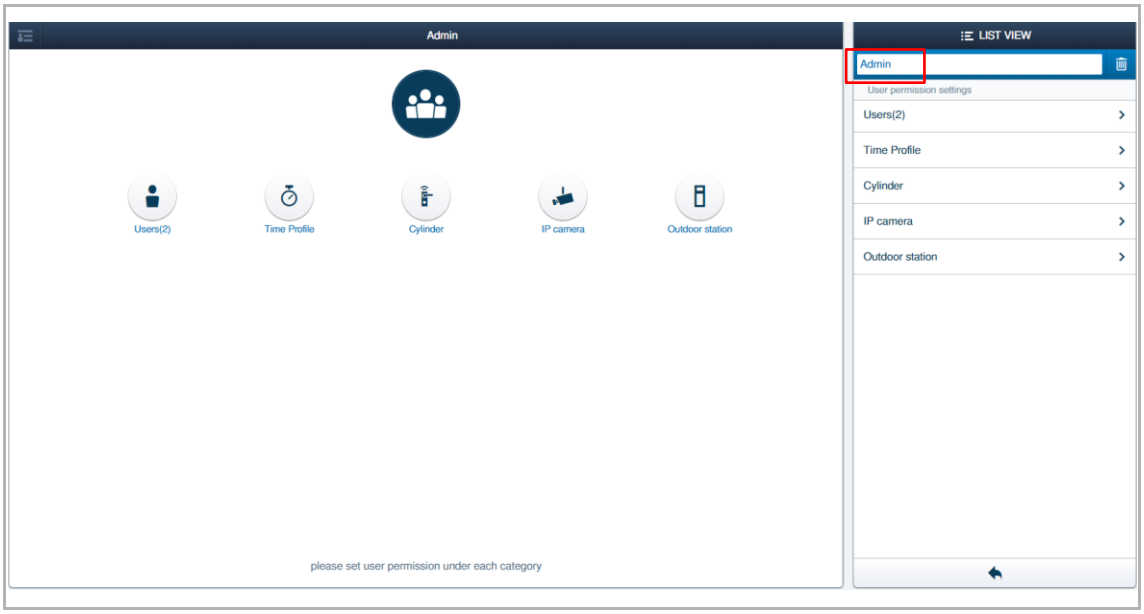
Accessing the designated group screen

On the "User groups" screen, click the designated group to access the designated group screen.



1. Changing the group name

On the designated group screen, click the group name and enter a new one.



13.4 Updating the firmware

13.4.1 Updating the firmware for "Smart Access Point"

1. Updating the firmware via local PC

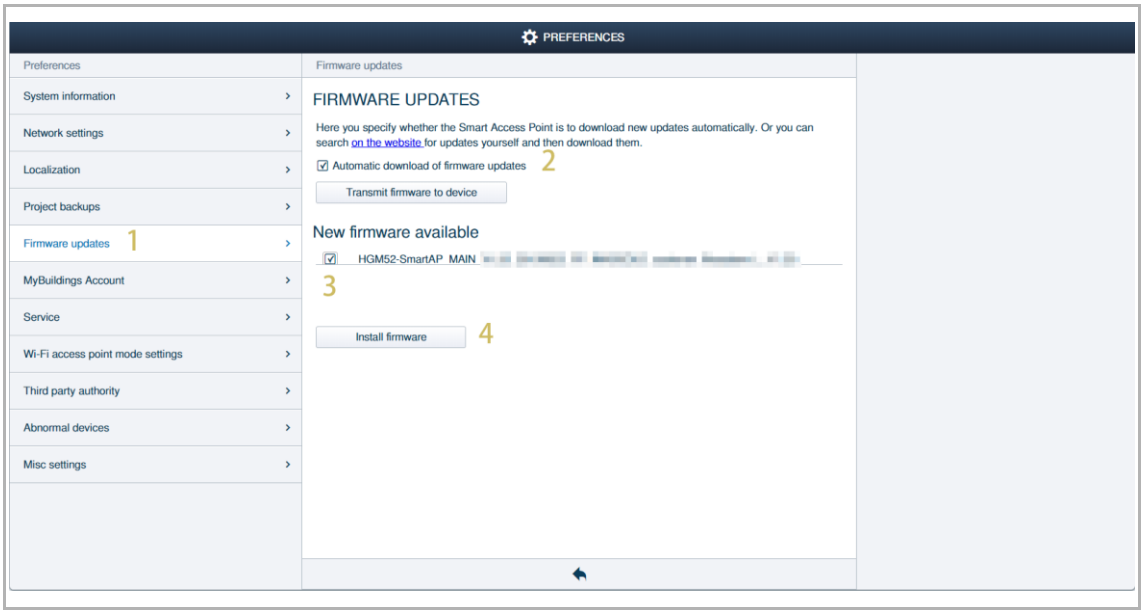
Please follow the steps below:

[1] On the "Preference" screen, click "Firmware updates".

[2] Tick the check box "Automatic download of firmware update". "Smart Access Point" will download the latest firmware from the website automatically.

[3] The latest firmware version is displayed here. Tick the designated check box.

[4] Click "Install firmware".



Note

"Smart Access Point" can only be updated to newer firmware.

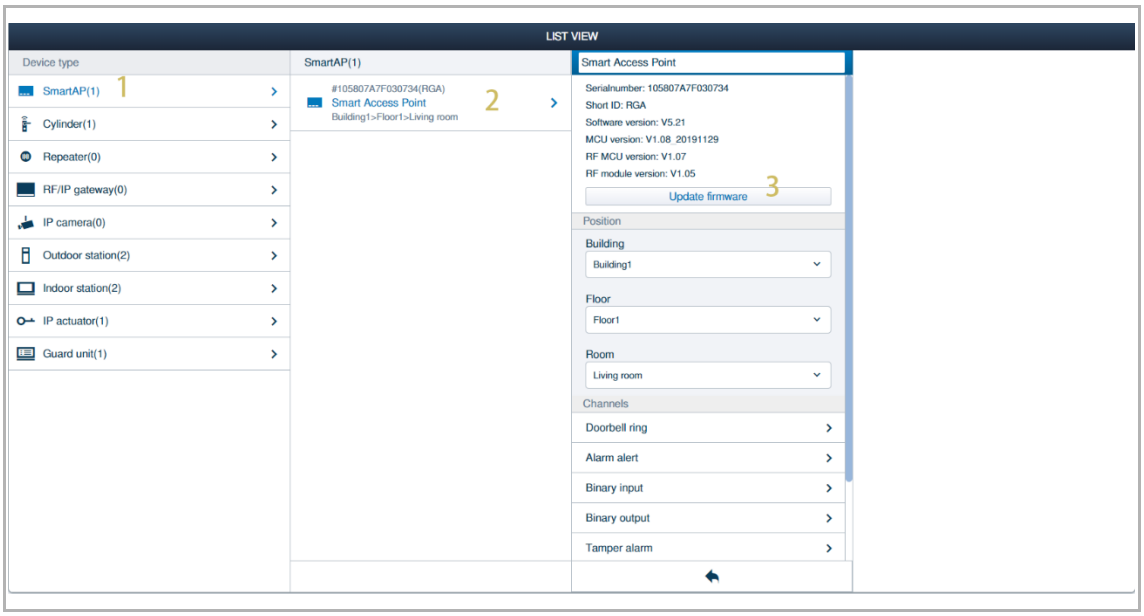
2. Updating the firmware via website

Please follow the steps below:

[1] On the "Device configuration" screen, click "SmartAP".

[2] Click "Smart Access Point".

[3] Click "Update firmware".



Note

"Smart Access Point" can only be updated to newer firmware.

13.4.2 Updating the firmware for Door Entry System devices

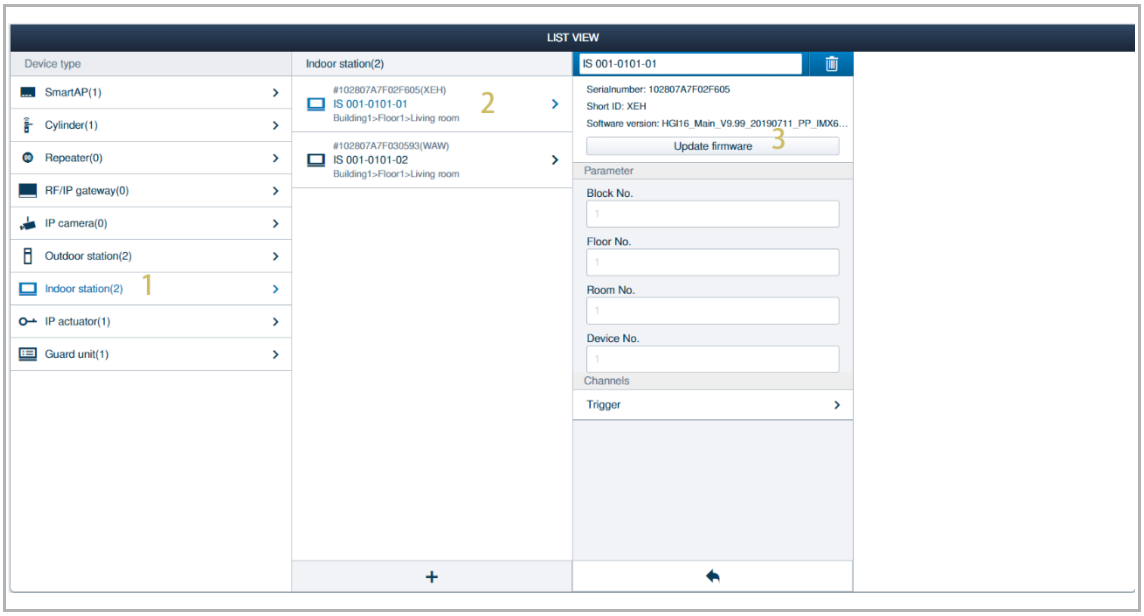
1. Updating the devices one by one

Please follow the steps below:

[1] On the "Device configuration" screen, click a Door Entry System device (e.g. "Indoor station").

[2] Click the designated Door Entry System device (e.g. "Indoor station 001").

[3] Click "Update firmware".



2. Updating the same types of devices in batches

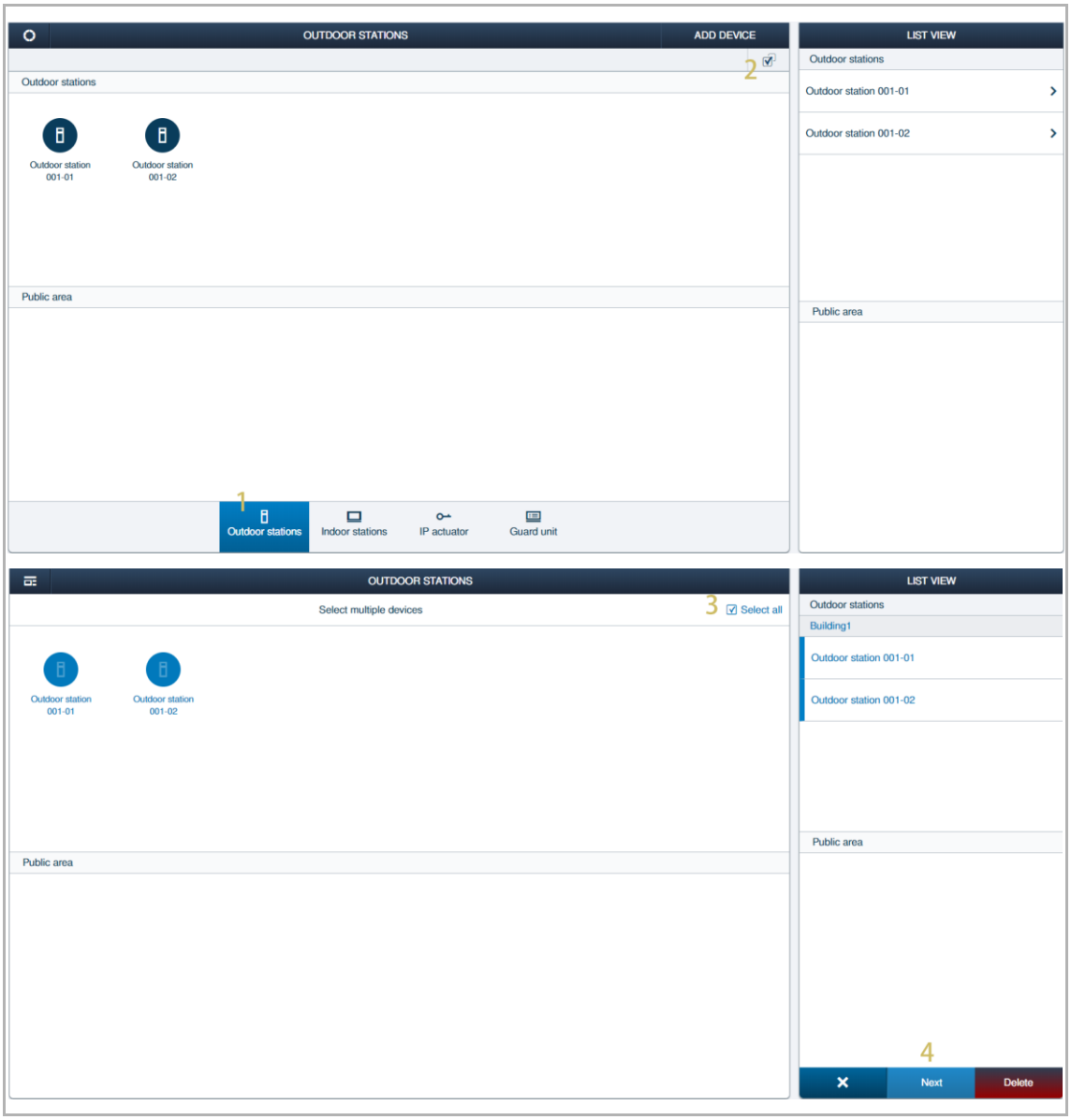
Please follow the steps below:

[1] On the "Device configuration" screen, click a Door Entry System device (e.g. "Outdoor station").

[2] Click "  ".

[3] Click "Select all" to select all devices or click the designated device one by one to select multiple devices.

[4] Click "Next".

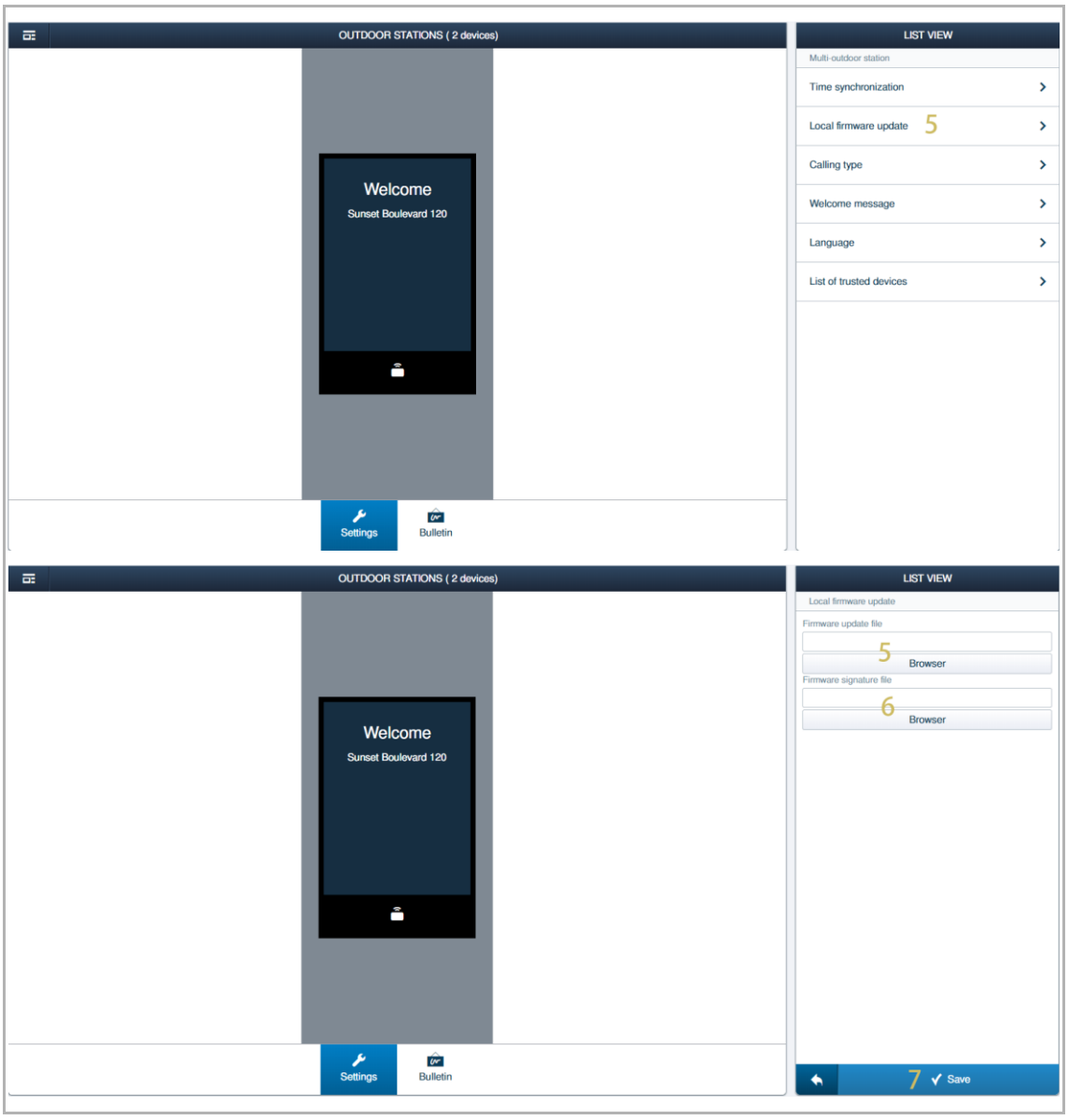


[5] Click "Local firmware update".

[6] Upload the firmware.

[7] Upload the signature.

[8] Click " √ " to save.



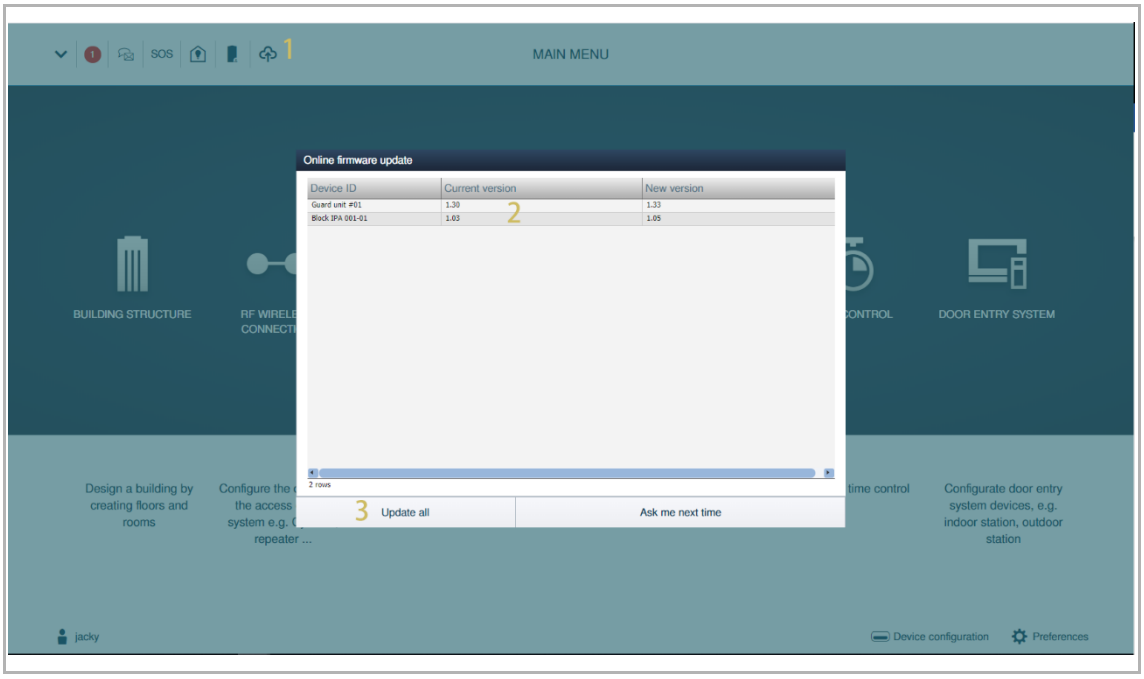
3. Updating the different types of devices in batche

Please follow the steps below:

[1] On the configuration screen, click " " ".

[2] The devices to be updated are displayed on the screen.

[3] Click "Update all" to update all the devices in batches.



Note

Only the Door Entry System devices which are placed on the public areas (e.g. Guard unit, building IPA, network IPA etc.) can be updated via this method.

13.4.3 Updating the firmware for AccessControl devices

1. Updating the firmware via local PC

Please follow the steps below:

[1] On the "Device configuration" screen, click an AccessControl device (e.g. "Cylinder").

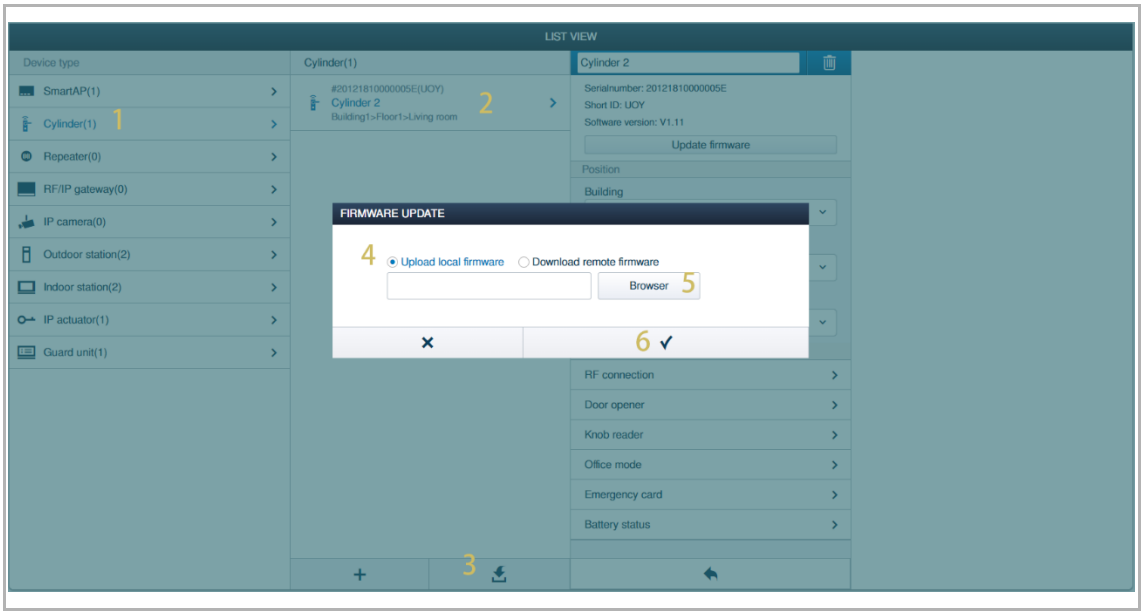
[2] Click the designated AccessControl device (e.g. "Cylinder2").

[3] Click "  ".

[4] Click "Upload local firmware".

[5] Browse your PC to select the firmware.

[6] Click " √ ".



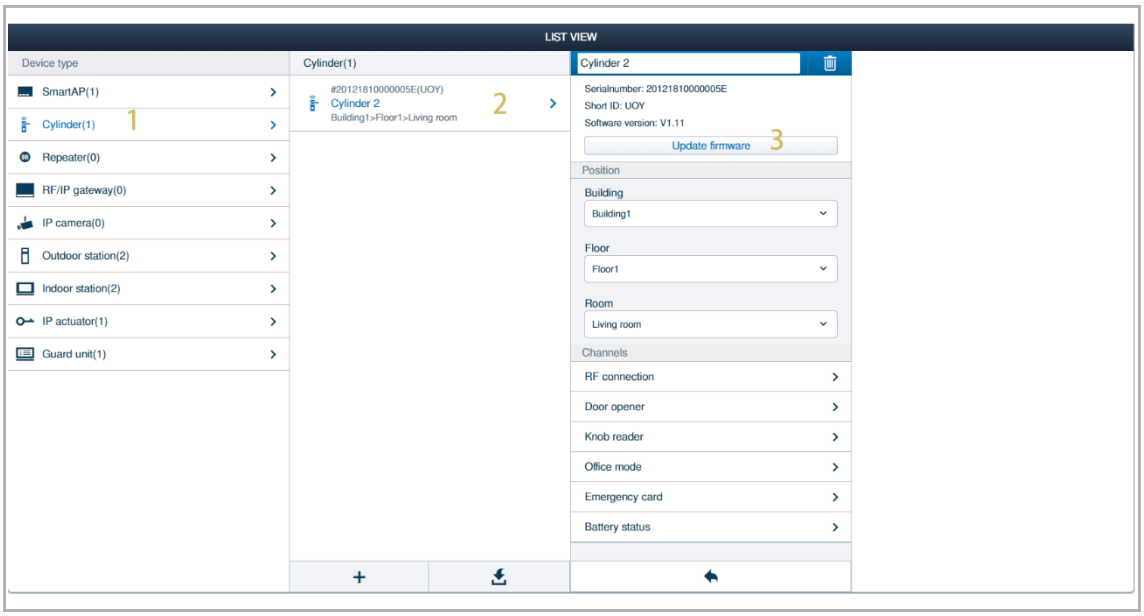
2. Updating the firmware via website

Please follow the steps below:

[1] On the "Device configuration" screen, click an AccessControl device (e.g. "Cylinder").

[2] Click the designated AccessControl device (e.g. "Cylinder2").

[3] Click "Update firmware".



13.5 Managing the backup

Overview of the backup

The following information will be stored in the backup:

- Device settings, user settings, building structure, place & link, message & logs.
- RF connections of the AccessControl devices.
- RF connections of "RF/IP Gateways".
- Certificates.

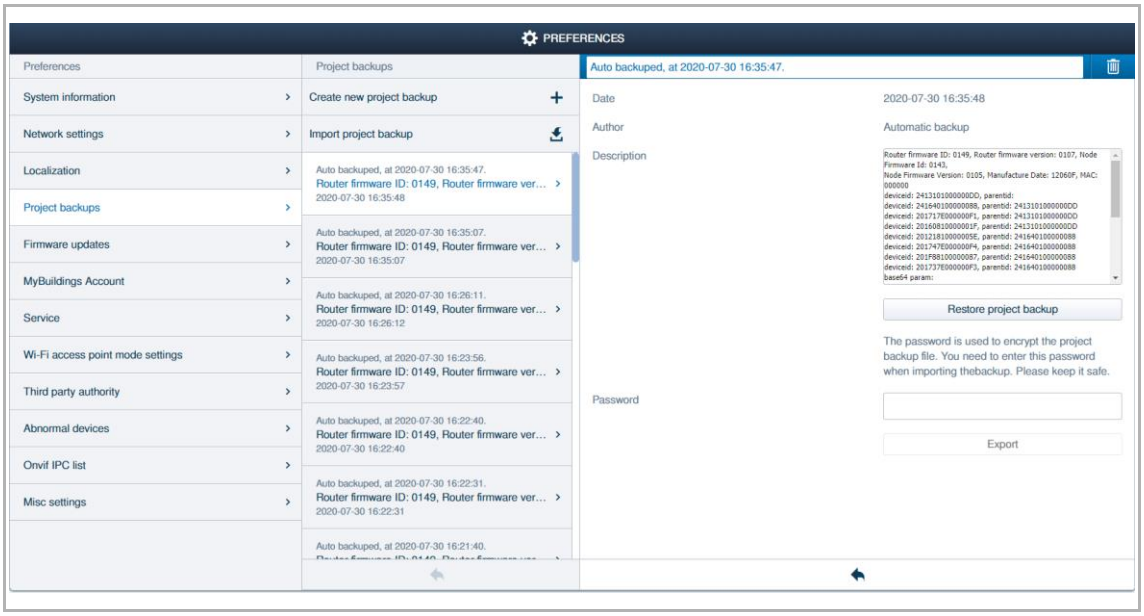
Attention!

A project backup is very important and necessary for the AccessControl devices. If no backup is created in advance, all the AccessControl devices will be invalid when current "Smart Access Point" is broken. These AccessControl devices can’t be used by a new "Smart Access Point" directly without a backup. You have to send these devices back to the factory to repair.

Access the backup screen

On the configuration screen, click ""Preferences", followed by "Project backups" to access the backup screen.

There are some auto-saved backups displayed in the list.



13.5.1 Creating the backup

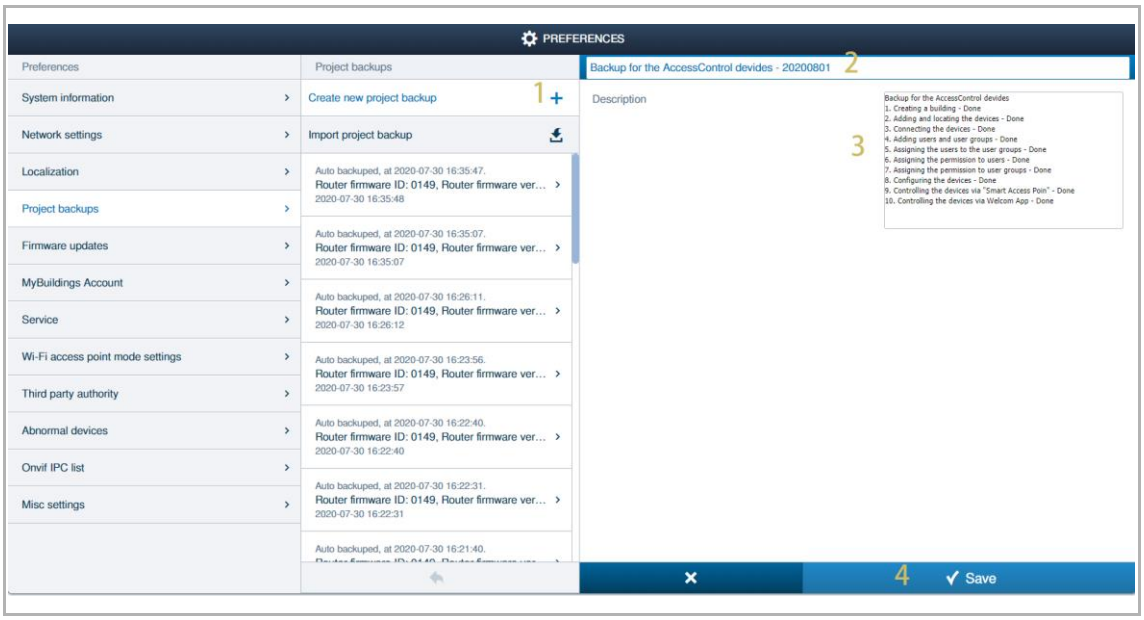
Please follow the steps below to create a backup and save it on the current "Smart Access Point":

[1] On the backup screen, click " + ".

[2] Enter the name.

[3] Enter the description.

[4] Click " √ " to save.



Attention!

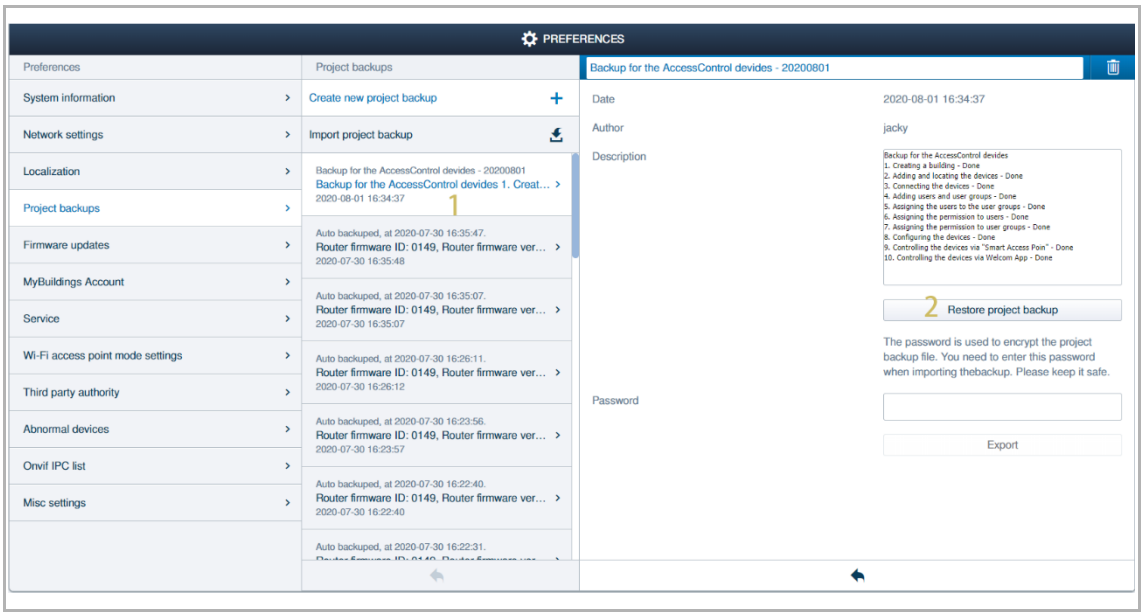
The backup is saved to the current "Smart Access Point". It is recommended to export the backup to PC in case the current "Smart Access Point" is broken.

13.5.2 Restoring the backup

Please follow the steps below to restore a backup from the current "Smart Access Point":

[1] On the backup screen, click the designated backup.

[2] Click "Restore project backup".



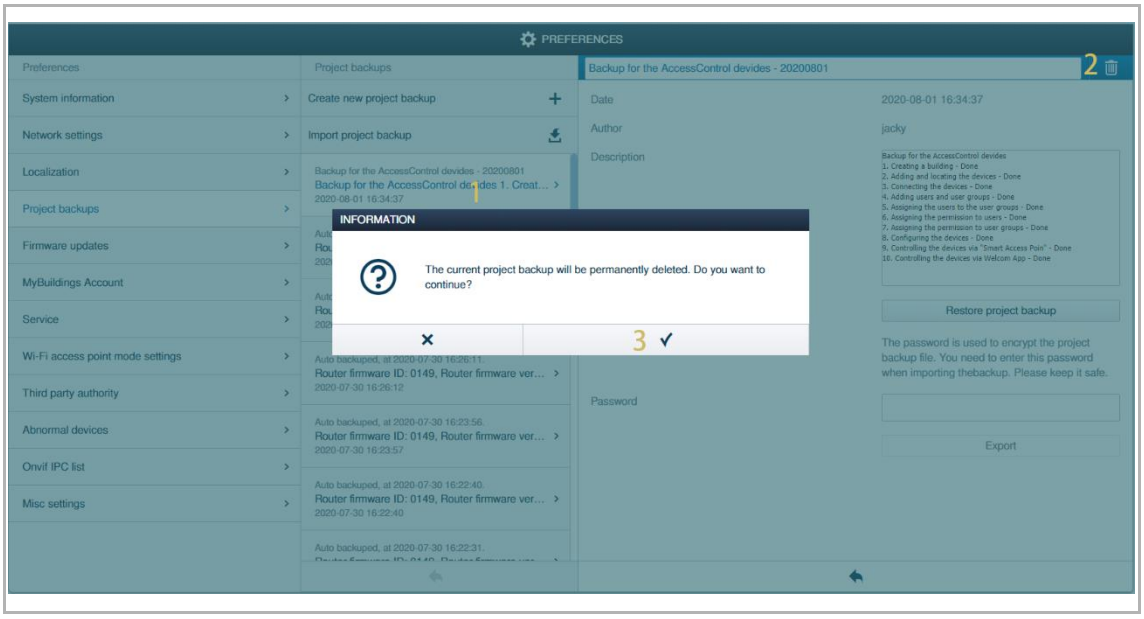
13.5.3 Removing the backup

Please follow the steps below to remove a backup from the current "Smart Access Point":

[1] On the backup screen, click the designated backup.

[2] Click " " ".

[3] Click "√" to confirm.



13.5.4 Exporting the backup

Please follow the steps below to export a backup from the current "Smart Access Point" to PC:

[1] On the backup screen, click the designated backup.

[2] Enter a recovery password according the password rule. The recovery password is used to import the backup from PC.

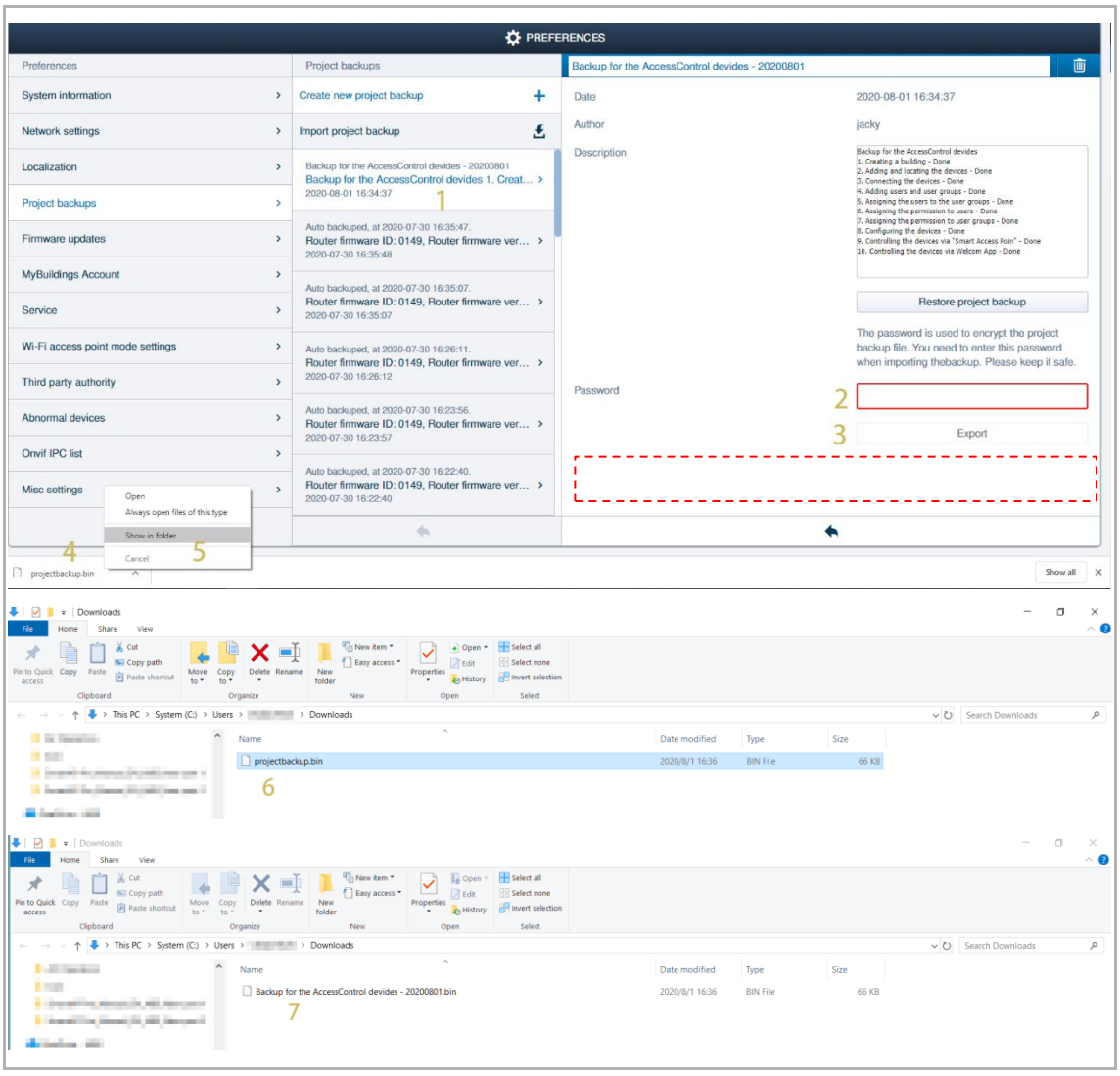
[3] Click "Export" to export the backup to PC.

[4] Right click the backup file.

[5] Click "Show in folder".

[6] The backup is displayed in the folder.

[7] Rename the backup.



13.5.5 Importing the backup

Please follow the steps below to import a backup from PC:

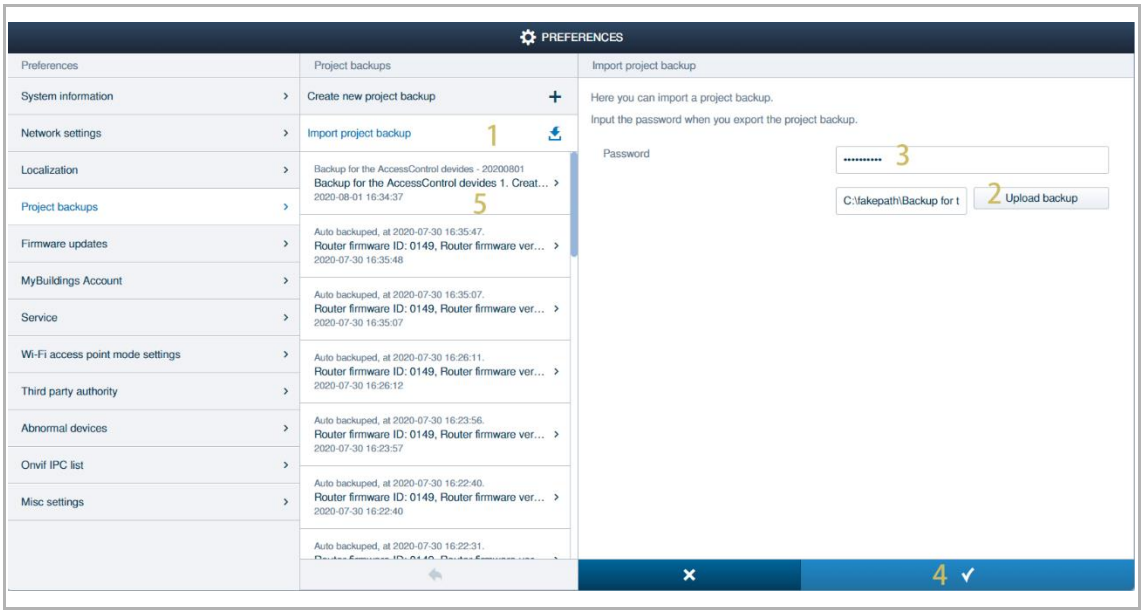
[1] On the backup screen, click " ".

[2] Click "Upload backup", select the backup from your PC.

[3] Enter the recovery password. see chapter 13.5.4 “Exporting the backup“ on page 330.

[4] Click " √ ".

[5] The backup is displayed in the list.



Note

You need to continue the "Resorting a backup" operation for the imported file to take effect. see chapter 13.5.2 “Restoring the backup“ on page 328.

13.6 Restoring to factory default

13.6.1 Restoring the AccessControl devices

You can reset the building If you want to reset all the AccessControl devices.

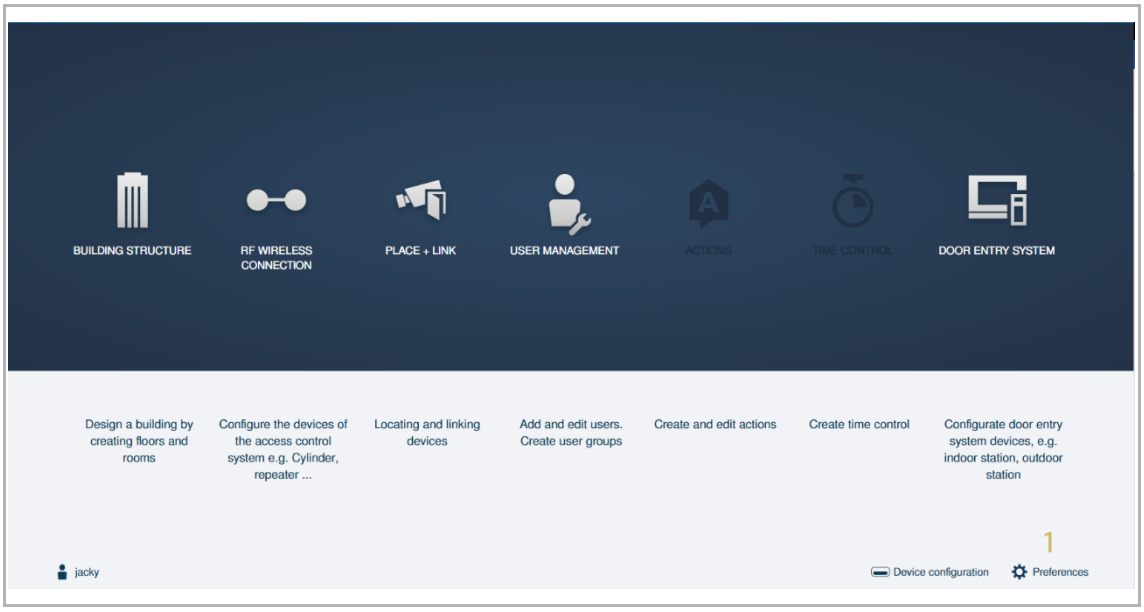
Attention!

You need to create a backup for the AccessControl devices before reset the building. see chapter 13.5.1 “Creating the backup“ on page 327.

You need to disconnect all the AccessControl devices before resetting the building. see chapter 10.11 “Disconnecting the devices“ on page 259.

Please follow the steps below:

[1] On the configuration screen, click "Preference" to access the corresponding screen.



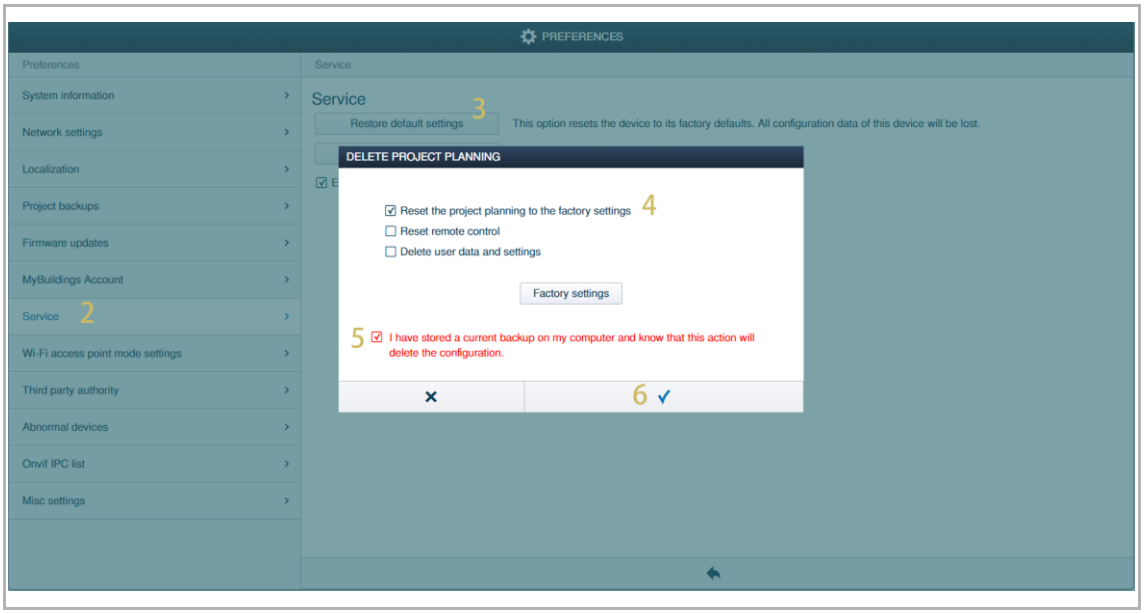
[2] On the "Preference" screen, click "Service".

[3] Click “Restore default settings".

[4] Tick the check box "Reset the project planning to the factory settings".

[5] Tick the check box "I have stored …".

[6] Click "√" to confirm.



13.6.2 Accessing "Smart Access Point" remotely

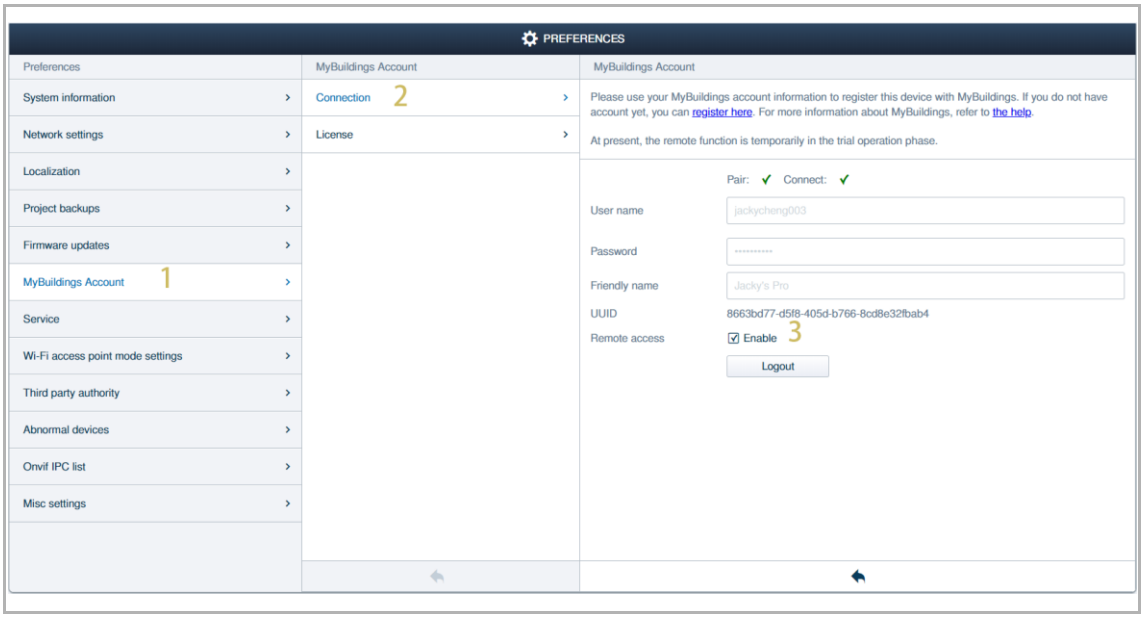
1. Enable the "Remote access" function

Please follow the steps below:

[1] On the "Preference" screen, click "MyBuildings Account".

[2] Click "Connection".

[3] Tick the check box "Remote access".

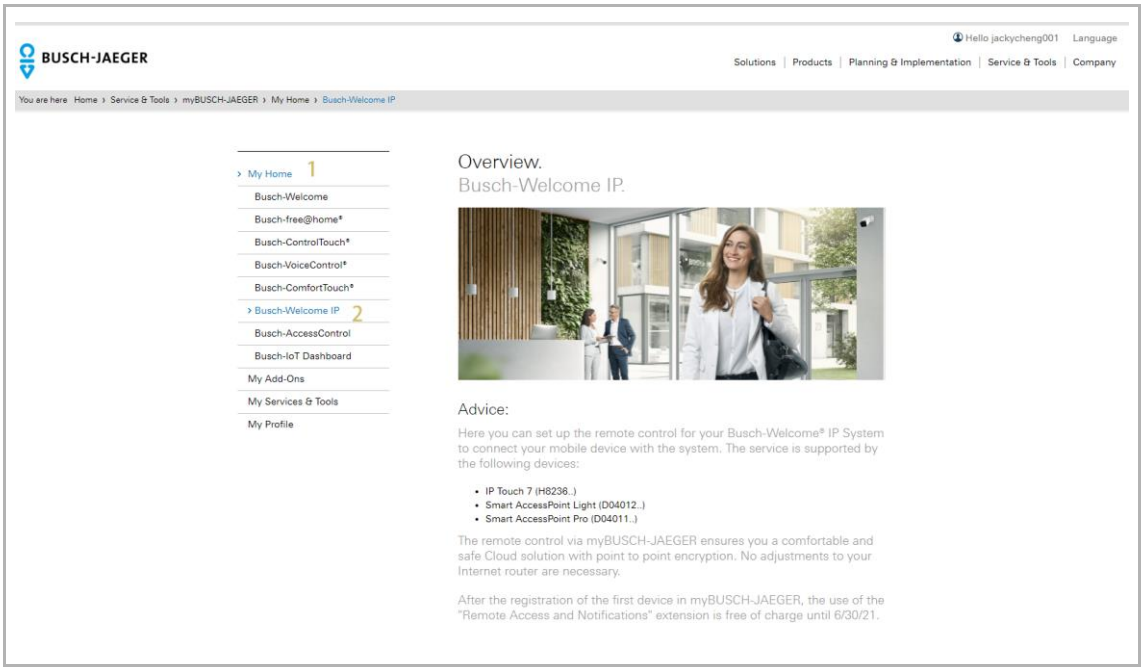


2. Accessing "Smart Access Point" on the myBUSCH-JAGER Portal

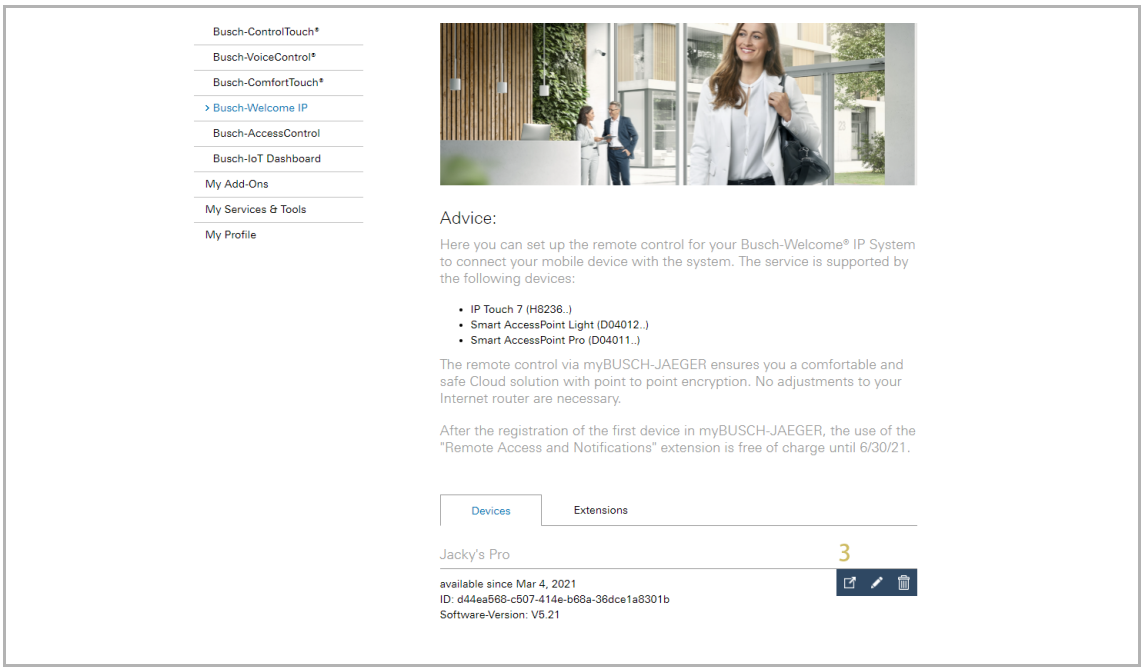
Please follow the steps below:

[1] On the home page of the myBUSCH-JAGER, click "My Home".

[2] Click "Busch-Welcome IP".



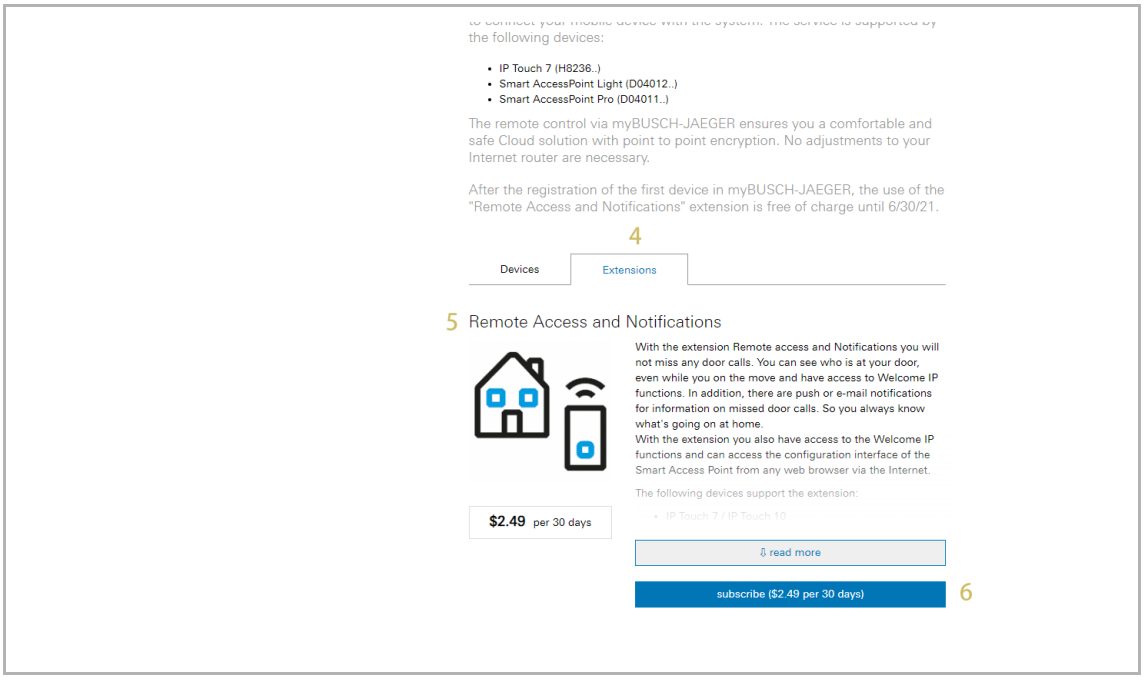
[3] Scroll down the screen and find your "Smart Access Point", click " ".



[4] If you cannot open the screen, click "Extensions".

[5] Find the "Remote Access and Notifications" item.

[6] Click "Subscribe" to purchase the service.



13.6.3 Restoring the "Remote control" function

"Smart Access Point" can be accessed remotely on the myBUSCH-JAEGER portal. see chapter 13.6.2 “Accessing "Smart Access Point" remotely“ on page 334.

If you want to restore the "Remote control" function, please follow the steps below:

[1] On the configuration screen, click "Preference" to access the corresponding screen.

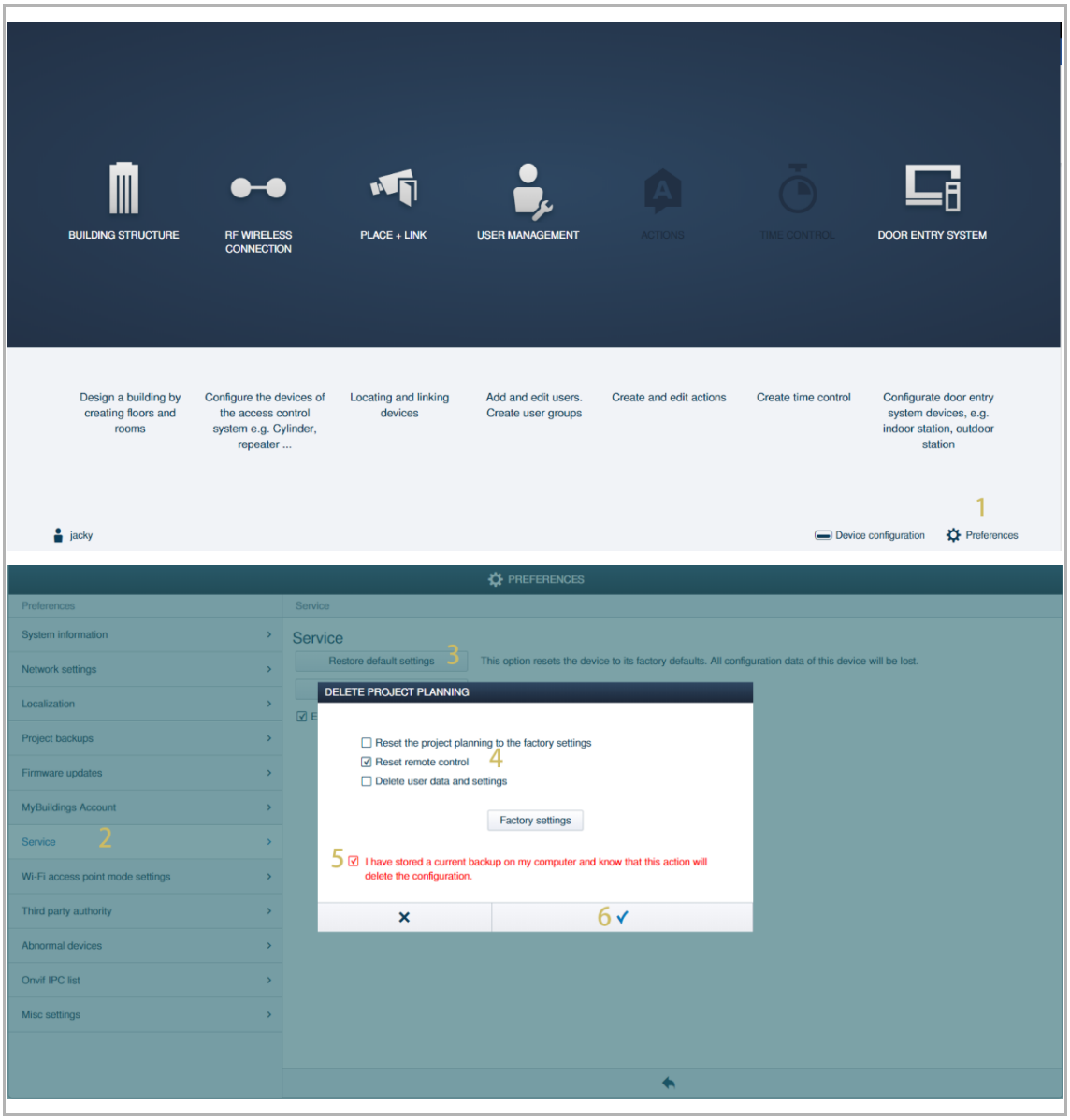
[2] On the "Preference" screen, click "Service".

[3] Click “Restore default settings".

[4] Tick the check box "Reset remote control".

[5] Tick the check box "I have stored …".

[6] Click "√" to confirm.



13.6.4 Restoring all settings to the factory defaults

Please follow the steps below:

[1] On the configuration screen, click "Preference" to access the corresponding screen.

[2] On the "Preference" screen, click "Service".

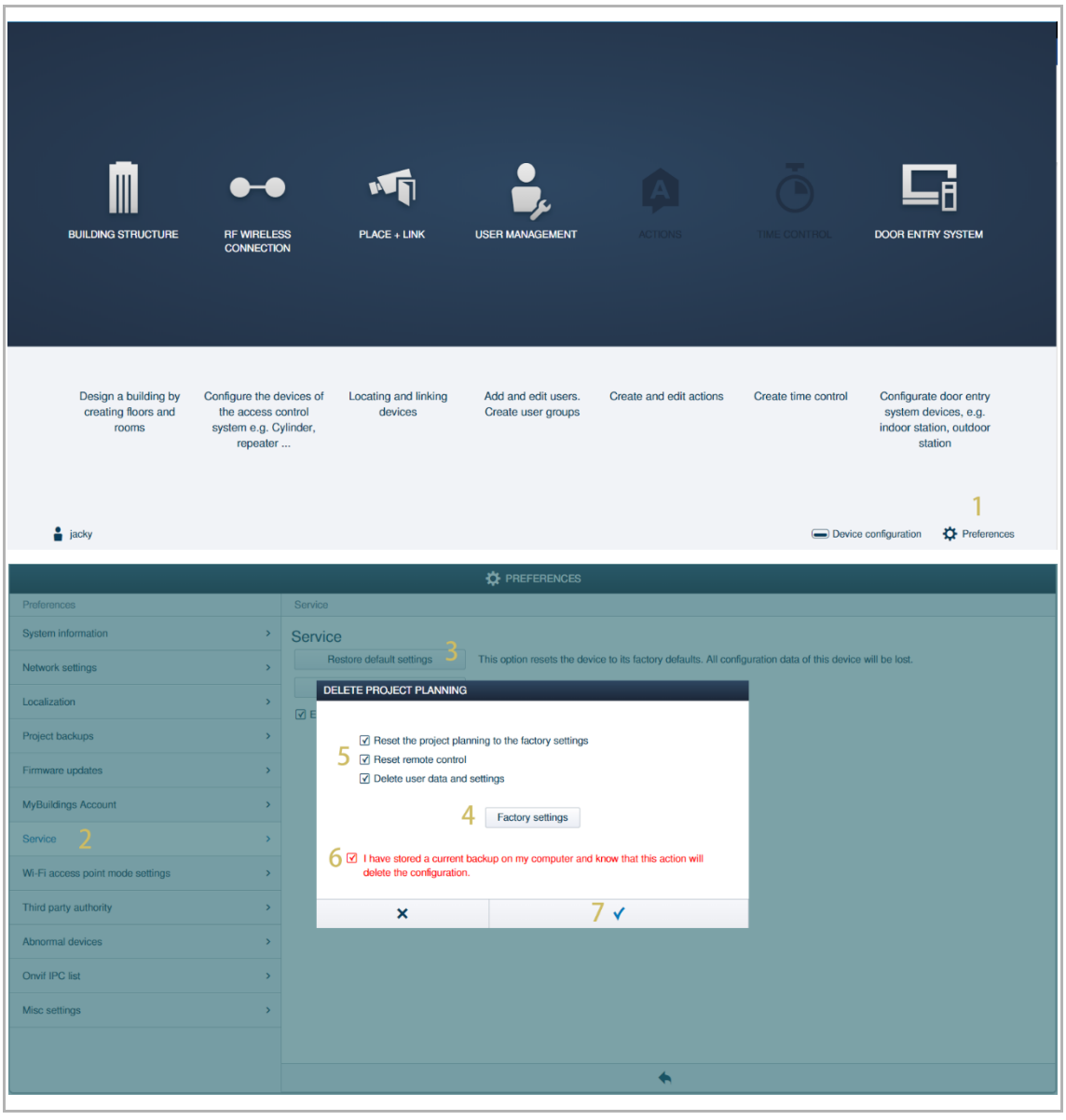
[3] Click “Restore default settings".

[4] Click "Factory settings".

[5] All the check boxes are ticked automatically.

[6] Tick the check box "I have stored …".

[7] Click "√" to confirm.

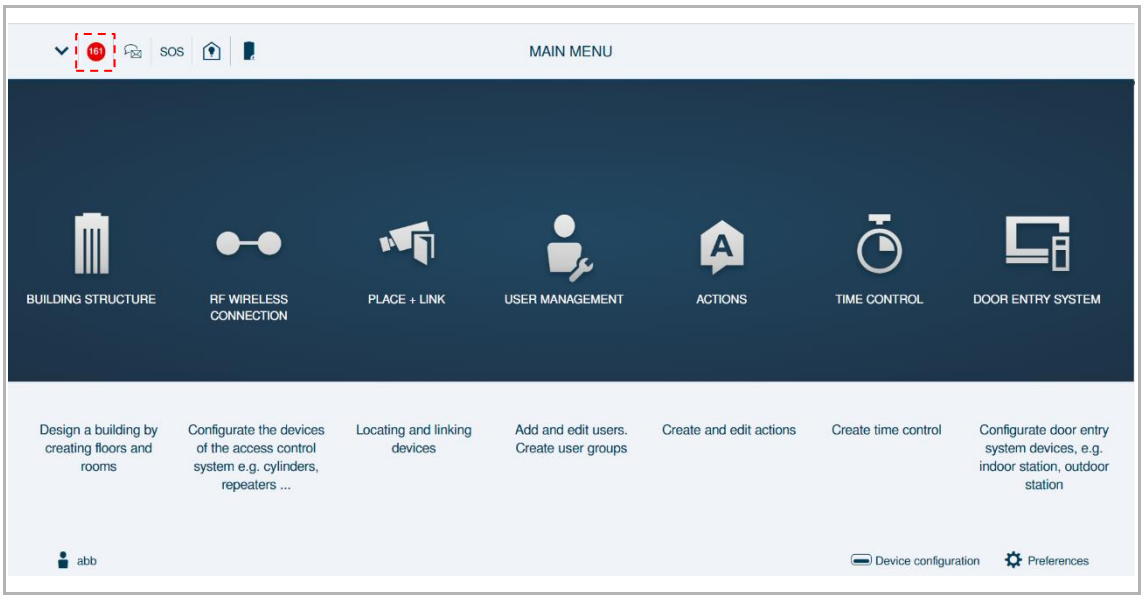


13.7 Notification

Access the "Notification" screen

On the configuration screen, click  to access the "Notification" screen.

A maximum of 16,000 notifications are supported on "Smart Access Point".



13.7.1 Notification

In the "Notification" view, all notifications that are defined and triggered under "Actions" are documented in the Smart Access Point.

A notification is not always associated with an action by the administrator and is used for information purposes only.

Please follow the steps below:

[1] On the "Notification" screen, click "Notification".

[2] Enter the key word.

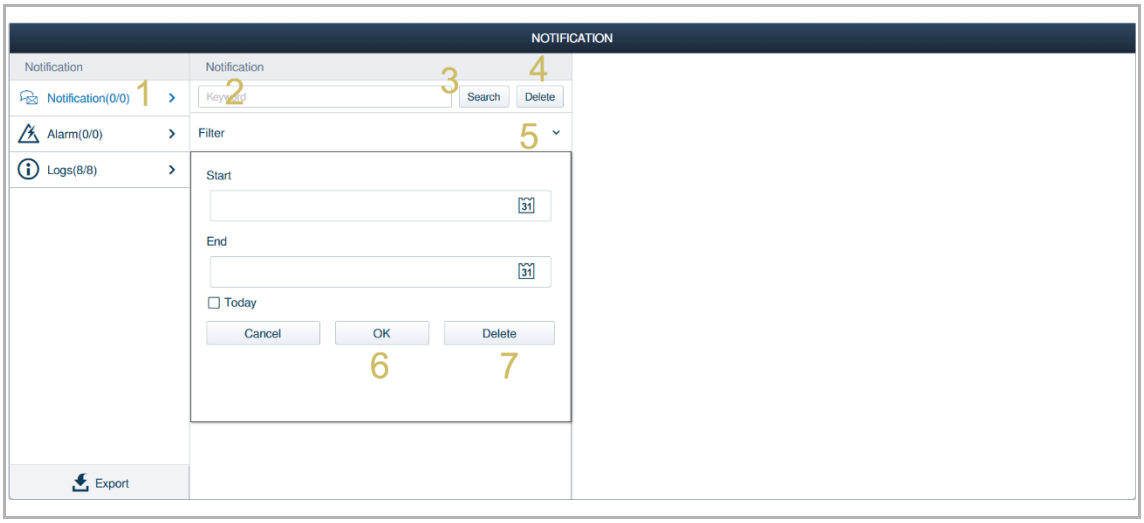
[3] Press "Search", all results will be displayed on the screen, click a result to view the details and click to remove this record.

[4] Press "Delete" to delete all the searching results.

[5] Click " " to set the filter. Enter the start date and end date to filter the notifications by date. Tick the check box "Today" to filter today's notifications.

[6] Click "OK" to confirm the filter.

[7] Click "Delete" to clear the filter.



13.7.2 Alarm record

In the "Alarm" view, alarms that occur in the system are documented in the Smart Access Point.

An alarm is always associated with an action by the administrator. e.g. battery change on the cylinder is necessary.

Please follow the steps below:

[1] On the "Notification" screen, click "Alarm".

[2] Enter the key word.

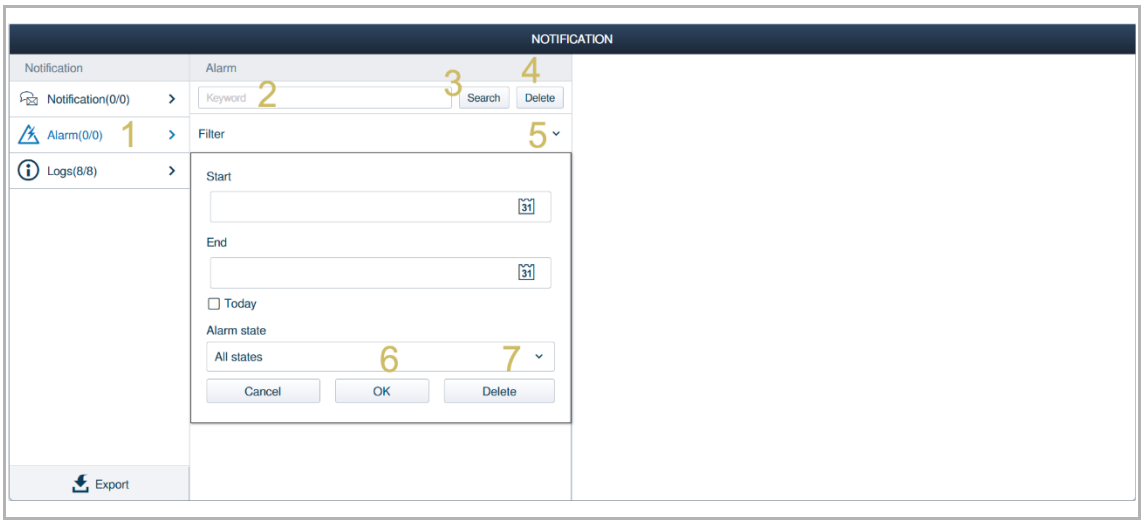
[3] Press "Search", all results will be displayed on the screen, click a result to view the details and click  to remove this record.

[4] Press "Delete" to delete all the searching results.

[5] Click " ⌄ " to set the filter. Enter the start date and end date to filter the notifications by date. Tick the check box "Today" to filter today's notifications.

[6] Click "OK" to confirm the filter.

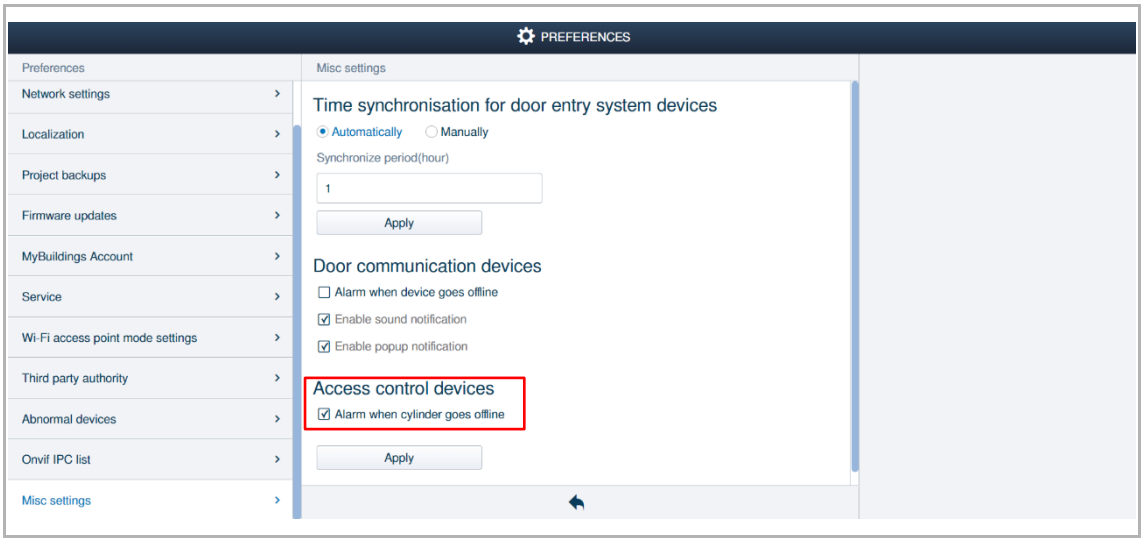
[7] Click "Delete" to clear the filter.



Alarm records about AC devices

On the "Preferences" – "Misc settings" screen, tick the checkbox "Alarm when cylinder goes offline".

After this setting, when the AC devices are offline, alarm records about AC devices will be created.



13.7.3 Logs

In the "Log" view, non-critical actions that occur in the system are documented in the Smart Access Point.

A log entry is not associated with an action by the administrator and is used for information purposes only.

Please follow the steps below:

[1] On the "Notification" screen, click "Logs".

[2] Enter the key word.

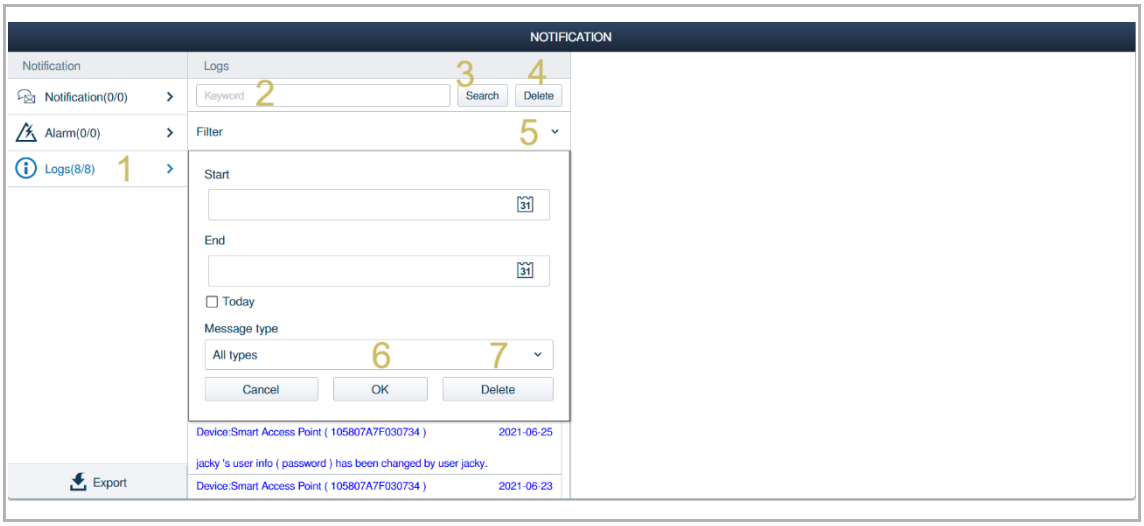
[3] Press "Search", all results will be displayed on the screen, click a result to view the details and click  to remove this record.

[4] Press "Delete" to delete all the searching results.

[5] Click " ⌄ " to set the filter. Enter the start date and end date to filter the notifications by date. Tick the check box "Today" to filter today's notifications.

[6] Click "OK" to confirm the filter.

[7] Click "Delete" to clear the filter.



13.7.4 Exporting the notifications

Please follow the steps below:

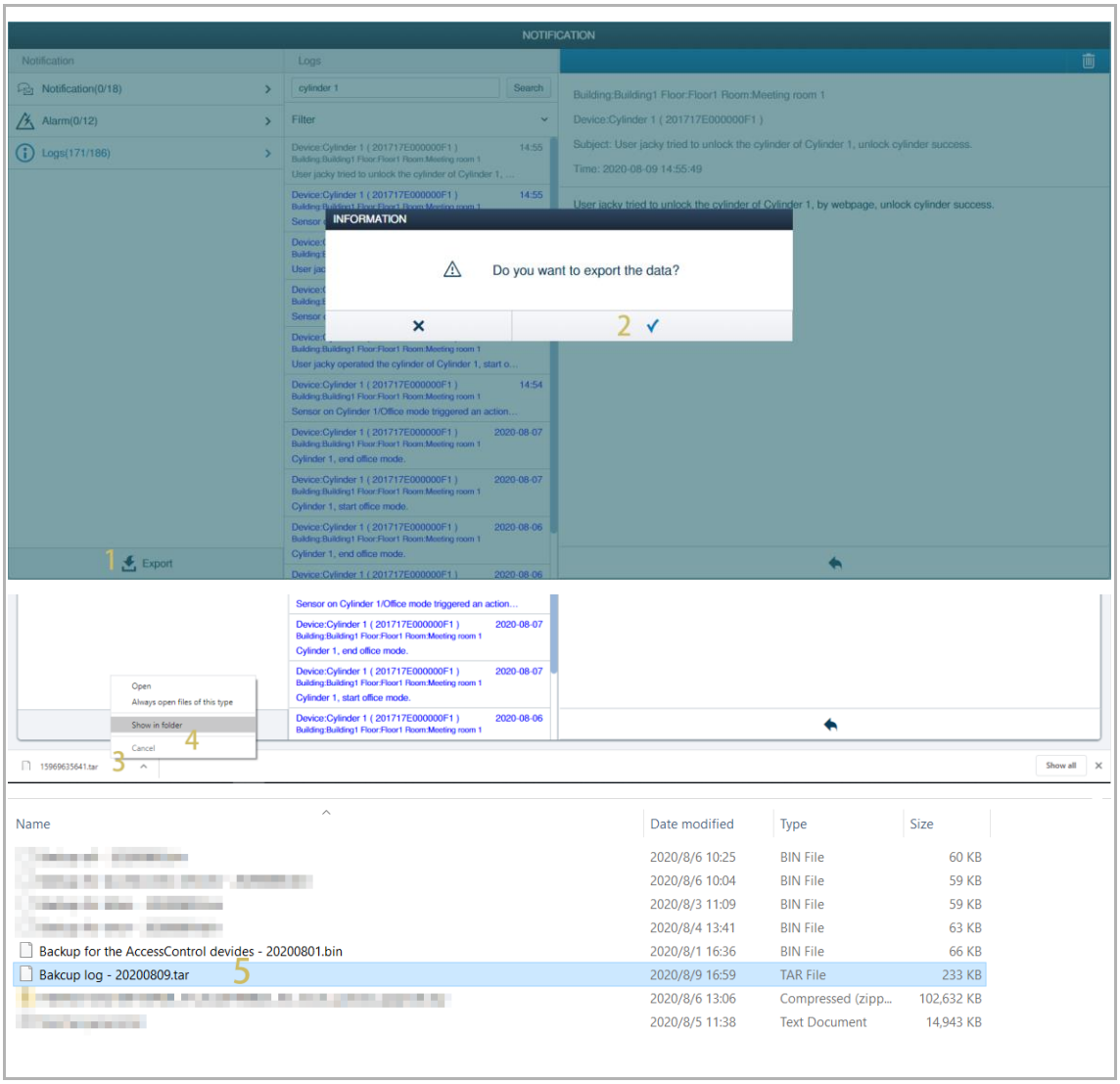
[1] On the "Notification" screen, click "Export".

[2] Click " √ ".

[3] Right click the exported file.

[4] Click "Show in folder".

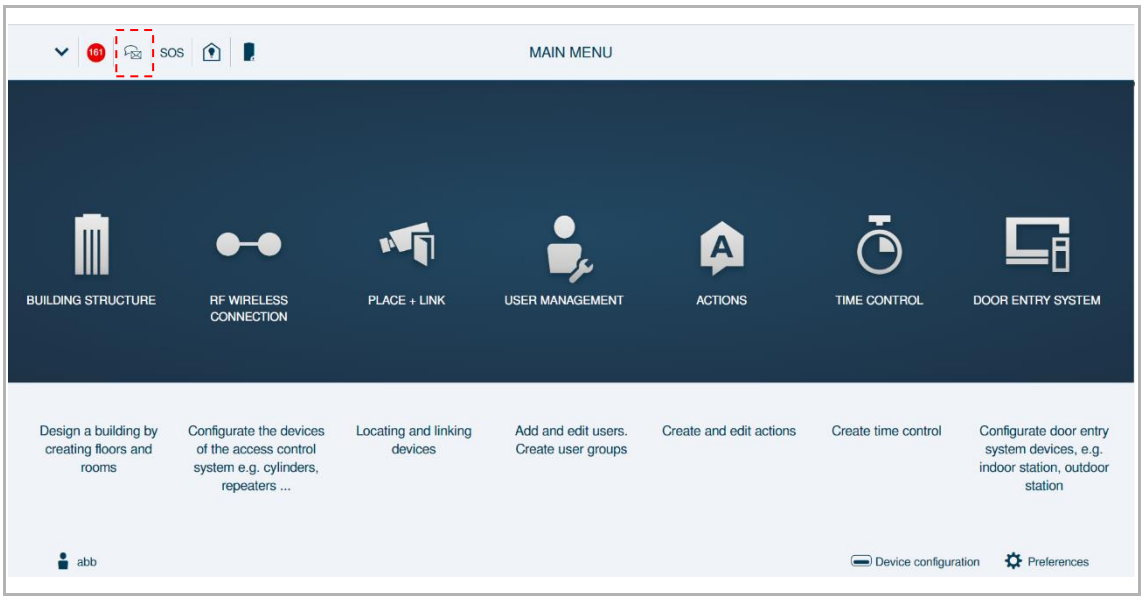
[5] Rename the log file.



13.8 Message center

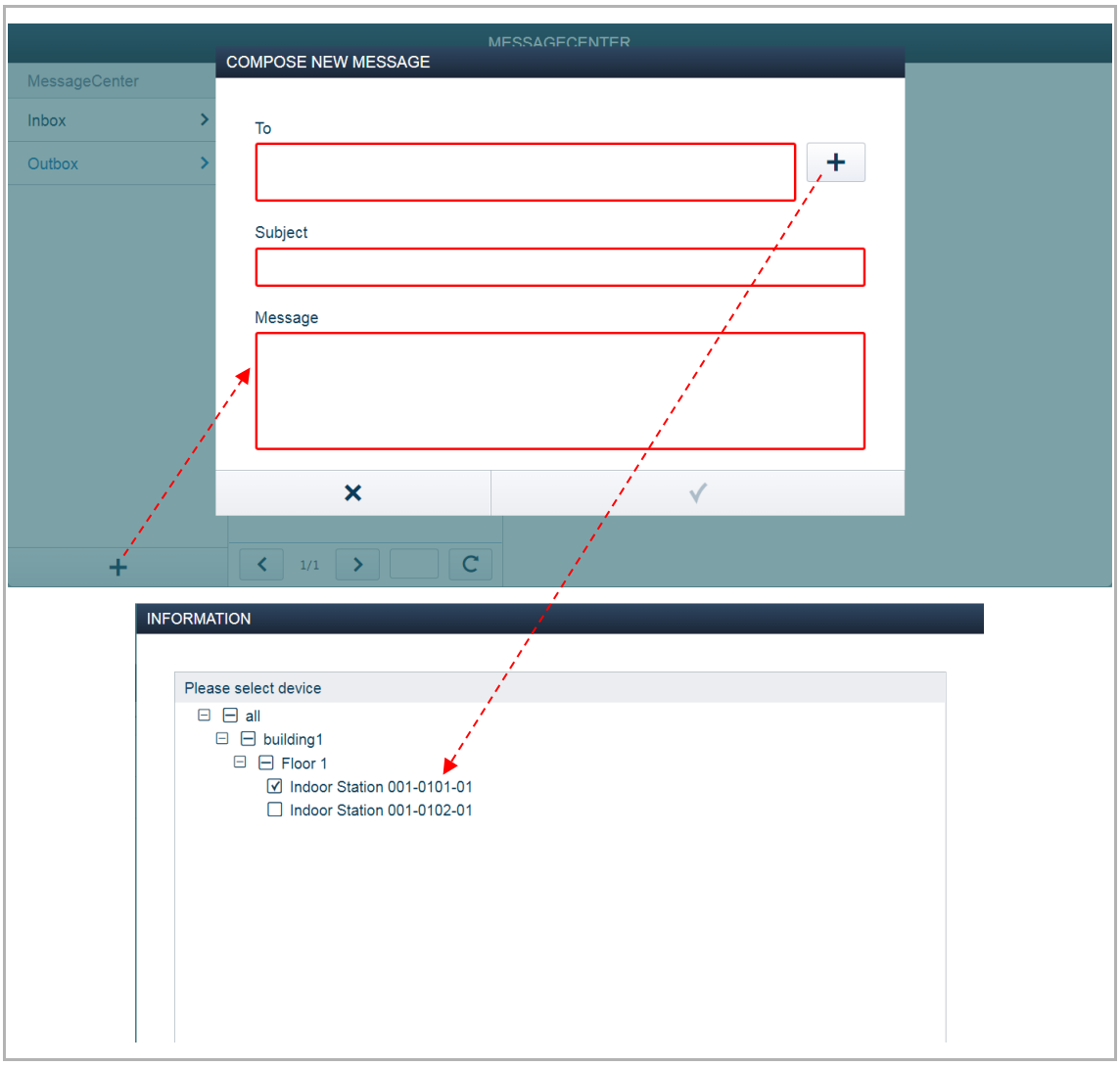
Accessing the "Message center" screen

On the configuration screen, click " " to access the corresponding screen.



13.8.1 Creating a message

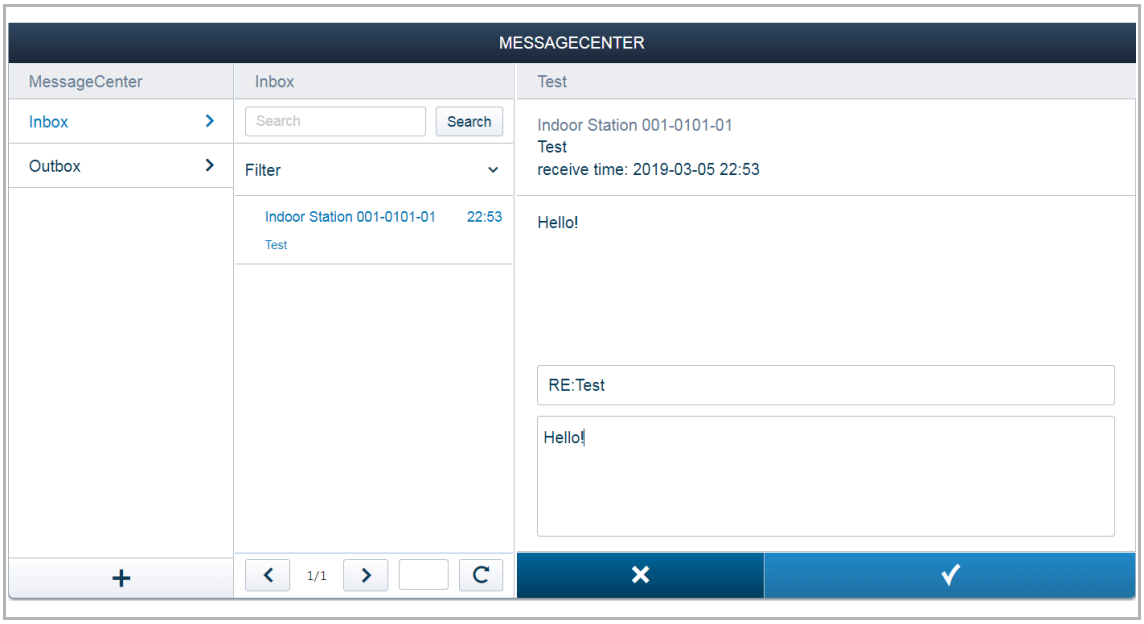
On the "Message center" screen, click "+" to set a recipient, then enter the subject and the message, click "√" to create and send the message.



13.8.2 Replying to a message

On the "Message center" screen, click "Inbox" to view the message received from the indoor stations. You can click on a message and reply to it directly.

A maximum of 1000 messages is supported.



14 Notice

We reserve the right to at all times make technical changes as well as changes to the contents of this document without prior notice.

The detailed specifications agreed to at the time of ordering apply to all orders. Busch-Jaeger accepts no responsibility for possible errors or incompleteness in this document.

Service

ABB AG – BUSCH-JAEGER
Freisenbergstr. 2, DE-58513 Lüdenscheid

BUSCH-JAEGER.de
go.abb/contact

2TMD041800D0090

BUSCH-JAEGER