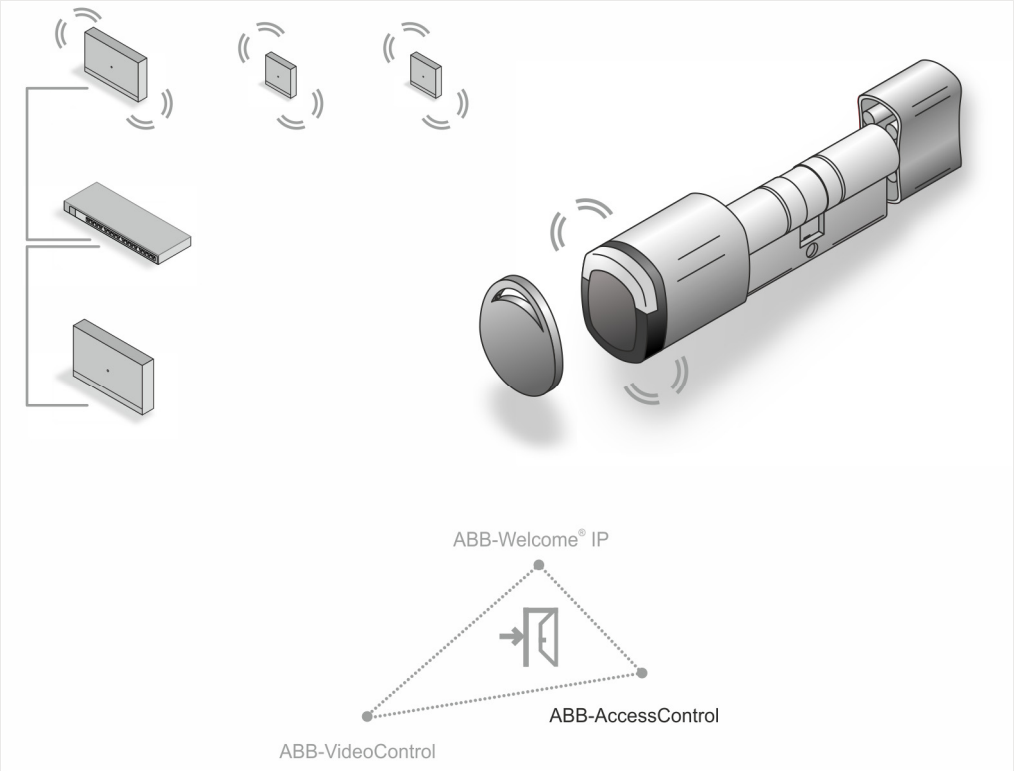
System Manual | 01.03.2021

ABB-AccessControl



1 Overview

1.1 Information on the manual

This manual describes the ABB-AccessControl system. It supports you in the selection and planning of the correct structure.

It contains an overview of currently available components and provides ideas for practical combination and integration.

For detailed technical information about the individual components please also note the respective product documentation.

In Chapter 4.3 “Case studies“ on page 69 the topics of this document are explained by means of examples. The information in the chapters is structured logically. If you wish to familiarise or re-familiarise yourself again with the topic, read through all the relevant subchapters on this topic.

1.2 Target group / Qualifications of personnel

Installation, commissioning and maintenance of the device must only be carried out by trained and properly qualified electrical installers.

The electrical installer must have read and understood the manual and follow the instructions provided.

The electrical installer must adhere to the valid national regulations in his/her country governing the installation, functional test, repair and maintenance of electrical products.

The specialist staff should have general knowledge about networks.

1.3 Introduction to ABB-AccessControl

The "Electronic cylindrical lock" are designed and provided for application within the "ABB-AccessControl" IP system.

Communication and current

The "Electronic cylindrical lock" communicate via radio control. A separate power supply is not required. The "Electronic cylindrical lock" obtain the necessary power via the supplied batteries.

Scalability

Smaller objects can be installed as easily as large objects. Existing installations can be extended at all times.

Operation

Central management of all access points via the ABB-Welcome® App app.

Loss of keys

No change of hardware when keys are lost.

New or retrofitting

The "Electronic cylindrical lock" can be installed on almost all doors. Either new or for retrofitting.

Power failure

The "Electronic cylindrical lock" obtain the necessary power via the supplied batteries.

– The "Electronic cylindrical lock" are used independently:
  – The "Electronic cylindrical lock" continue to function.
– The "Electronic cylindrical lock" are integrated in a system:
  – The "Electronic cylindrical lock" continue to function, the system does not.

1.4 ABB-AccessControl and smartIP

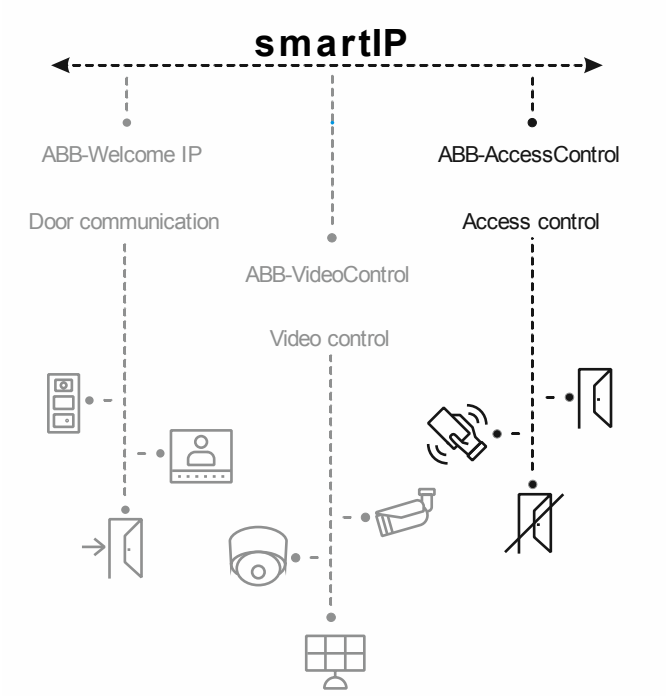


Fig. 1: ABB-AccessControl and smartIP

The ABB-AccessControl access control is an integral part of the entire smartIP system.

The ABB-AccessControl access control can be used exclusively for itself. Or it can, as desired, be supplemented by additional systems or also be integrated into additional systems. This can take place at any time in the future.

For planning purposes, a separate system manual is available for each system.

1.5 Fundamentals of structured cabling

Structured cabling is a uniform setup plan for a network infrastructure. The network infrastructure is independent of the application and future-oriented. Additional designations for the structured cabling are Universelle Gebäudeverkabelung (UGV) (universal structured cabling) or Universelle Kommunikationsverkabelung (UKV) (universal communication cabling).

Structured cabling is to prevent expensive faulty installations and extensions and also make the installation of new network components easier.

Unstructured cabling is normally bound to requirements or a specific application. If the changeover to a new technology or technology generation becomes necessary, this could easily lead to a cost explosion.

Structured cabling is based on a generally valid cabling structure. This cabling structure, among others, takes the requirements for several years into the future into consideration. It contains reserves and can be used independent of the applications. E.g., one lets the local network and the telephony operate via the same cabling.

Structured cabling includes the following points:

- Standardized components (wires, connectors, etc.)
- Hierarchical network topology (star, tree, etc.)
- Recommendations for laying and installation
- Standardized measuring, testing and documentation processes

Objectives of structured cabling

- Support of all current and future communication systems
- Reserve of capacity regarding limiting frequency
- Neutral behaviour of the network regarding the transmission protocol and terminal devices
- Flexible expandability
- Fail-safe due to star-shaped cabling
- Implementation of data protection and security
- Adherence to existing standards

Standards for structured cabling

Area of validity	Standard	Description
Europe	EN 50173-1 (2003)	Cabling standard information system - application-neutral cabling systems
North America	TIA/EIA 568 B.1 (2001) / B.2 1 (2001)	Telecommunication cabling standard for building cabling
World	ISO/IEC 11801 (2002)	Cabling standard for application-neutral building cabling

Table 1: Standards for structured cabling

ISO/IEC 11801 (2002) and EN 50173-1 (2003)

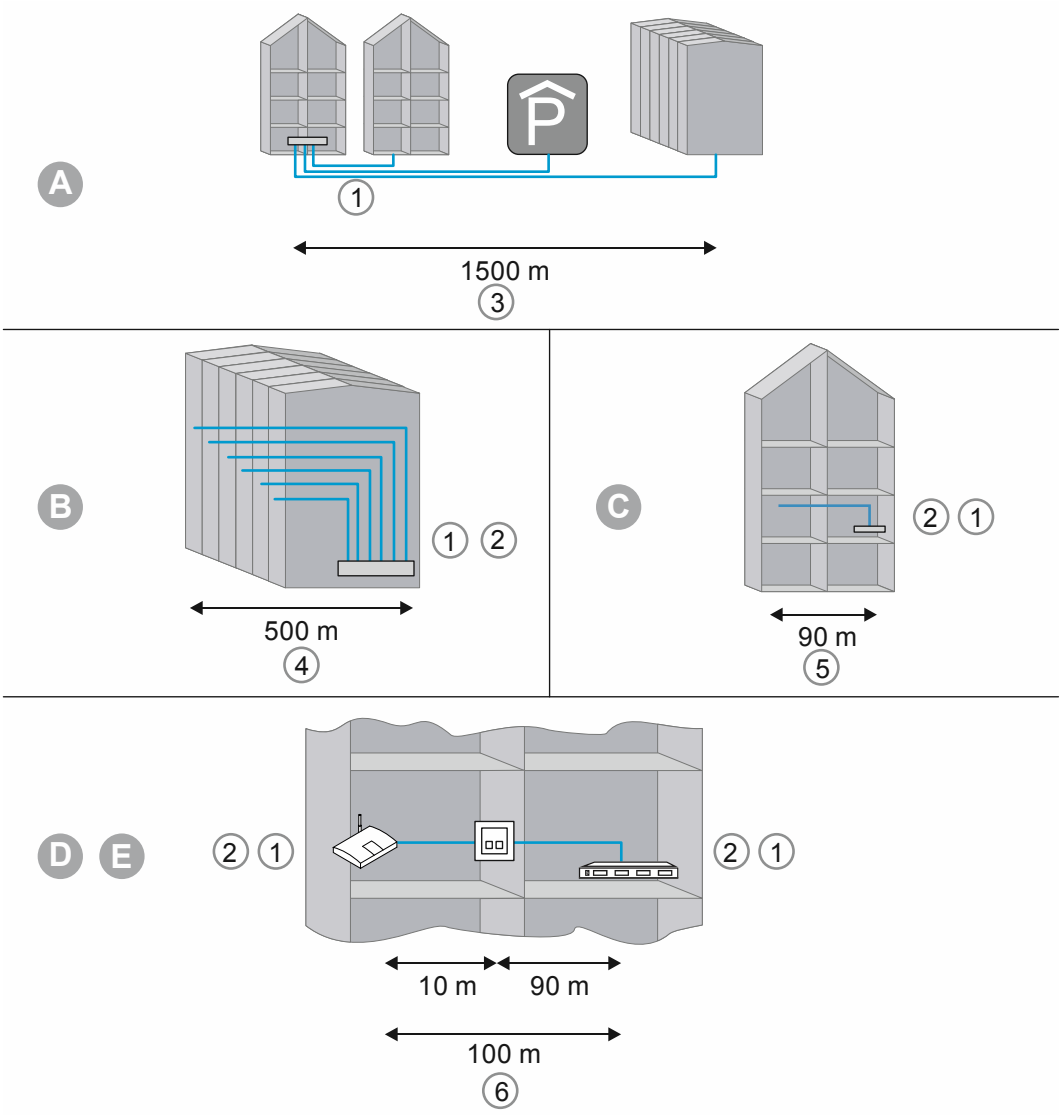


Fig. 2: Structured cabling

A	Location distributor
B	Building distributor
C	Floor distributor
D	Connection unit
E	Terminal device
1	Optical fibre
2	Copper conductor
3	Primary area
4	Secondary area
5	Tertiary area
6	Tertiary area including patch cable

Table 2: Structured cabling

In the European standard (EN) and the globally valid ISO standard, structuring is carried out in the form of hierarchical levels. These levels are formed by groups. These groups are joined topologic and administrative.

Cabling is divided into the following areas:

- Site cabling (primary cabling)
- Building cabling (secondary cabling)
- Floor cabling (tertiary cabling)

The cabling standards are optimized for the following geographic expansion:

- Expansion: 3000 m,
- Area: 1,000,000 sqm
- Users: 50 - 50,000

Maximum admissible cable lengths have been specified in every cabling sector and must be adhered to during installation. Many transmission techniques refer to the defined cable lengths and quality requirements.

Notice
All ISO standards are recommendations for handling. The adherence to the ISO standard is voluntary. Adherence to the ISO standards my be demanded by different parties, such cooperation partners, manufacturers and customers.

Primary cabling - Site cabling

The primary area is designated as campus cabling or site cabling. The primary area implements the joint cabling of individual buildings. The primary area includes large distances, high transmission rates as well as a minimum number of stations.

In most cases is glass fibre cable (50 µm) with a maxim length of 1,500 m used. Normally these are glass fibre cables with multi-mode fibres or also single-mode cables in case of greater distances. Sometimes also copper cables are used for smaller distances.

The primary area should fundamentally be planned in greater detail. The transmission medium should, with regard to the transmission speed, be open upwards. This equally applies to the transmission system used. As a rule of thumb, a 50 percent reserve applies to the current requirement of the investment.

Secondary cabling - building cabling

The secondary area is designated as building cabling or rising area cabling. The secondary area implements the joint cabling of individual floors or storeys within a building. Here the preferred use is glass fibre cables (50 µm) or copper cables with a maximum length of 500 m.

Tertiary cabling - floor cabling

The tertiary area is designated as floor cabling. The tertiary area implements the cabling of floor or storey distributors to the connection sockets. While a network cabinet with a patch field is located in the storey distributor, the cable at the workplace of the user leads to a connecting socket on the wall, to a cable duct or a floor tank with outlet.

Twisted pair cables are used for these relatively short distances whose length is limited to a total of 100 m (90 m plus 2 x 5 m connecting cable). Also glass fibre cables (62.5 µm) are used as an alternative.

Components of structured cabling:

- Patch field (patch panel)
- Patch cable
- Connection sockets
- Network cable
- Distributor cabinets
- Switch, hubs, router

1.6 Design lines

This system manual serves for the technical planning of the simple to complex installations.

The different design lines (with the respective special colours and shapes of the devices) are not listed in this system manual.

Please obtain the desired current design versions and the corresponding complete article numbers as well as the order numbers from the respective product catalogues or the online catalogue at https://busch-jaeger-catalogue.com.

1.7 Basic principles

Information about basic functions and principles of operation of the devices are available at Chapter 4 “Information about planning and application“ on page 62.

2 Overview of product range

2.1 Application

The battery-operated access devices of the "ABB-AccessControl" are basically intended for application in an IP system. For the management of the battery-operated access devices, a "Smart Access Point Pro" is required. The battery-operated access devices and transponder keys as well as access authorizations for persons are managed in the management software of the "Smart Access Point Pro".

The local communication of the battery-operated access devices is carried out via radio control. The "ABB-AccessControl" can be operated independent or via the "Smart Access Point Pro" with additional systems, e.g. ABB-Welcome IP or the home network. This makes the battery-operated access devices part of the Smart Home. Also an app control via a smartphone is then possible.

2.2 Areas of application

Areas of application of wireless access systems

Possible accesses

Accesses
▪ Access doors ▪ Server and rack doors – Only for intended installation of "Electronic cylindrical lock" ▪ Machine doors ▪ Lifts

Table 3: Accesses

Areas of application	
PRIVATE HOMES	
TRADE AND INDUSTRY	
▪ Office buildings	▪ Industrial buildings
RETAIL BUSINESS	
EDUCATIONAL SYSTEMS	
▪ Universities ▪ Dormitories ▪ Academies	▪ Schools ▪ Research institutes ▪ Kindergartens
HEALTH SYSTEMS	
▪ Hospitals ▪ Nursing homes ▪ Assisted living	▪ Infirmaries ▪ Home nursing sevices
PUBLIC FACILITIES	
▪ Parliaments ▪ Town halls	▪ Ministries ▪ Authorities and administrative facilities
LOGISTICS	
▪ Airports ▪ Harbours ▪ Logistic centers	▪ Railway stations ▪ Ships ▪ Warehouses
HOTEL CHAINS	
▪ Design and luxury hotels ▪ Family hotels	▪ Business hotels ▪ Holiday facilities
LEISURE TIME and ENTERTAINMENT	
▪ Stadiums ▪ Cinemas and theatres ▪ Swimming pools ▪ Restaurants	▪ Fitness clubs ▪ Amusement parks ▪ Museums ▪ Sporting facilities

Table 4: Areas of application

2.3 Device overview

2.3.1 Setup of article numbers

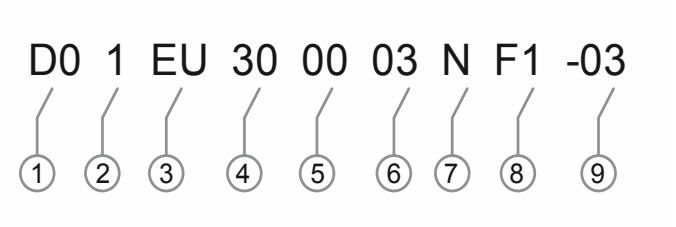


Fig. 3: Overview of article numbers

No.	Meaning		
1	System:	▪ D0	ABB-AccessControl
2	Device type:	▪ 1 ▪ 2 ▪ 5 ▪ 6 ▪ 8 ▪ 9	Cylindrical lock Reserved for: Fitting Reserved for: Wall reader Reserved for: Door controller Accessories Spare part
3	Profile type	▪ EU ▪ CH ▪ MO ▪ RIM ▪ SCAN ▪ DB	Europe Swiss Mortise RIM Scandinavian oval Deadbolt
4	Cylinder length for exterior side of door	▪ XX	In mm
5	Cylinder length for interior side of door	▪ XX	In mm
6	Spacing (between reading head and cylinder mechanics	▪ 3 ▪ 8 ▪ 13	3 mm Reserved for: 8 mm Reserved for: 13 mm
7	End piece	▪ T ▪ K ▪ N	Rotary knob Reserved for: Electronic reading head No end piece
8	Surfaces	Reading head: ▪ F1 ▪ F2 ▪ F3	 CSB (Chrome-Satin-Black) CWS (Reserved) PPB (Reserved)
		Transponder keys: ▪ C1 ▪ C2 ▪ C3	 GY: Grey WH: White (Reserved) BK: Black (Reserved)
9	Brand	▪ -03 ▪ -04	Busch-Jaeger ABB

2.3.2 Cylindrical lock

Cylindrical lock for Europe: Profile EU

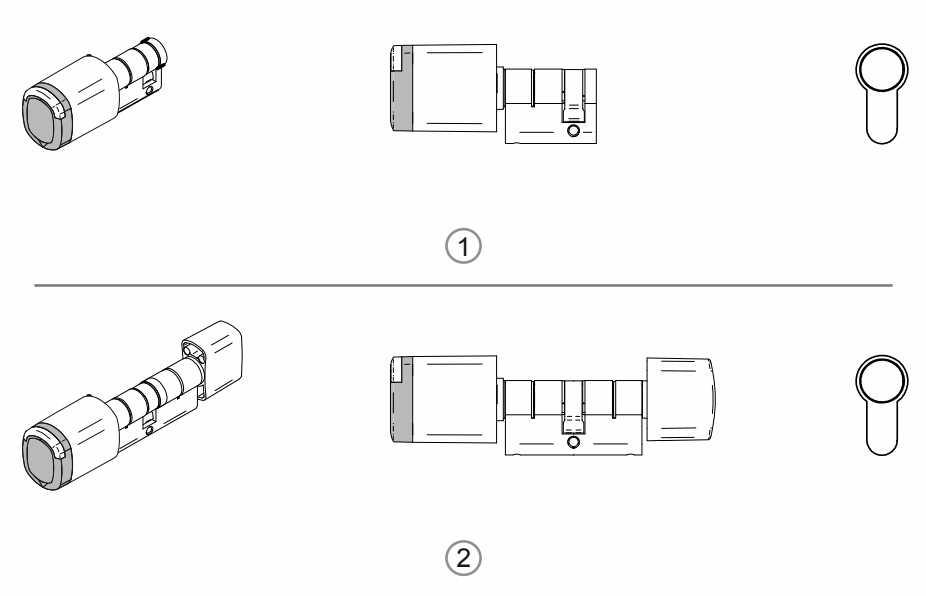


Fig. 4: Cylindrical lock profile EU

No.	Cylindrical lock
[1]	Semi-cylinder with reading head
[2]	Double-cylinder with reading head and hand knob

Cylindrical lock for Switzerland: Profile Switzerland oval

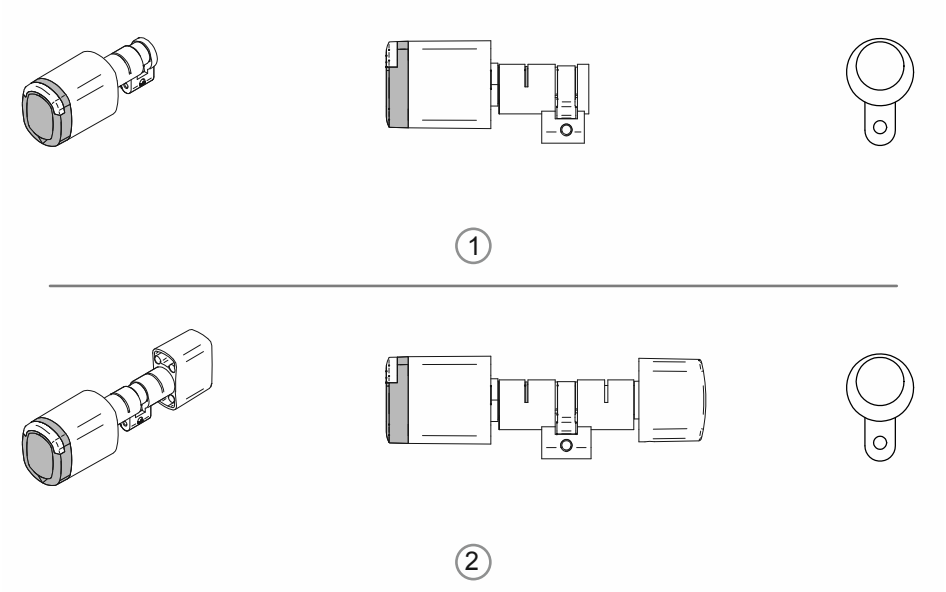


Fig. 5: Cylindrical lock profile Switzerland oval

No.	Cylindrical lock
[1]	Semi-cylinder with reading head
[2]	Double-cylinder with reading head and hand knob

Cylindrical lock for Scandinavia: Profile Scandinavian oval

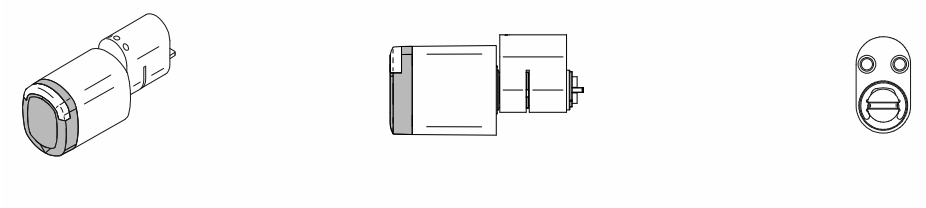


Fig. 6: Profile Scandinavian oval. Semi-cylinder with reading head

Cylindrical lock for Great Britain:

- RIM profile

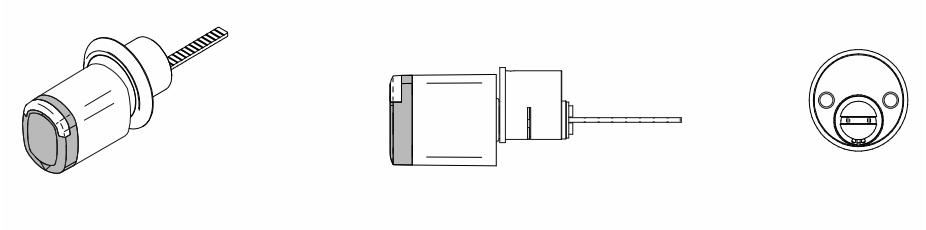


Fig. 7: RIM profile. Semi-cylinder with reading head

- Mortise profile

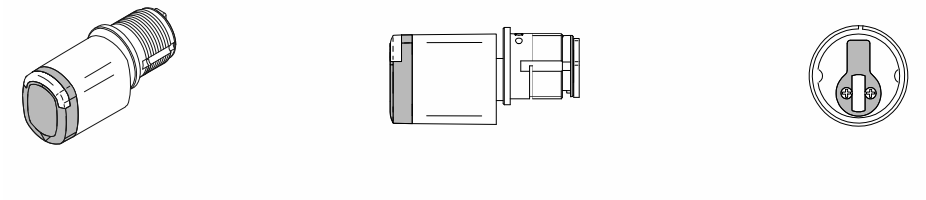


Fig. 8: Mortise profile. Semi-cylinder with reading head

2.3.3 System devices

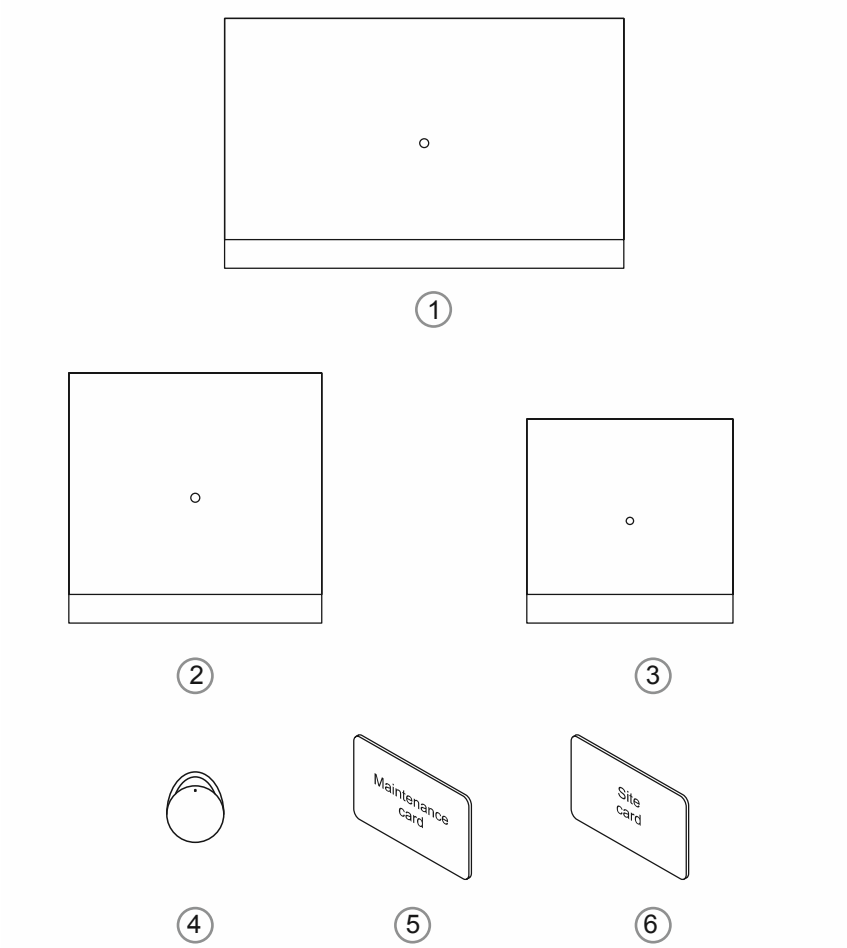


Fig. 9: System devices

[1] „Smart Access Point Pro“ D04011-04

The management software is installed on the "Smart Access Point Pro".

The "Smart Access Point Pro" offers the access point for commissioning and managing the "ABB-AccessControl" system with the PC or a mobile terminal device.

For opening the Web-based user interface of the "Smart Access Point Pro" you require a computer with a LAN or WLAN network adaptor and an installed Internet browser.

The "Smart Access Point Pro" has the following main functions:

- Direct activation of up to 16 "Electronic cylindrical lock".
- Managing up to 600 "Electronic cylindrical lock" in the "ABB-AccessControl" system
- Power supply via PoE or separate power supply adapter.

[2] "RF/IP Gateway"

The "RF/IP Gateway" extends the activation capacity of the "Smart Access Point Pro" to the "Electronic cylindrical lock". Up to 64 "RF/IP Gateway" can be connected to a "Smart Access Point Pro". The connection is made via a PoE switch.

The "RF/IP Gateway" has the following main functions:

- Activation of up to 16 "Electronic cylindrical lock".
- Transferring the communication between the activated "Electronic cylindrical lock" and the "Smart Access Point Pro".
- Floor distribution of the radio signal
- Power supply via PoE or separate power supply adapter.

[3] „RF Repeater“

The "RF Repeater" increases the radio range of the "Smart Access Point Pro" or a "RF/IP Gateway" to the "Electronic cylindrical lock". Up to 3 "RF Repeater" can be switched in sequence in one line on a "Smart Access Point Pro" or a "RF/IP Gateway".

The radio range between the devices amounts to a maximum of 10 meters.

The "RF Repeater" has the following main functions:

- Transferring the communication of up to 16 "Electronic cylindrical lock".
- Power supply via a separate power supply adapter.

[4] Transponder keys

The "Electronic cylindrical lock" are operated with the transponder keys.

The transponder keys are ordered separately.

The transponder keys are preconfigured and ready for operation.

The transponder keys are personalized in the management software of the "Smart Access Point Pro" in three steps:

– A user is created in the management software of the "Smart Access Point Pro".
– The user is assigned a transponder key, which he is permitted to use.
– The user is assigned the "Electronic cylindrical lock", which he is permitted to open.

A user is then permitted or not permitted to open a door via the communication of the "Electronic cylindrical lock" with the management software of the "Smart Access Point Pro".

[5] Maintenance card

The reading heads of the "Electronic cylindrical lock" are put into operation with the maintenance card.

– For commissioning, a radio connection must be established between the reading head of a "Electronic cylindrical lock" and the "Smart Access Point Pro".

A maintenance card is ordered separately.

Maintenance card is preconfigured and ready for operation. There is no personalization. A maintenance card can be used in every "ABB-AccessControl" system.

[6] Construction site card

With the construction site card the reading heads of the "Electronic cylindrical lock" can be operated when they are already installed but have not yet been put into operation.

– To operate the construction site card no radio connection is required between the reading head of a "Electronic cylindrical lock" and the "Smart Access Point Pro".

A construction site card is ordered separately.

A construction site card is preconfigured and ready for operation. There is no personalization. A construction site card can be used in every "ABB-AccessControl" system.

2.3.4 Accessories

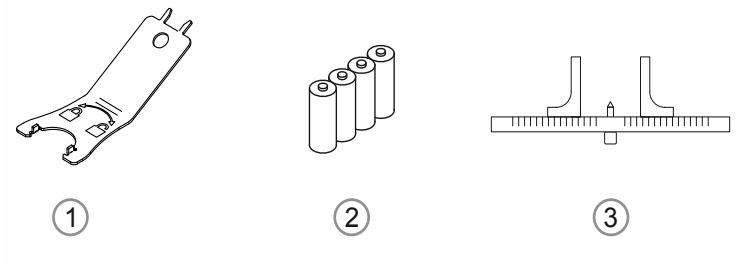


Fig. 10: Accessories

1	Mounting tool	Article number: D080MT-04
2	Batteries (commercially available)	▪ One set of batteries (4x LR1) is enclosed with every "Electronic cylindrical lock". – For normal use, this set lasts approximately 2 to 3 years. – For normal use, this set lasts for approximately 130,000 actuations. ▪ Commercially available LR1 batteries are used for replacement.
3	Gauge for cylindrical lock (commercially available)	To facilitate the measuring of the width of doors the trade offers a variety of gauges. – Yet, special gauges are not absolutely necessary for measuring the width of doors.

2.3.5 Mounting possibilities

2.3.6 Prerequisites

Safety fittings

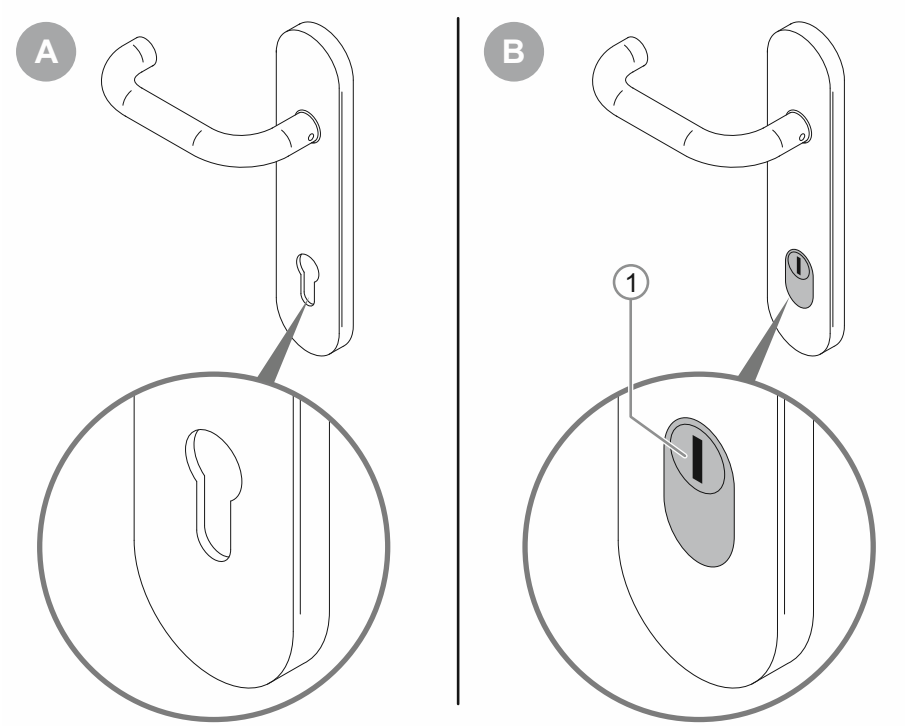


Fig. 11: Mounting situation for safety fittings

[A]: Standard door fitting

– Mounting the "Electronic cylindrical lock" possible.

[B]: Door safety fitting with core pulling protection / cylinder protection

– Mounting the "Electronic cylindrical lock" is not possible.

Conditions of space

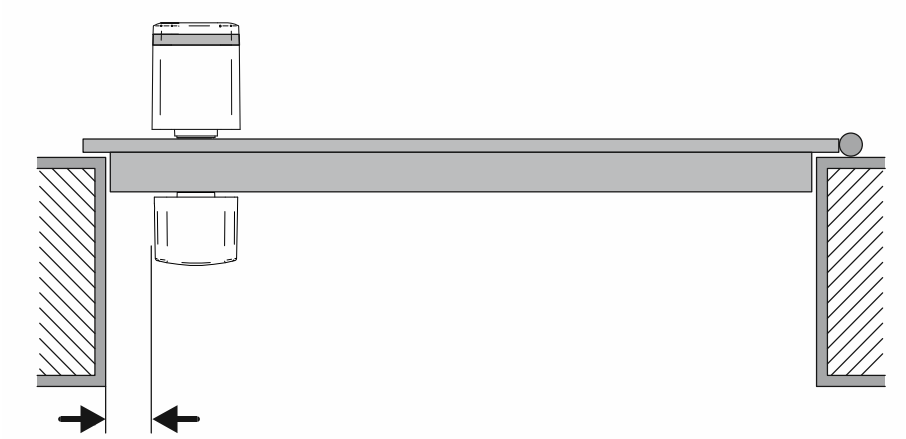


Fig. 12: Mounting situations and conditions of space

To mount the "Electronic cylindrical lock", sufficient space must be available to the door frame. After the "Electronic cylindrical lock" is mounted, one should still be able to fully wrap the fingers around the the knob. During the cold season or in refrigerated areas also when wearing gloves.

2.3.7 Measuring the cylindrical lock

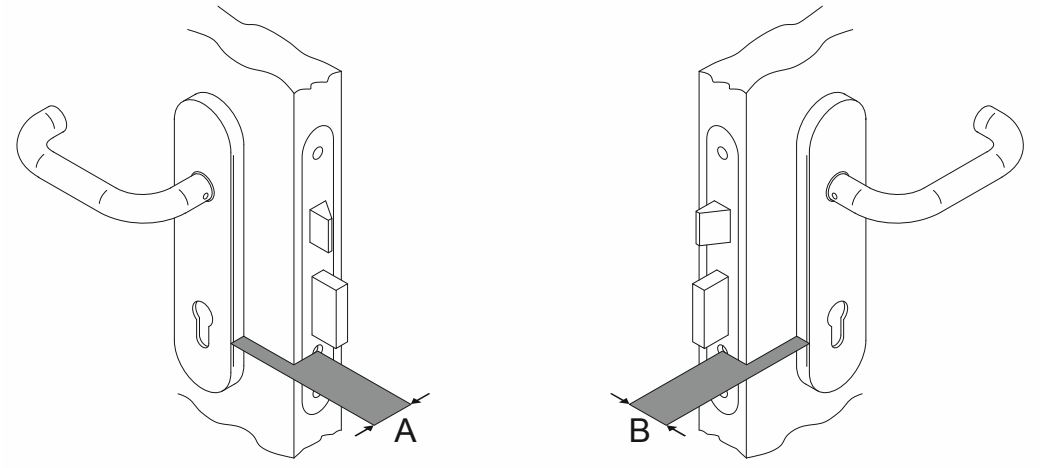


Fig. 13: Measuring the cylindrical lock: Width of door

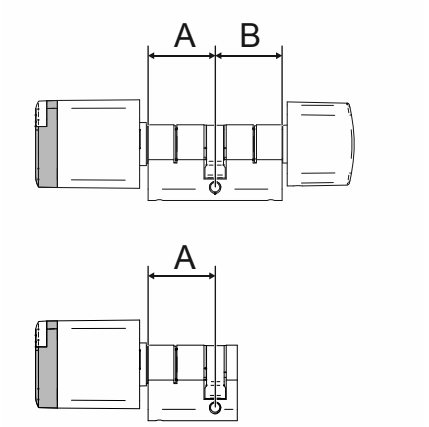


Fig. 14: Cylindrical lock: Width of cylinder profile EU

		A								
		30	**35**	**40**	**45**	**50**	**55**	**60**	**65**	**70**
B	**30**	x*	x	x	x	x	x	x	x	x
	35	x*	x	x	x	x	x	x	x	x
	40	x	x*	x	x	x	x	x	x	x
	45	x	x	x*	x	x	x	x	x	x
	50	x	x	x*	x	x	x	x	x	x
	55	x	x	x	x	x	x	x	x	x
	60	x	x	x	x	x	x	x	x	x
	65	x	x	x	x	x	x	x	x	x
	70	x	x	x	x	x	x	x	x	x

Table 5: Lengths in millimetres

* : Standard sizes

– Standard sizes are available immediately.

– All other sizes have delivery period of 4 to 6 weeks.

2.3.8 Dismantling old cylindrical locks

Aside from the normal local standard cylinders, also other cylinder systems are used when the situation requires it. If for the use of the "ABB-AccessControl" old cylindrical locks must be removed, you will find information in the following about the dismantling of conventional cylindrical locks.

Dismantling old cylinders: Profile Europe (EU) and Switzerland (CH)

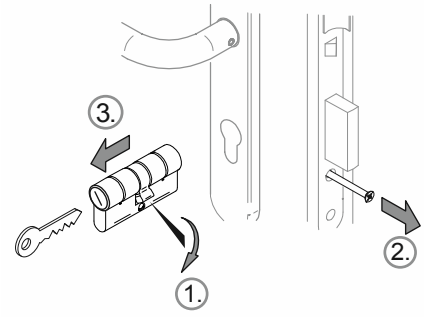


Fig. 15: Dismantling old cylinders: Profile Europe (EU) and Switzerland (CH)

To dismantle the existing old cylinders, perform the following items:

1. Turn the driver down vertically.
2. Screw out the forend screw.
3. Remove the cylinder.

Dismantling old cylinders: Profile Scandinavian oval

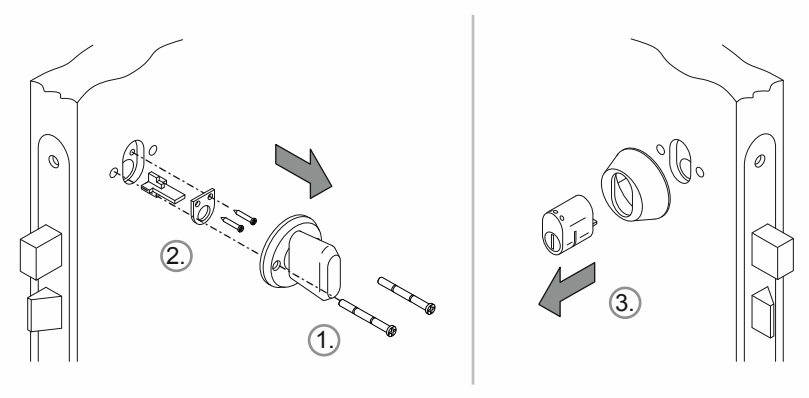


Fig. 16: Dismantling old cylinders: Profile Scandinavian oval

To dismantle the existing old cylinders, perform the following items:

1. Dismantle the head on the interior side.
2. Dismantle the mounting set of the cylindrical lock on the interior side.
3. Remove the cylinder on the exterior side.

Dismantling old cylinders: Profile RIM

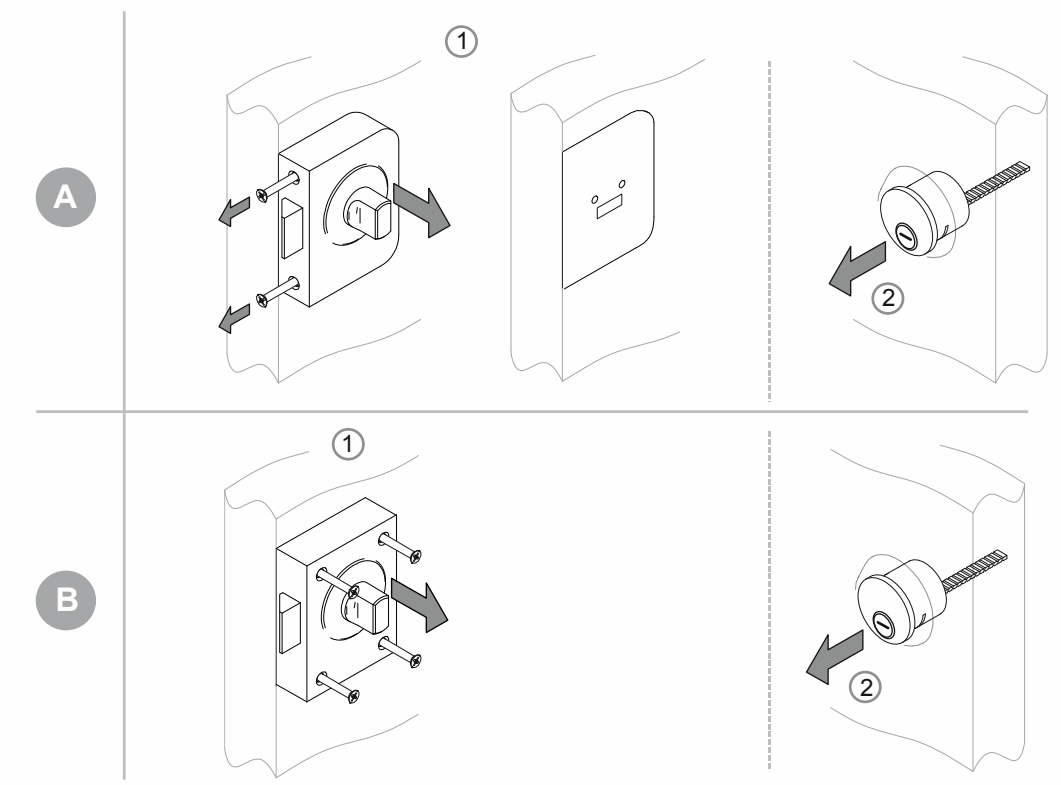


Fig. 17: Dismantling old cylinders: Profile RIM

For the "RIM" cylinder profile there are two basic types of locks.

[A] With base and separate base plate

[B] Complete lock body

[A]

1. Screw out the lateral screws and remove the lock body.
   – The baseplate remains in position.
2. Remove the cylindrical lock.

[B]

1. Screw out the screws and remove the entire lock.
2. Remove the cylindrical lock.

Dismantling old cylinders: Mortise profile

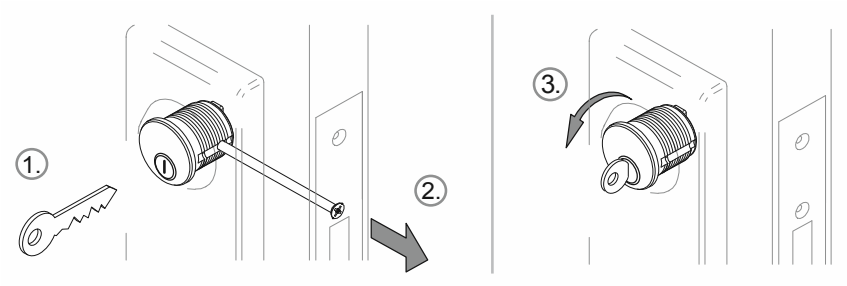


Fig. 18: Dismantling old cylinders: Mortise profile

1. Insert the key.
2. Loosen the fixing screw to the point where the cylinder can be turned.
3. Screw out the cylinder with the aid of the key.

3 Commissioning

3.1 Overview of commissioning

During commissioning it is differentiated between the commissioning of the system devices ("Smart Access Point Pro", "RF/IP Gateway" and "RF Repeater") and the adding and commissioning of "Electronic cylindrical lock".

If the "Smart Access Point Pro" or the building structure already exists, e.g. in a "ABB-Welcome IP" system, this part of commissioning is dropped. The same applies when a device is not required in the planned system. The further steps can be carried out directly in the management software of the "Smart Access Point Pro".

Step 1	Initial commissioning of "Smart Access Point Pro"	see chapter 3.1.4 “Commissioning the "Smart Access Point"“ on page 36
Step 2	Creating the building structure	see chapter 5.2 “Building structure“ on page 95
Step 3	Placing of "Smart Access Point Pro"	▪ Placing the "Smart Access Point Pro" in building structure of the management software: – see chapter 5.4.1 “Placing the "Smart Access Point Pro"“ on page 114
Step 4	Commissioning of "RF/IP Gateway"	▪ Commissioning the "RF/IP Gateway" in the management software of the "Smart Access Point Pro": – see chapter 3.2.3 “"RF/IP Gateway"“ on page 55
Step 5	Commissioning of "RF Repeater"	▪ Commissioning the "RF Repeater" in the management software of the "Smart Access Point Pro": – see chapter 3.2.4 “"RF Repeater"“ on page 56
Step 6	Adding "Electronic cylindrical lock"	▪ Commissioning the "Electronic cylindrical lock": – see chapter 3.2.1 “"Electronic cylindrical lock"“ on page 51 – The "Electronic cylindrical lock" is already mounted: see chapter 5.3.2 “Add "Electronic cylindrical lock"“ on page 105 – "Electronic cylindrical lock" is not yet mounted: see chapter 3.2.2 “Adding larger projects / devices in advance“ on page 55

3.2 Prerequisites

„Electronic cylindrical lock“

- Every reading head must have a radio connection to the "Smart Access Point Pro" during commissioning.
  - This radio connection can be established directly or indirectly via other devices.
  - The connecting path to their later area of application must be specified in the management software of the "Smart Access Point Pro" prior to the installation of the devices.
- All "Electronic cylindrical lock" can be commissioned together locally. For this all devices of the system must be located in close proximity to the "Smart Access Point Pro". After the joint commissioning, the devices are then mounted at their area of application.
- If additional devices are required for the application of the "Electronic cylindrical lock" ("RF/IP Gateway" or "RF Repeater"), they should have already been put into operation for the commissioning of the "Electronic cylindrical lock".

"Smart Access Point Pro"

A "Smart Access Point Pro" is required for the application of the "ABB-AccessControl" system.

3.1 Commissioning of the system - "Smart Access Point Pro"

3.1.1 Overview

Commissioning of the "Smart Access Point Pro" system is carried out in 3 sections.

– Please observe the order of the steps. They are dependent on each other.

1.	Connect the "Smart Access Point Pro" via WLAN with a computer any call up the website of the "Smart Access Point Pro".	see chapter 3.1.2 “Connecting a PC with the "Smart Access Point ““ on page 33
2.	Make a preliminary decision about the system mode.	see chapter 3.1.3 “Preliminary information: Selection of the system mode“ on page 35
3.	Run through the wizard with selection of the system mode.	see chapter 3.1.4 “Commissioning the "Smart Access Point"“ on page 36

3.1.2 Connecting a PC with the "Smart Access Point “

Attention! Loss of data

The "Smart Access Point" safely integrates the device found into the system with the aid of certificates. This makes encrypted communication between all devices possible.

- Perform a backup after commissioning.
  – If the Smart Access Point becomes defective, without a backup you would need to re-commission the entire system.

Connecting the "Smart Access Point" with the PC via WLAN

Fig. 19: Connecting the "Smart Access Point" with the PC (Access-Point mode)

As soon as the "Smart Access Point" is supplied with voltage via the PoE switch, the device boots up automatically.

The device is in Access-Point mode (the LED lights up permanently red).

Use the following steps to connect with the PC:

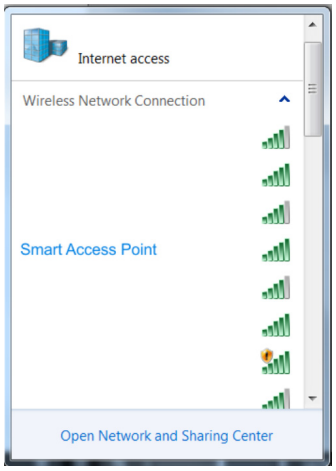


Fig. 20: "Smart Access Point" in the network list of the PC

1. Connecting the PC with the WLAN of the "Smart Access Point".
   – The WLAN access data are located on the device. Remove the cover of the device.

Fig. 21: Entering the IP address in a browser

2. Call up the start page of the "Smart Access Point" in a commercially available browser.
   – For this, enter the IP address "192.168.3.1" in the address line of the browser.

3.1.3 Preliminary information: Selection of the system mode

The meaning of the operating mode can be illustrated best with the example of a "ABB-Welcome IP" system.

Also when an integration of additional systems is not or not yet intended, you should already now consider the selection of the system mode. The system mode cannot be changed later.

Preliminary information about the selection of the system modes

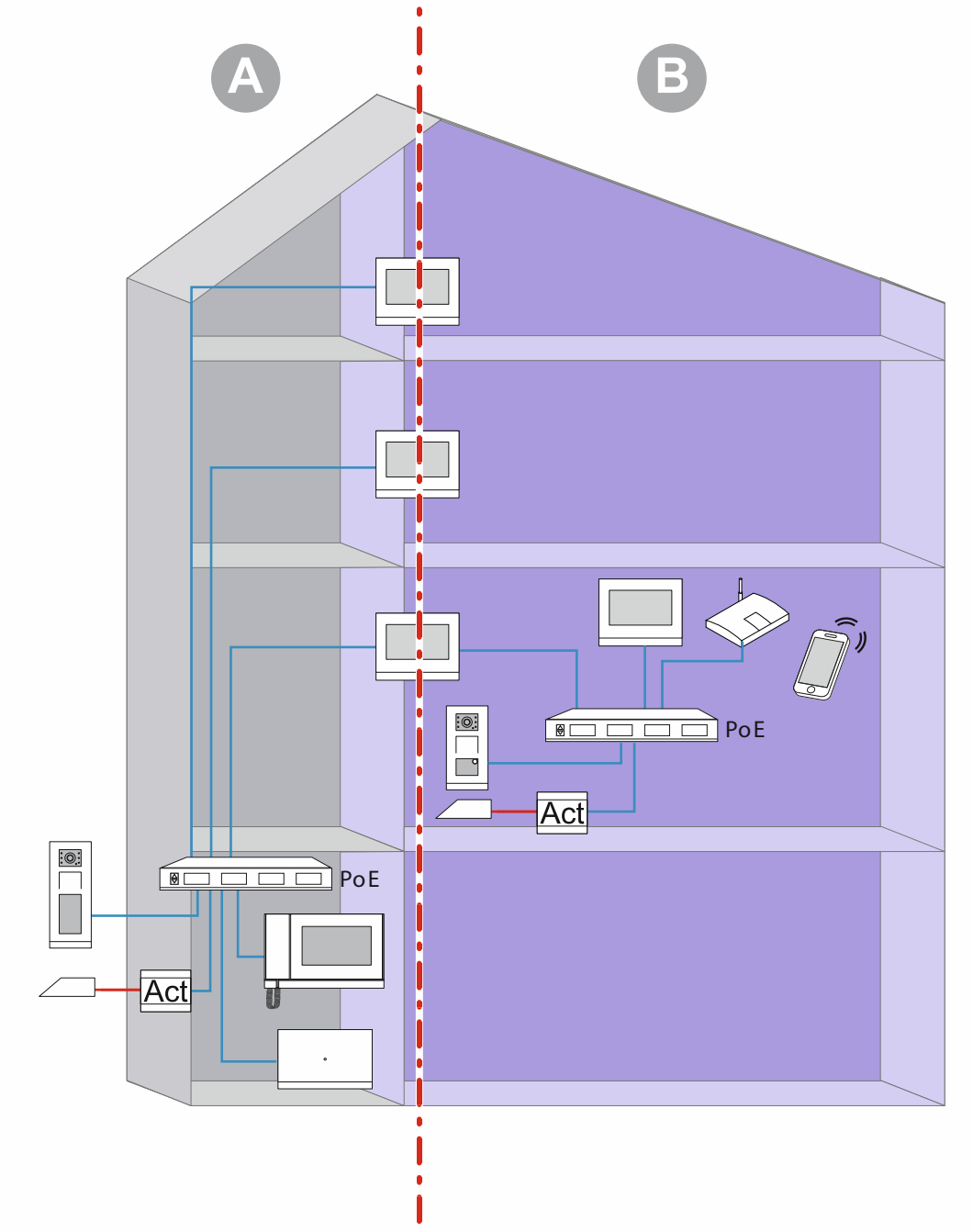


Fig. 22: Preliminary information about the selection of the system modes

The graphics illustrate two basic areas within buildings (here a residential building). Both areas of the installation are strictly separated by the first indoor station (master) of a unit which operates as IP gateway. No area can access the other area.

- Area [A]: The public area (building network)
  - Here, for example, the caretaker receives the visitors and guides them to the individual apartments.
- Area [B]: The private area (units network)
  - This area is, as the name indicates, private. The public area cannot access the private area from behind the 1st indoor station. Access is also not possible from the private area to the public area.

System modes of the "Smart Access Point"

For the later adding of the devices the system mode must already be specified during the processing steps of the commissioning of the "Smart Access Point".

- Mode "Multi-unit house / commercial":
  - For a building network.
  - The "Smart Access Point" is located in the building network.
  - The "Smart Access Point" has the static IP address "10.0.0.1".
    - The 10s IP address range is used to communicate with the "ABB-Welcome IP" participants.
    - In parallel the "Smart Access Point" can be connected with a router per WLAN or LAN and act as DHCP Client. Here the device receives an additional IP address assigned by the router. This it uses in addition to its own 10s IP address.
- Mode "One-family house / terraced house":
  - For a units network.
  - The "Smart Access Point" is located in the units network.
  - The "Smart Access Point" has the static IP address "10.0.0.1".
    - The 10s IP address range is used to communicate with the "ABB-Welcome IP" participants.
    - In parallel the "Smart Access Point" can be connected with a router per WLAN or LAN and act as DHCP Client. Here the device receives an additional IP address assigned by the router. This it uses in addition to its own 10s IP address.

3.1.4 Commissioning the "Smart Access Point"

When the "Smart Access Point" is connected to the PC and the start page of the "Smart Access Point" is called up in the browser, the "Smart Access Point" is ready for commissioning.

During commissioning a wizard guides through the individual steps.

Commissioning must be carried out in the following situations:

- For initial commissioning
- After a reset to the factory settings

To commission the device, perform the following steps:

Fig. 23: Commissioning "Smart Access Point": Language

1. Select the language.

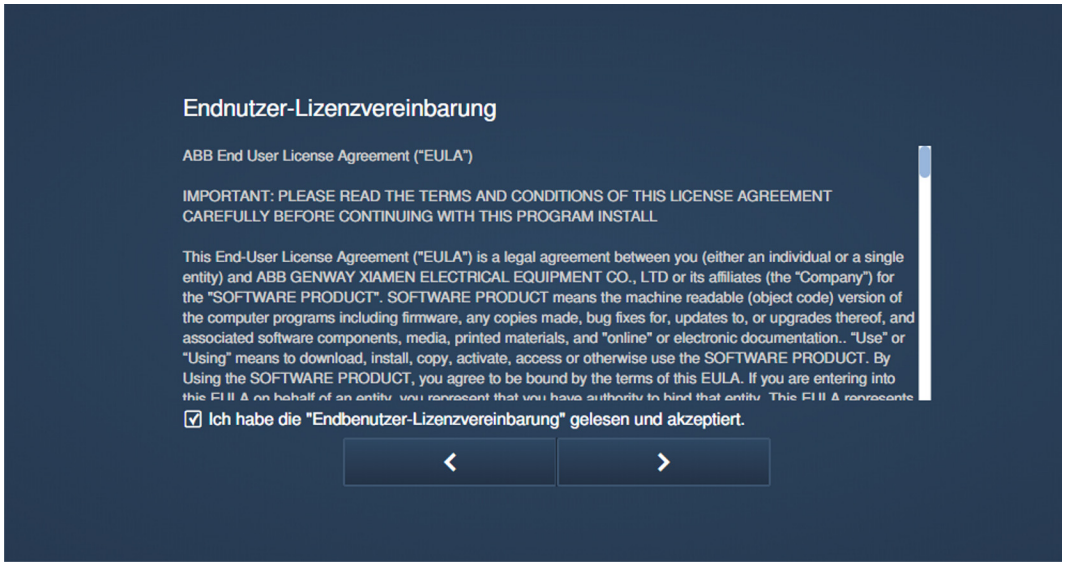


Fig. 24: Commissioning "Smart Access Point": Licence agreements

2. Accept the following licence agreements:
   - End-user licence agreement
   - Software licence agreement
   - Data protection declaration

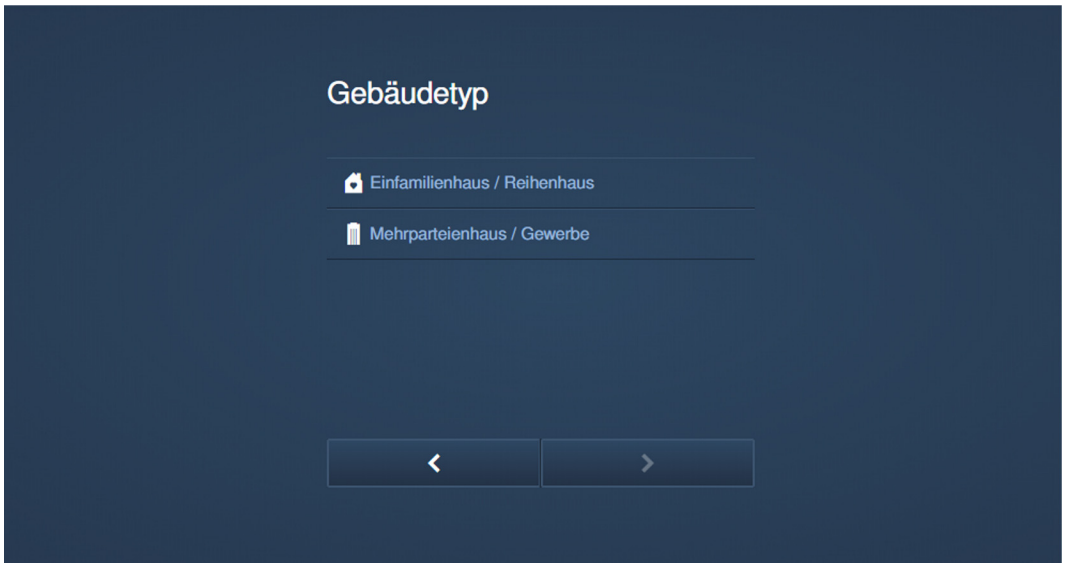


Fig. 25: Commissioning "Smart Access Point": Building type

3. Select the building type (system mode).
   – Detailed information: see chapter 0 “Mode "Multi-unit house / commercial"“ on page 36.
   – Attention:

     The building type can only be specified 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 the "Smart Access Point" to the factory settings.

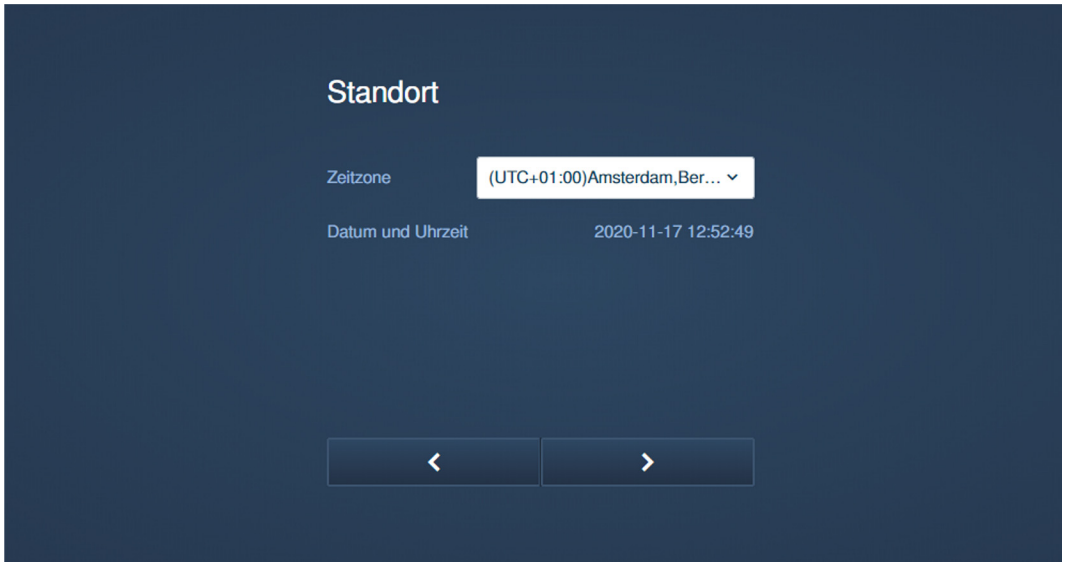


Fig. 26: Commissioning "Smart Access Point": Location

4. Enter the location.
   – A time zone can be selected from a drop-down menu.
   – This step can be skipped. During the later reconnection there is an automatic request for an adjustment if the values between the PC and the "Smart Access Point" do not match.

Fig . 27: Commissioning "Smart Access Point": WIFI settings

5. Entering the WIFI settings of the "Smart Access Point".
   - SSID (Name):
     - The name can be freely selected. This can, for example, be the name of the device (located on the device) or the name of the building in which the "Smart Access Point" is located.
   - Password:
     - The password must be changed during the initial setup. The password rule is displayed in a dialogue window when you enter the password.

       This password replaces the previous WLAN Access Point password of the "Smart Access Point". The factory password is printed on the "Smart Access Point".
     - The password is later necessary each time the "Smart Access Point" is called up.
     - Note down the password.
   - Country code
     - Ensure that the country code is selected correctly for the location of the device.

       The "Country code" setting ensures that your router will only activate WLAN settings that conform with the country's official regulatory laws.

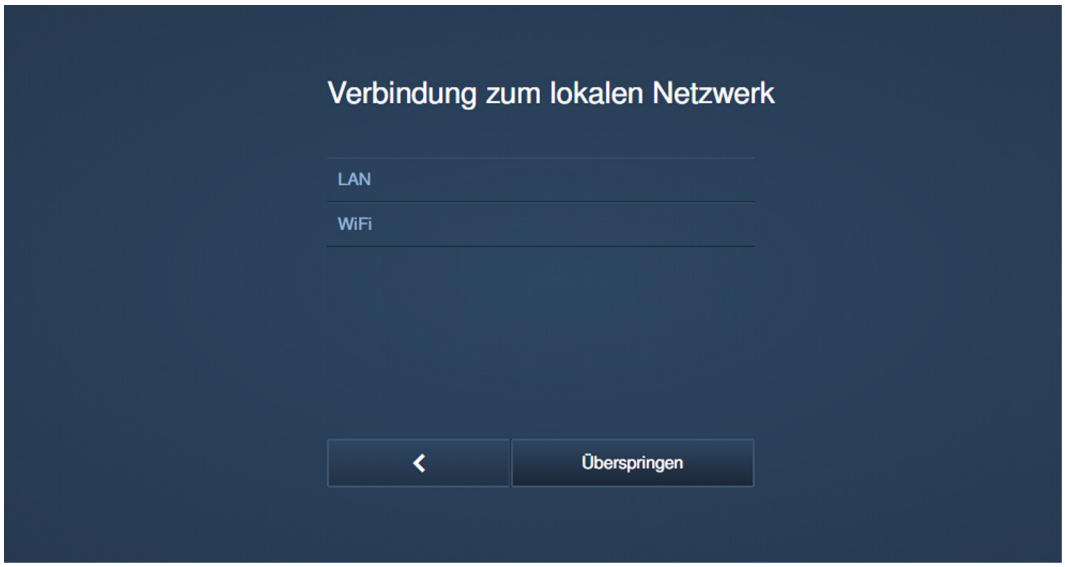


Fig. 28: Commissioning "Smart Access Point": Connection to the local network

6. Connection to the local network
   – Attention! Do **not** skip this step if devices are to be integrated now or later into the ABB-Welcome IP.

     For the application of the "Smart Access Point" in the "ABB-Welcome IP" system a selection of the type of connection is absolutely necessary. Even when no connection to a local network is planned. If this step is skipped, no devices can be added to the system after commissioning.

     If currently no connection to a local network is currently planned, select "LAN" or "WIFI".

- Option 1: LAN
  - All communication with system devices of the ABB-Welcome IP is carried out via a LAN interface.
  - All system devices of the ABB-Welcome IP keep their own IP address when they are used in the building network. The "Smart Access Point" can reach them even if they use a DHCP client IP address.
- Option 2: WLAN
  - All communication with system devices of the ABB-Welcome IP is carried out via a WLAN interface.
  - All system devices of the ABB-Welcome IP keep their own IP address when they are used in the building network. The "Smart Access Point" can reach them even if they use a DHCP client IP address.
- Option 3: Skip the selection
  - Communikation with system devices of the ABB-Welcome IP is not possible.

Fig. 29: Commissioning "Smart Access Point": LAN Network settings

7. Network settings
   - If a LAN connection was selected, the IP address must be specified to establish the LAN connection.
   - Checkbox "Obtain IP address automatically' is activated:
     - The "Smart Access Point" functions as DHCP client.
     - If the "Smart Access Point" is connected to DHCP server/router, the IP address is assigned automatically.
   - Checkbox "Obtain IP address automatically' is deactivated:
     - The "Smart Access Point" is to be reached in a network that operates with static IP addresses.
     - Here the network parameters such as IP address, subnet mask and gateway must be configured manually.

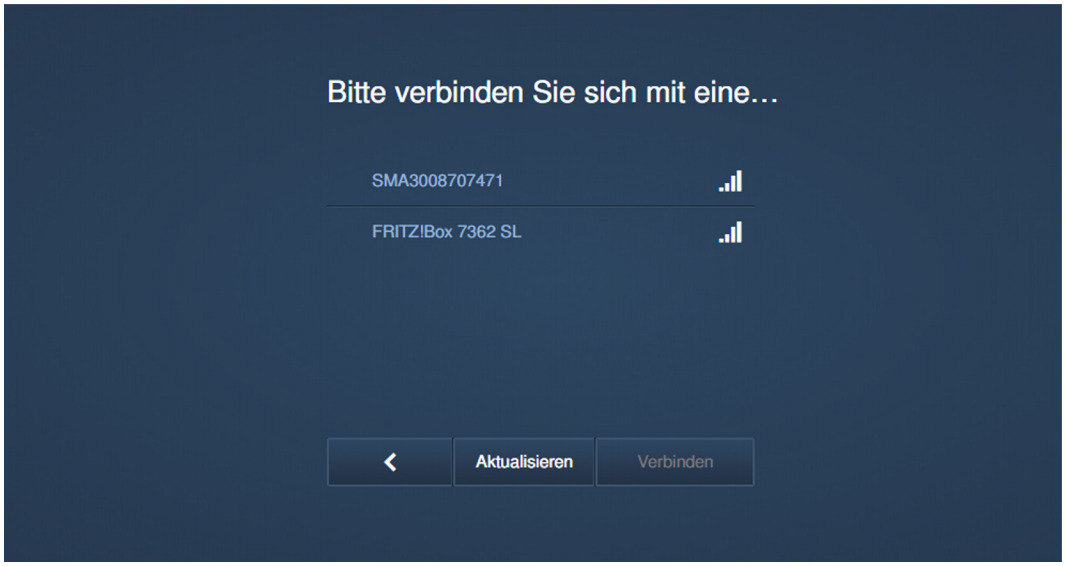


Fig. 30: Commissioning "Smart Access Point": WLAN connection

- If a WLAN connection is selected, a connection with a WLAN network must be established.
  - All available nearby WLAN networks will be displayed on the list.
  - If you can’t find the desired WLAN network, click the "Update" button to search again.
  - Click on the desired WLAN name (SSID) in the list, enter the password and then click on "Connect" to establish the connection to the WLAN network.

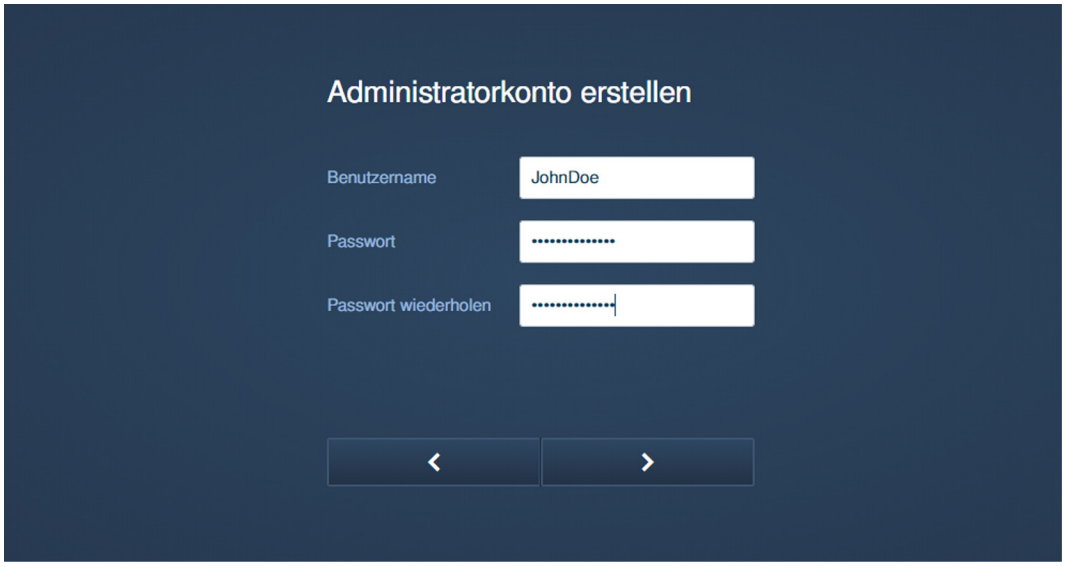


Fig. 31: Commissioning "Smart Access Point": Administrator account

8. Create administrator account (first admin user)
   - The administrator account has management and modification rights for the entire system. Additional accounts can be added at a later point in time. For example, an account with rights only for the administration of keys and names.
   - 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 3.5.1 “"Smart Access Point"“ on page 60.

Fig. 32: Commissioning "Smart Access Point": Options for resetting

9. Options for resetting the "Smart Access Point".
   - Without MyBuildings account
     - If this option is selected, anyone can reset the password for the first admin user by pressing the reset button.
     - This configuration is used when the "Smart Access Point" is installed in a private area and is not physically accessible to unauthorized users.
   - With MyBuildings account
     - If this option is selected, a one-time valid security code is needed to reset the password for the first admin user by pressing the reset button. The security code will only be sent to the email specified during the initial setup.
     - This configuration is used when the "Smart Access Point" is installed in a public area and is not physically accessible to unauthorized users.
     - For this option the registration for a "myBuildings account" is necessary.

       If you are not yet registered for a "myBuildings account", this can be done for this selection in the next step.

Notice
- The reset option can only be specifies during the initial setup and cannot be changed after the initial setup.
  - The reset option can only be changed later when you restore the "Smart Access Point" to the factory settings.
- An Internet connection is required for the reset option of "With MyBuildings account". If this is not available or it should not be used, skip the next step.

10. Performing "myBuildings" settings:

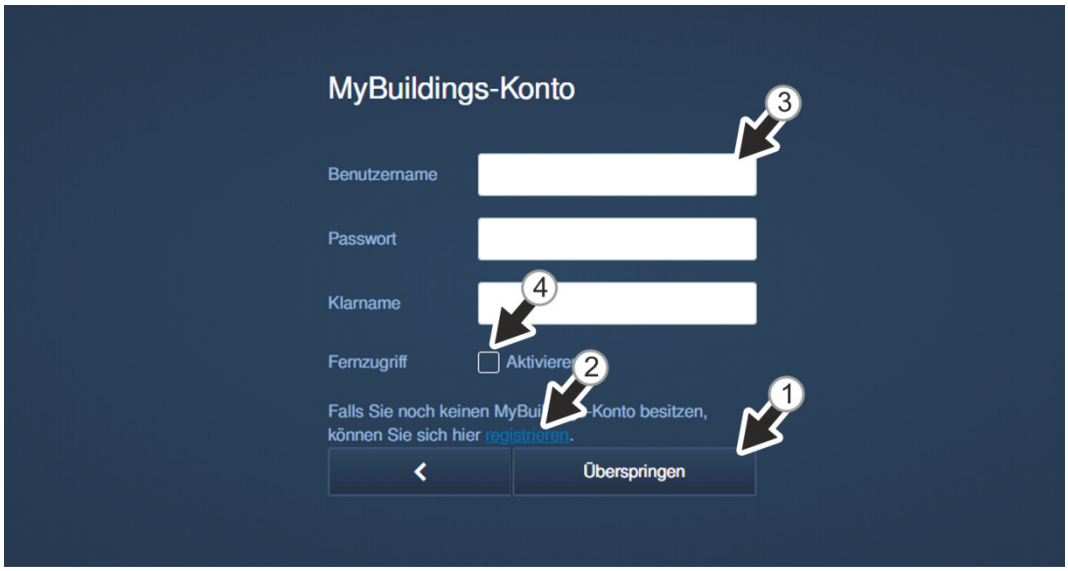


Fig. 33: Commissioning "Smart Access Point": Without myBuildings account

- Reset option: "Without myBuildings account"
  - This page is displayed when the reset option is set on "Without myBuildings account".

[1] Click on the "Skip" button to change to the next step if no connection is to be established with myBuildings.

[2] The myBuildings portal is called up via the "Register" link. There an account can be registered if necessary.

[3] Enter the user name, the password and the display name. Then click on "Connect". A connection with the MyBuildings portal is established.

[4] If access is to be gained to the "Smart Access Point" via the MyBuildings portal, the remote access must be activated (activate the checkbox).

Fig. 34: Commissioning "Smart Access Point": With myBuildings account

- Reset option: "With myBuildings account"
  - This page is displayed when the reset option is set on "With myBuildings account".

  [1] A myBuildings account is required for this reset option. The myBuildings portal is called up via the "Register" link. There an account can be registered if one is not yet available.

  [2] Enter the user name, the password and the display name. Then click on "Connect". A connection with the myBuildings portal is established.

  [3] Enter the e-mail address that is to be used to activate the myBuildings account. This e-mail address will receive a security code when the first admin user is to be reset. If you want to reset the password for the first administrator, see chapter 3.5.1 “"Smart Access Point"“ on page 60.

  [4] If access is to be gained to the "Smart Access Point" via the myBuildings portal, the remote access must be activated (activate the checkbox).

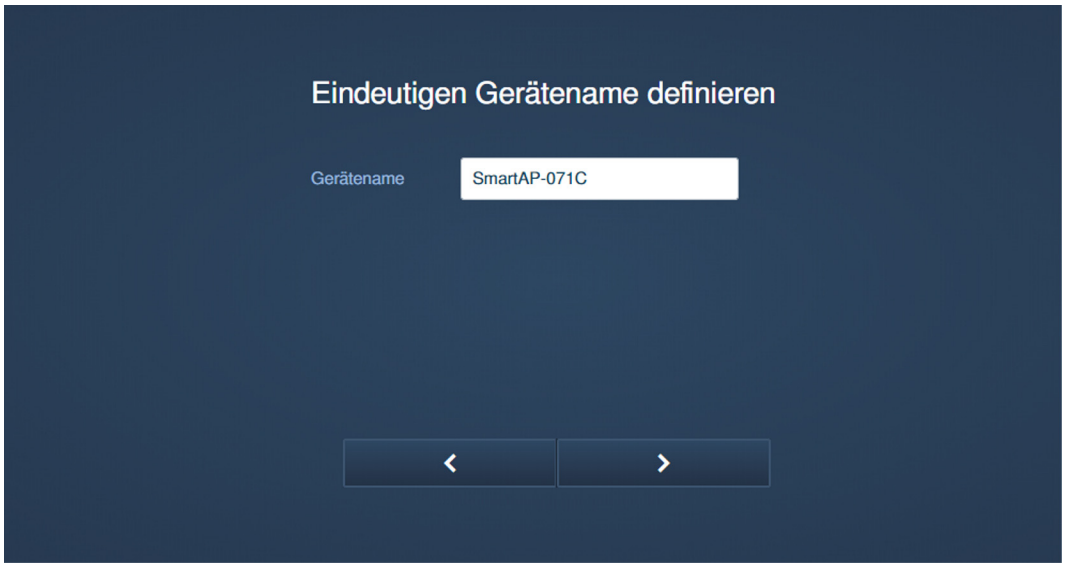


Fig. 35: Commissioning "Smart Access Point": Device name

11. Define an unmistakable device name.
    - The UPnP device name is defined with the device name.
    - The device name will be displayed on the log in screen.

Fig. 36: Commissioning "Smart Access Point": Overview of settings

12. Overview of settings
    - The "Overview of settings" page is merely a display in which all the settings made can be checked again.
        - If you navigate with the mouse pointer to the right next to the text, a photo sequence is faded in.
    - If a setting is to be changed, navigate via the forward/back buttons to the page with the desired settings to change them. All other settings are retained.

Fig . 37: Commissioning "Smart Access Point": Confirm settings

13. Confirm the settings made.
    – The system configures itself.

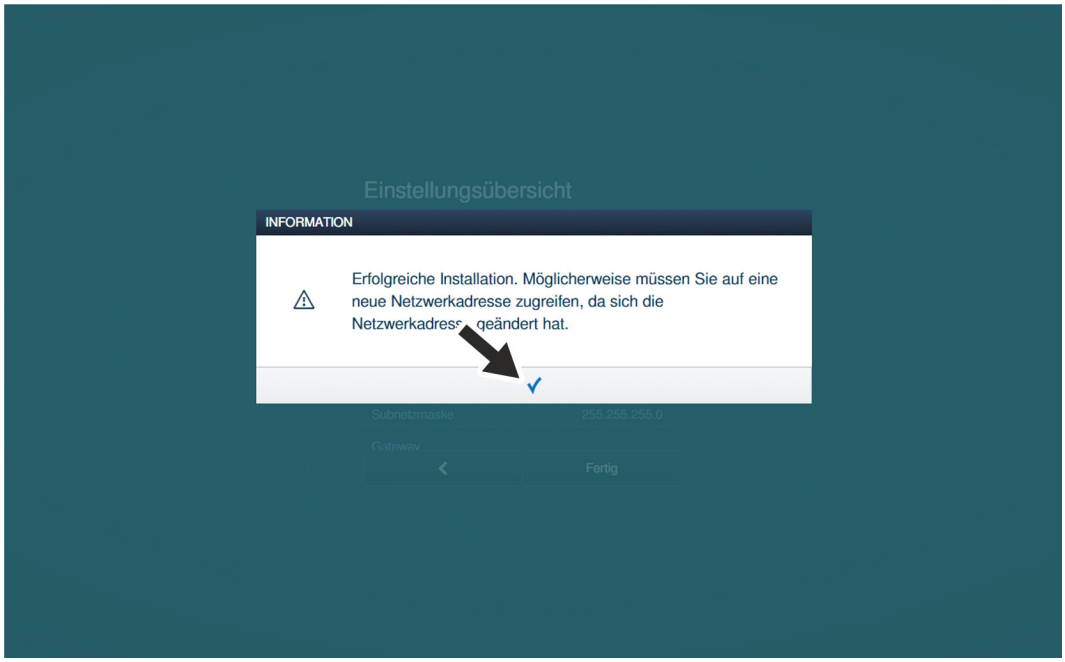


Fig . 38: Commissioning "Smart Access Point": Confirm commissioning

14. Confirm the configuration.

Fig. 39: Commissioning "Smart Access Point": Separation of connection

- At the end of initial commissioning the "Smart Access Point" switches automatically into the Access-Point mode (the LED lights up red).
- The WLAN connection with the "Smart Access Point" is activated with the new data.
- From now on the "Smart Access Point" switches directly into the Access-Point after every boot-up.

For the additional commissioning access can be gained to the Smart Access Point either via WLAN AP or via LAN.

- Attention:

  The "Smart Access Point" can only be accessed via WLAN with the new access data.

3.1.5 Preliminary information: Adjusting IP addresses to a PC

Depending on the setup of the system, the IP address of the connection must be put on the same area on the PC / laptop as that of the device (only required once). Otherwise the Web browser does not establish a connection to the device.

Setting of the IP address according to the example of Windows 10 operating system

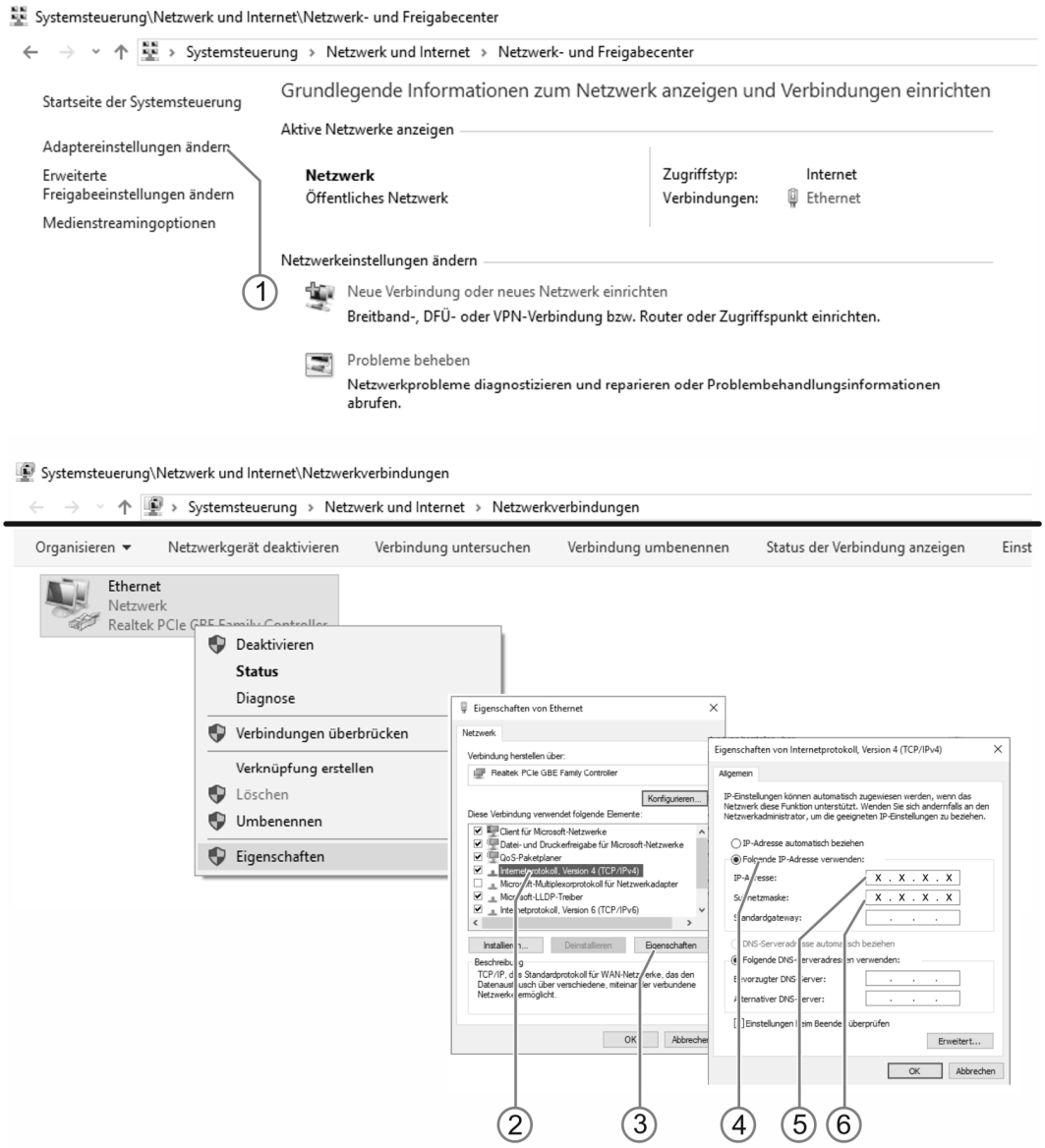


Fig. 40: Setting the IP address in the PC (example Windows 10)

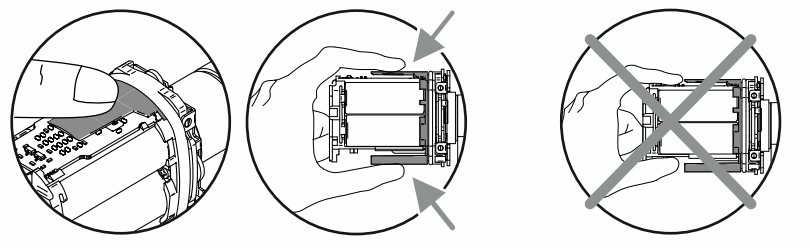
Use the following steps to set the IP address:

1. Switch to the system controller.
2. Open: The network and the enabling centre.
   – "Network and Internet" / "Network and enabling centre".
3. Open: "Changing the adapter settings" [1].
   – The dialogue field "Network connections" is displayed.
4. Mark the network connections in the dialogue field and open them with a right click: Properties [3].
5. Mark in dialogue field: "Internet protocol Version 4 (TCP/IPv4)" [2].
6. Open in dialogue field: Properties [3].
7. Activate in dialogue field: Use the following IP address [4].
8. Enter the desired IP address at "IP address" [5].
9. At "Subnet mask": Only enter a click [6].
   – The address is located automatically.
10. Confirm and close all windows.

The device can now be called up via a Web browser.

3.2 Adding devices

3.2.1 "Electronic cylindrical lock"



Attention! - Damage to the electronics

When touching electronic components they can be damaged by the electrostatic discharge of a person.

– When pulling the knob housing off, keep the reading head on the contact protection provided.

The method of commissioning of the "Electronic cylindrical lock" is the same for all profile types.

The following points are a prerequisite for commissioning the "Electronic cylindrical lock":

- A connection to the "Smart Access Point Pro". This must be the "Smart Access Point Pro" that is used in the system.
  - "Smart Access Point Pro":
    - The "Smart Access Point Pro" must be ready for operation.
    - A PC is connected with the "Smart Access Point Pro".
    - The management software of the "Smart Access Point Pro" is opened on the PC.
- The serial number of the "Electronic cylindrical lock". This is located on the reading head.
- The batteries of the "Electronic cylindrical lock" (are supplied).
- The maintenance card.
- If locking rights for persons are to be assigned already during commissioning, also transponder keys are required.
  – It is recommended, however, to carry this out separately especially for larger projects.
  – For the assigning of locking rights, see chapter 5.5 “User management“ on page 131.

Use the following points for commissioning the "Electronic cylindrical lock":

1. Ensure that there is a radio connection between the reading head and the "Smart Access Point Pro". The radio connection can be implemented in different ways.
   - The "Electronic cylindrical lock" is already mounted:
     – The communication is carried out directly with the "Smart Access Point Pro" or via the already available installation of interconnected auxiliary devices ("RF Repeater" / "RF/IP Gateway".
     – If communication is not possible, the reading head of the "Electronic cylindrical lock" must be dismantled and put near the "Smart Access Point Pro". For additional information: see chapter 3.2.2 “Adding larger projects / devices in advance“ on page 55.
   - The "Electronic cylindrical lock" is not yet mounted:
     – The "Electronic cylindrical lock" together with the required ancillary devices is brought into the radio range of the "Smart Access Point Pro". For additional information: see chapter 3.2.2 “Adding larger projects / devices in advance“ on page 55.

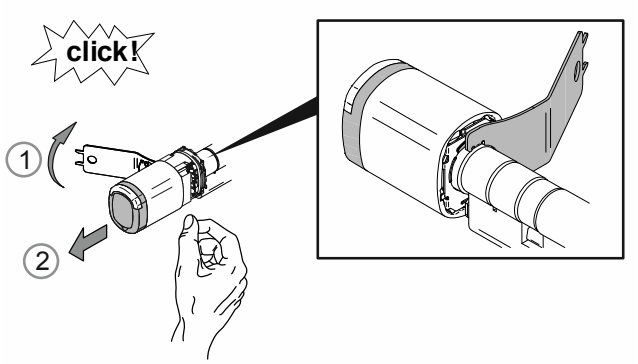


Fig. 41: Pulling the head housing off

2. Unlock the head housing of the reading head with the mounting tool [1] and pull it off [2].

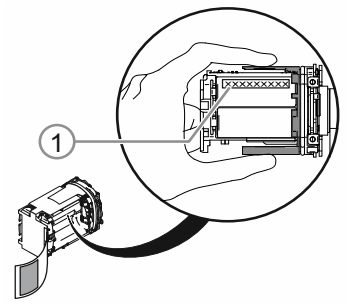


Fig. 42: Serial number

3. Note down the serial number [1].
   – The serial number is necessary for logging into the management software of the "Smart Access Point Pro".
   - Also scanning the QR code and logging in with the ABB-Welcome® App is possible.

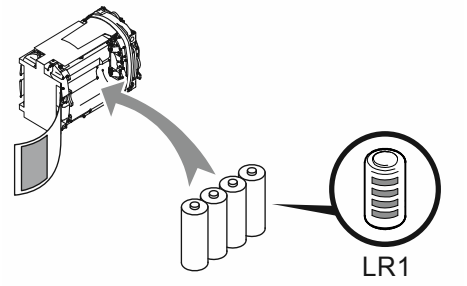


Fig. 43: Inserting the batteries

4. Inserting the batteries of the "Electronic cylindrical lock".

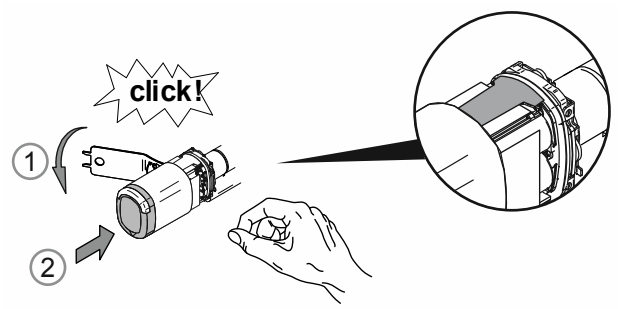


Fig. 44: Mounting the head housing

5. Remount the head housing of the reading head.
   – Ensure that the contact protection remains within the head housing and does not buckle during mounting.

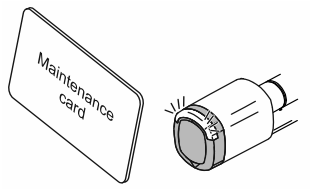


Fig. 45: Maintenance card

6. Log the reading head into the "Smart Access Point Pro" with the maintenance card.
   – To log in the reading head, change into the management software of the "Smart Access Point Pro.
   – For the necessary steps in the management software, see chapter 5.2.2 “Creating floors“ on page 99.
     – The reading head is added to the list of available devices.
7. Placing the reading head in the building structure of the "Smart Access Point Pro".
   – To place the reading head, change into the management software of the "Smart Access Point Pro.
   – For the necessary steps in the management software, see chapter 5.4.3 “Placing the "Electronic cylindrical lock"“ on page 120.
     – If the building structure is not yet available, first create it, see chapter 5.3.2 “Add "Electronic cylindrical lock"“ on page 105.

8. Coupling the reading head in building structure of the "Smart Access Point Pro" with the "Smart Access Point Pro", "RF/IP Gateway" or a "RF Repeater".
   – To couple the reading head, change into the management software of the "Smart Access Point Pro.
   – For the necessary steps in the management software, see chapter 5.4.4 “Coupling the "Electronic cylindrical lock" with the "Smart Access Point Pro"“ on page 122.
      – If the "Smart Access Point Pro", "RF/IP Gateway" or "RF Repeater" is not yet placed, carry this out first, see chapter 5.2 “Building structure“ on page 95 and see chapter 5.4 “Access control“ on page 113.

If the "Electronic cylindrical lock" is logged, placed and coupled into the management software of the "Smart Access Point Pro", locking rights for the lock can be created for persons.

– To assign locking rights, change into the management software of the "Smart Access Point Pro.
– For the necessary steps in the management software, see chapter 5.5 “User management“ on page 131.

3.2.2 Adding larger projects / devices in advance

Adding the "Electronic cylindrical lock" can become a time-consuming and bothersome matter particularly for larger projects. Especially when the "Electronic cylindrical lock" are mounted further removed from the "Smart Access Point Pro".

In such cases it is recommended to commission all devices ("Electronic cylindrical lock", "RF Repeater", etc) directly on the "Smart Access Point Pro" before mounting, and to mount them only later at their area of application. Create for this an appropriate plan.

One thing needs to be observed for this procedure. During commissioning of the "Electronic cylindrical lock" the entire communication path between the reading head and the "Smart Access Point Pro" is stored in the management software. If the "Electronic cylindrical lock", with the additional devices that may be required, is later mounted at the area of application, this communication path must match. If it does not, the respective "Electronic cylindrical lock" is displayed as not recognized and must be commissioned again.

This also applies if a "Electronic cylindrical lock" is mounted at a different area of application at a later point in time.

Notice
This slightly more complex commissioning takes place against the background that the entire device control is carried out outside of the battery-operated access devices. This reduces the energy consumption of the reading heads and increases the service life of the batteries.

3.2.3 "RF/IP Gateway"

The following points are a prerequisite for commissioning the "RF/IP Gateway".

- The "RF/IP Gateway" is connected to the network.
- The power supply of the "RF/IP Gateway" is established.
  - Via PoE or via a separate 24 V power supply.
- The serial number of the "RF/IP Gateway". This is located on the device.
- The "Smart Access Point Pro" is ready for operation. This must be the "Smart Access Point Pro" that is used in the system.
  - „Smart Access Point Pro“:
    - A PC is connected with the "Smart Access Point Pro".
    - The management software of the "Smart Access Point Pro" is opened on the PC.

If the commissioning process has been prepared, the "RF/IP Gateway" is added in the management software of the "Smart Access Point Pro".

Use the following points for commissioning the "RF/IP Gateway":

1. Add the "RF/IP Gateway" in the "Smart Access Point Pro".
   - To add, change into the management software of the "Smart Access Point Pro".
   - For the necessary steps in the management software, see chapter 5.3.4 “Add "RF/IP Gateway"“ on page 108

2. Place the "RF/IP Gateway" in building structure of the "Smart Access Point Pro".
   – To place the "RF/IP Gateway", change into the management software of the "Smart Access Point Pro".
   – For the necessary steps in the management software, see chapter 5.4.2 “Placing the "RF/IP Gateway"“ on page 117
      – If the building structure is not available, first create it, see chapter 5.2 “Building structure“ on page 95

Notice

Depending on the installation, it can be practical to commission the "RF/IP Gateway" in advance together with the "Electronic cylindrical lock".

– For the advance commissioning, see chapter 3.2.2 “Adding larger projects / devices in advance“ on page 55

3.2.4 "RF Repeater"

The following points are a prerequisite for commissioning the "RF Repeater".

- The power supply of the "RF Repeater" is established.
  – The power is supplied via a separate 24 V power supply.
- The serial number of the "RF Repeater". This is located on the device.
- A connection to the "Smart Access Point Pro". This must be the "Smart Access Point Pro" that is used in the system.
  - "Smart Access Point Pro":
    - The "Smart Access Point Pro" must be ready for operation.
    - A PC is connected with the "Smart Access Point Pro".
    - The management software of the "Smart Access Point Pro" is opened on the PC.

Use the following points for commissioning the "RF Repeater":

1. Ensure that there is a radio connection between the "RF Repeater" and the "Smart Access Point Pro". The radio connection can be implemented in different ways.
   - The "RF Repeater" is already mounted:
     – The communication is carried out directly with the "Smart Access Point Pro" or via the already available installation of interconnected additional "RF Repeater".
     – If communication is not possible, the "RF Repeater" must be dismantled and put near the "Electronic cylindrical lock". For additional information: see chapter 3.2.2 “Adding larger projects / devices in advance“ on page 55.
   - The "RF Repeater" is not yet mounted:
     – The "RF Repeater" together with the required ancillary devices is brought into the radio range of the "Smart Access Point Pro". For additional information: see chapter 3.2.2 “Adding larger projects / devices in advance“ on page 55.
2. Add the "RF Repeater" in the "Smart Access Point Pro".
   – To add, change into the management software of the "Smart Access Point Pro".
   – For the necessary steps in the management software, see chapter 5.3.5 “Add "RF Repeater"“ on page 111

3. Place the "RF Repeater" in building structure of the "Smart Access Point Pro".
   – To place the "RF Repeater", change into the management software of the "Smart Access Point Pro".
   – For the necessary steps in the management software, see chapter 5.4.5 “Placing the "RF Repeater"“ on page 126
      – If the building structure is not available, first create it, see chapter 5.2 “Building structure“ on page 95
4. Coupling the "RF Repeater" in building structure of the "Smart Access Point Pro" with the "Smart Access Point Pro", "RF/IP Gateway" or a "RF Repeater".
   – To couple, change into the management software of the "Smart Access Point Pro".
   – For the necessary steps in the management software, see chapter 5.4.6 “Coupling the "RF Repeater"“ on page 129
      – If the "Smart Access Point Pro", "RF/IP Gateway" or an additional "RF Repeater" is not yet placed, carry this out first, see chapter 5.3 “Device configuration“ on page 103 and see chapter 5.4 “Access control“ on page 113

Notice

Depending on the installation, it can be practical to commission the "RF Repeater" in advance together with the "Electronic cylindrical lock".

– For the advance commissioning, see chapter 5.5 “User management“ on page 131

3.3 Delete device in the "Smart Access Point"

3.3.1 "Electronic cylindrical lock"

If the "Electronic cylindrical lock" is to be removed from the system, this is carried out in the management software of the "Smart Access Point Pro".

1. Uncoupling the "Electronic cylindrical lock", see chapter 5.7.1 “Uncoupling "Electronic cylindrical lock" from "Smart Access Point Pro" “ on page 153.
2. Removing the "Electronic cylindrical lock" from the building structure, see chapter 5.7.2 “Removing the "Electronic cylindrical lock" from the room “ on page 156.
3. Removing the "Electronic cylindrical lock" from the management software, see chapter 5.8.1 “Deleting the "Electronic cylindrical lock" from the system“ on page 162.

3.3.2 "RF/IP Gateway"

If the "RF/IP Gateway" is to be removed from the system, this is carried out in the management software of the "Smart Access Point Pro".

1. Removing the "RF/IP Gateway" from the building structure, see chapter 5.7.5 “Removing the "RF Repeater" from the room“ on page 160.
2. Removing the "RF/IP Gateway" from the management software, Page 164.

3.3.3 "RF Repeater"

If the "RF Repeater" is to be removed from the system, this is carried out in the management software of the "Smart Access Point Pro".

1. Uncoupling the "RF Repeater", see chapter 5.7.4 “Uncoupling the "RF Repeater" Fehler! Textmarke nicht definiert.“ on page 158.
2. Removing the "RF Repeater" from the building structure, see chapter 5.7.5 “Removing the "RF Repeater" from the room“ on page 160.
3. Removing the "RF Repeater" from the management software, see chapter 5.8.2 “Deleting the "RF Repeater" from the system“ on page 163.

3.4 Backup / restore the project

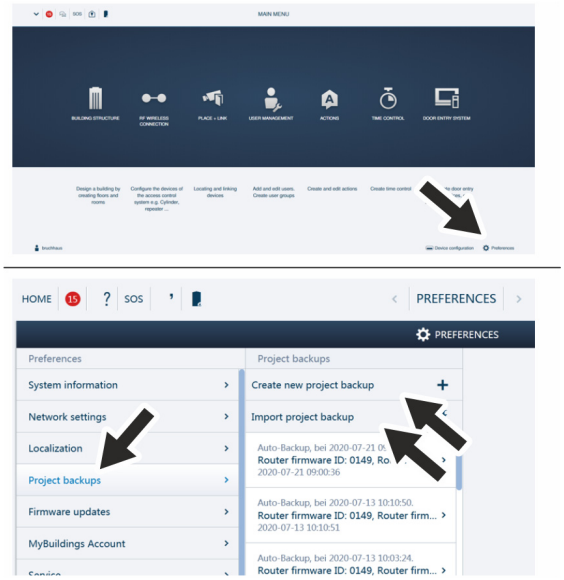


Fig. 46: Data backup / data restoration

Create the first data backup after the first initialization has been completed.

Then create a backup after every major change, such as the addition or deletion of devices.

To create the data backup, carry out the following steps:

1. Connect a PC with the "Smart Access Point".
   – More detailed information for connecting, see chapter 3.1.2 “Connecting a PC with the "Smart Access Point ““ on page 33
2. In the main menu of the "Smart Access Point", change to the "Settings" function.
3. Change to the "Project backup“ function.

Creating data backup

1. The backup file is created via the "Create new project backup" function.

Playback of data backup

1. The backup file is imported via the "Import project backup" function.

Attention! Loss of data

If no backup is available and the data in the "Smart Access Point" are lost, the battery-operated access systems can no longer be uncoupled for re-commissioning. The old data remain in the reading heads. Since these are locking systems, access from outside is not possible. This could be an unauthorized access.

– The battery-operated access systems must then be reset in the manufacturer's factory.
  – Make absolutely certain that you have a backup of the data of the "Smart Access Point".

3.5 RESET (Reset system / devices)

3.5.1 "Smart Access Point"

Completely resetting the "Smart Access Point".

– Here all entered data, performed settings, etc., are deleted. After the reset the "Smart Access Point" will be in the state at the point of delivery.
– After the reset, an initial commissioning of the "Smart Access Point" must be carried out.
– After the initial commissioning, old data can be read in via an available backup.

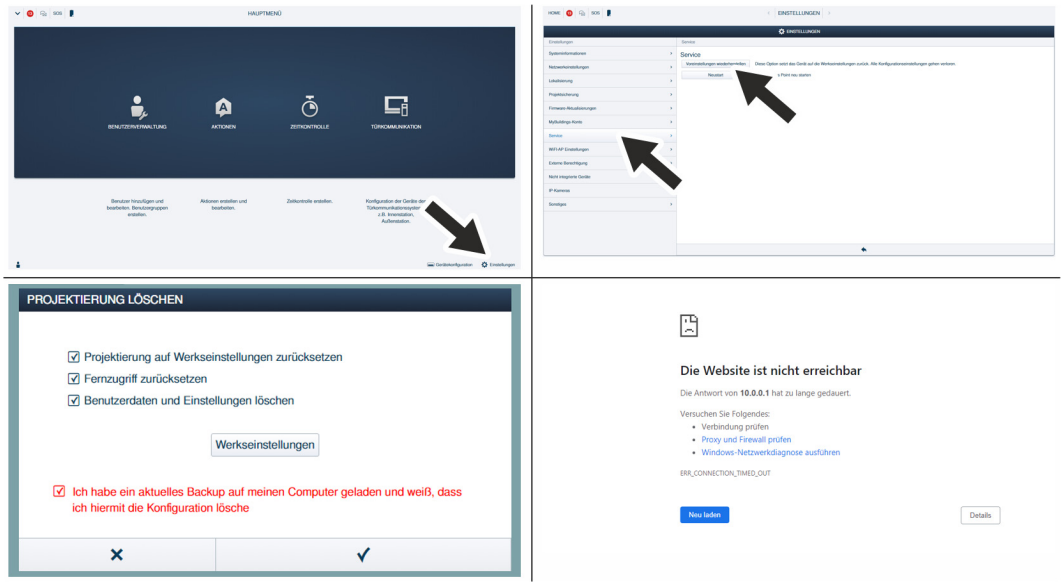


Fig. 47: Completely resetting the "Smart Access Point"

Use the following steps for the reset:

1. Connect a PC with the "Smart Access Point".
   – More detailed information for connecting, see chapter 3.1.2 “Connecting a PC with the "Smart Access Point ““ on page 33.
2. Change to the "Settings" / "Service" function.
3. Call up the "Reset default settings" function.
4. Select the areas that are to be reset.
5. Confirm the selection.
   – The "Smart Access Point" is being reset.
   – After the reset the connection to the "Smart Access Point" is no longer active.
   – The "Smart Access Point" must be put back into operation via an initial commissioning, see chapter 3.1 “Commissioning of the system - "Smart Access Point Pro"“ on page 33.

Resetting the password of the 1st administrator.

The reset depends on the option of resetting that was selected for the commissioning of the "Smart Access Point".

- Option "Without MyBuildings account":
  - The password of the 1st administrator is reset on the rear side of the "Smart Access Point" via the "Reset" button.
- Option "With MyBuildings account":
  - The password of the 1st administrator is reset via a security release that is sent by e-mail via the "myBuildings account".

Resetting the settings when the "Smart Access Point" can no longer be reached.

This can happen, for example, when the network settings are entered incorrectly.

1. Connect a PC with the "Smart Access Point".
   - More detailed information for connecting, see chapter 3.1.2 “Connecting a PC with the "Smart Access Point ““ on page 33.
2. Call up the start page of the "Smart Access Point" in a commercially available browser with one of the following IP addresses.
   - Via the static IP address "10.0.0.1".
   - Via the IP address "192.168.3.1", if the "Smart Access Point" is in the Access-Point mode.
     - The "Smart Access Point" switches automatically into the Access-Point mode after every boot-up. The LED on the rear side of the device then lights up red.
   - Via an IP address that was assigned by the DHCP function of a router.
     - For this a router must be connected with the "Smart Access Point" in addition to the PC.
     - The assigned address is obtained via the router. This depends on the router used.

The settings can be changed normally if the start page of the "Smart Access Point" is called up.

4 Information about planning and application

4.1 Principles of function / principles of operation

"Electronic cylindrical lock" with transponder key (radio control communication device)

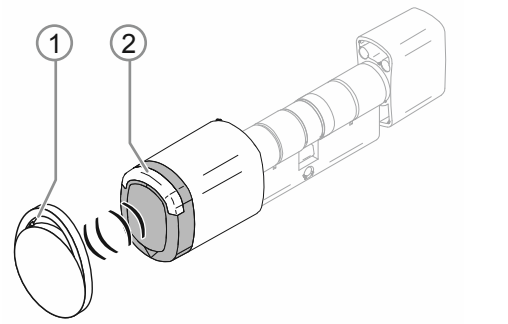


Fig. 48: "Electronic cylindrical lock" with transponder key

[1] Transponder key in the form of a tag

[2] Reading head "Electronic cylindrical lock"

The "Electronic cylindrical lock" is switched with the aid of a transponder key via RFID. The RFID transponder key is a small tag that contains a programmed chip. The transponder key that is held in front of the reading head of the "Electronic cylindrical lock" permits authorized persons access to the building or room.

Every transponder key has its own individual serial number that is stored in the "Smart Access Point Pro". It is only when this serial number is correctly recognized and the owner has access rights, does the reading head switch and the lock can be opened.

Switching process of the reading head

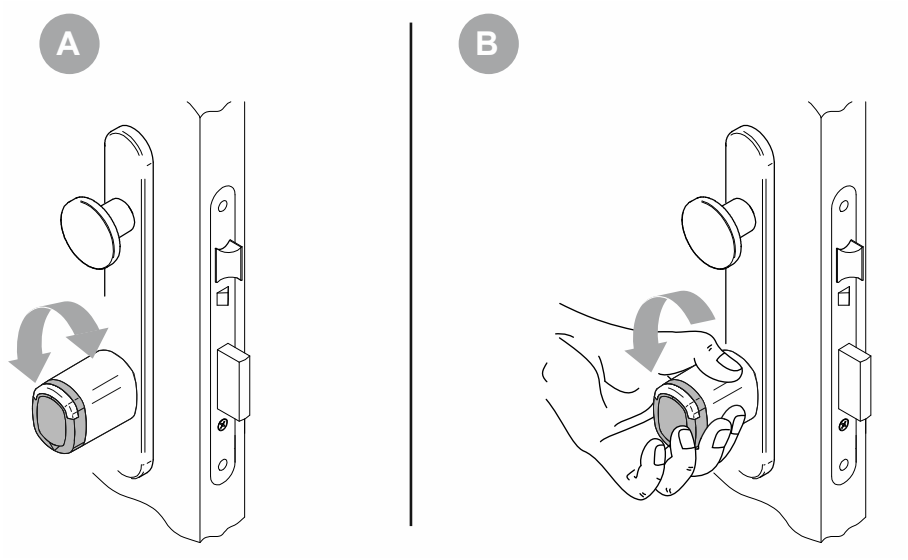


Fig. 49: Switching process of the reading head

In a locked state of the door the reading head can be freely turned in front of the cylinder (A). Operation of the cylindrical lock is not possible. It is only when a person with access rights holds his transponder key in front of the reading head that the reading head switches and establishes a mechanical connection to the cylindrical lock for a few seconds. The lock can then be opened (B). After the preset time has expired, the reading head automatically switches back into the locked state of the door.

Communication of the reading head

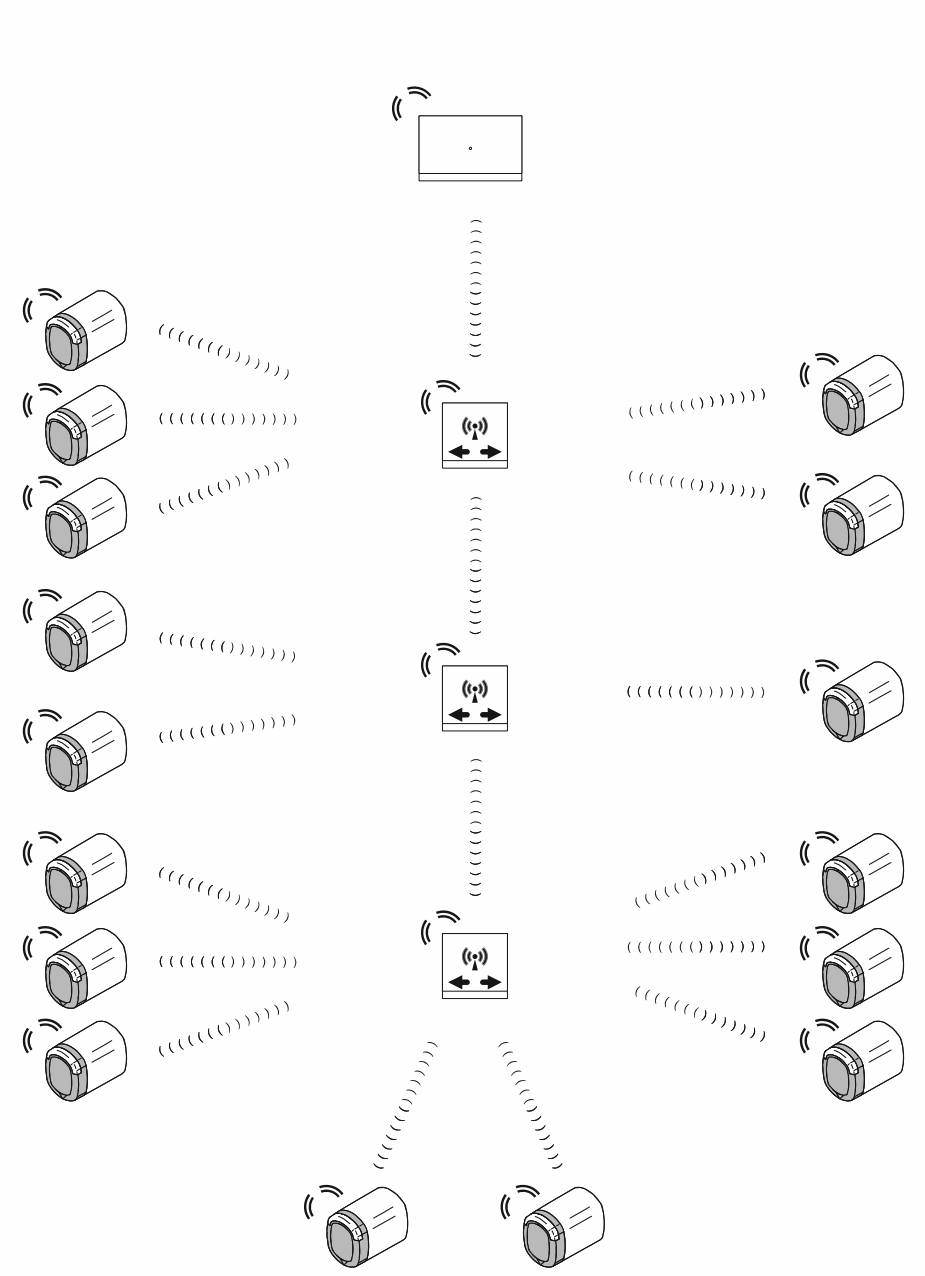


Fig. 50: Communication of the reading head

The communication of the reading head with the management software of the "Smart Access Point Pro" is carried out via the radio frequencies of Bluetooth. The transmission range between the individual devices therefore amounts to approximately 10 meters.

– To increase the transmission range, "RF Repeater" are used. With the use of "RF Repeater" the total transmission range in a radio line can be increased to approximately 40 meters.
– If a transmission range larger than 40 meters is required, this is implemented with the use of additional "RF/IP Gateway".

Notice

Only Bluetooth frequencies are used. The conventional functionalities of Bluetooth are not integrated (e.g. visibility of the reading head on a smartphone).

4.2 Capacity / Transmission range

Overview

System capacity "ABB-AccessControl"	
Management software in the "Smart Access Point Pro"	Up to 600 devices

Table 6: System capacity "ABB-AccessControl"

Activation capacity	
"Smart Access Point Pro"	Up to 16 "Electronic cylindrical lock" Up to 3 "RF Repeater" Up to 64 "RF/IP Gateway"
"RF Repeater"	Up to 16 "Electronic cylindrical lock" – Feed-through of the capacity of the "Smart Access Point Pro" / "RF/IP Gateway"
"RF/IP Gateway"	Up to 16 "Electronic cylindrical lock" Up to 3 "RF Repeater"

Table 7: Activation capacity

Transmission ranges	
Radio range between 2 individual devices	Approx. 10 meters
Radio range within a radio line	Approx. 40 meters
System range via radio and IP network	Up to approx. 1.5 kilometres

Table 8: Transmission ranges

Radio range

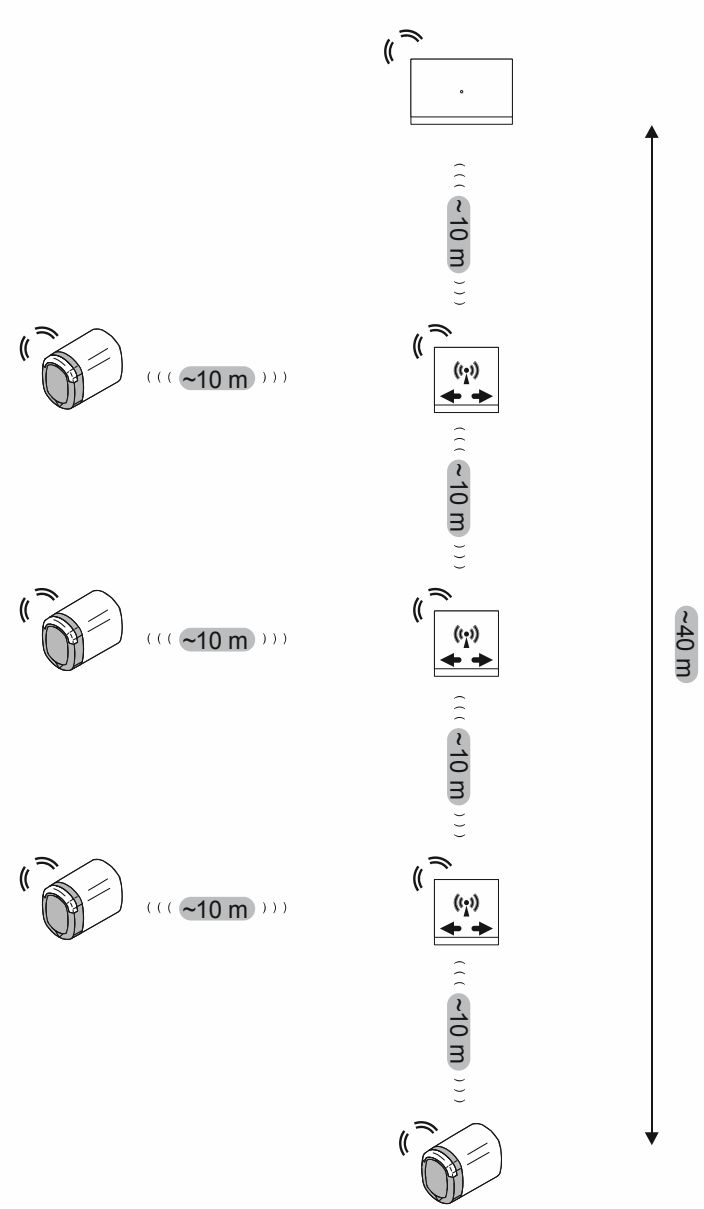


Fig. 51: Radio range between devices

The radio range between each device amounts to a maximum of 10 meters

Seen from a "Smart Access Point Pro" or "RF/IP Gateway", up to 3 "RF Repeater" can be switched in sequence. Such a sequence forms a radio line.

This results in a maximum radio range between a "Smart Access Point Pro" or "RF/IP Gateway" up to the remotest "Electronic cylindrical lock" of around 40 meters.

Maximum number of "Electronic cylindrical lock" in a radio line.

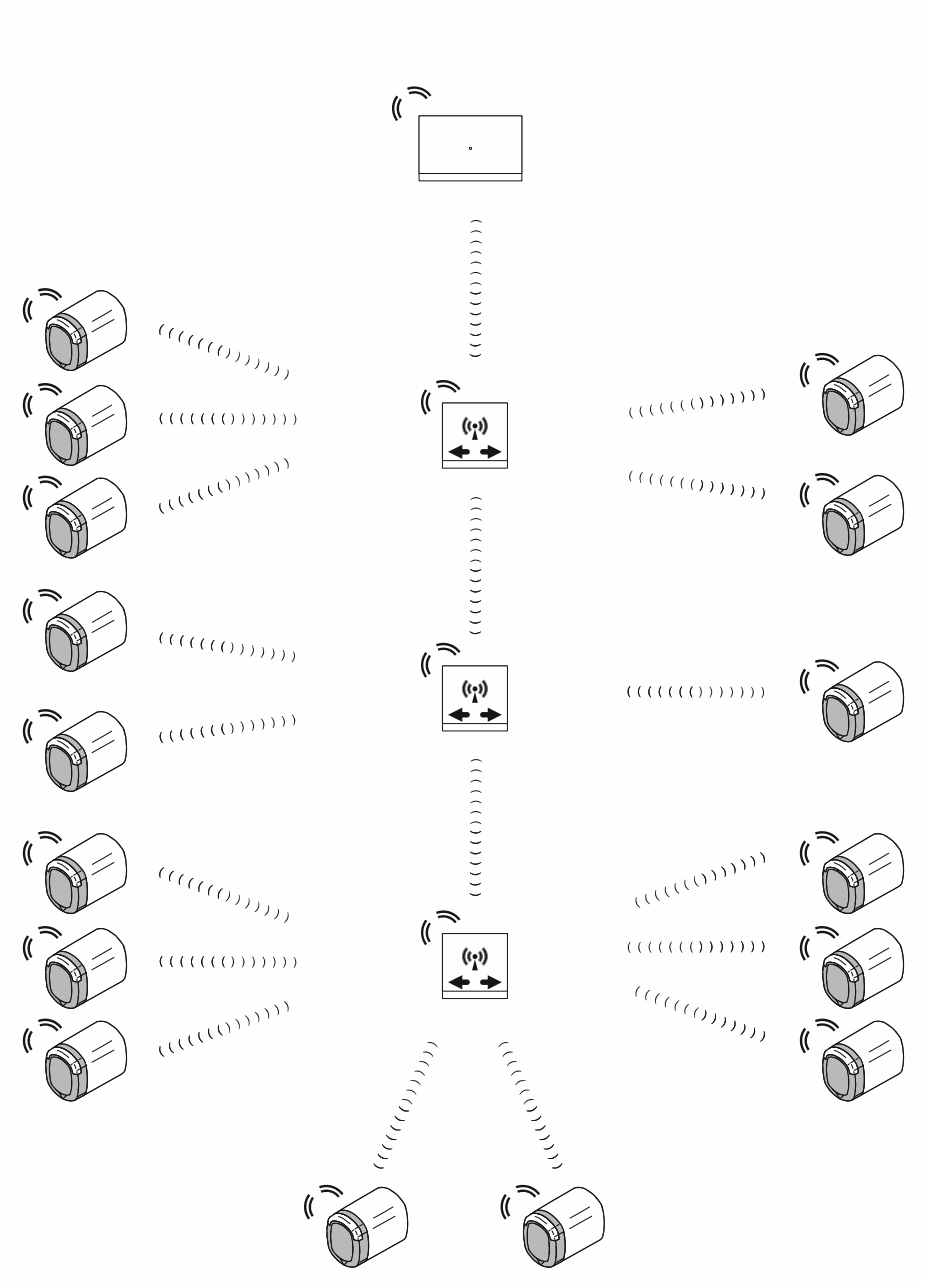


Fig. 52: Maximum number of "Electronic cylindrical lock" in a radio line

Up to a total of 16 "Electronic cylindrical lock" can be activated via the "Smart Access Point Pro" or a "RF/IP Gateway".

The "Electronic cylindrical lock" can be freely distributed in the radio line to the "RF Repeater". Each "RF/IP Gateway" in the radio line can operate from 0 to 16 "Electronic cylindrical lock".

– However, the maximum number of 16 "Electronic cylindrical lock" in the radio line must not be exceeded.

No "Electronic cylindrical lock" can be operated on the "Smart Access Point Pro" or "RF/IP Gateway" if the signals are transmitted to "RF Repeater".

Total capacity and total transmission range

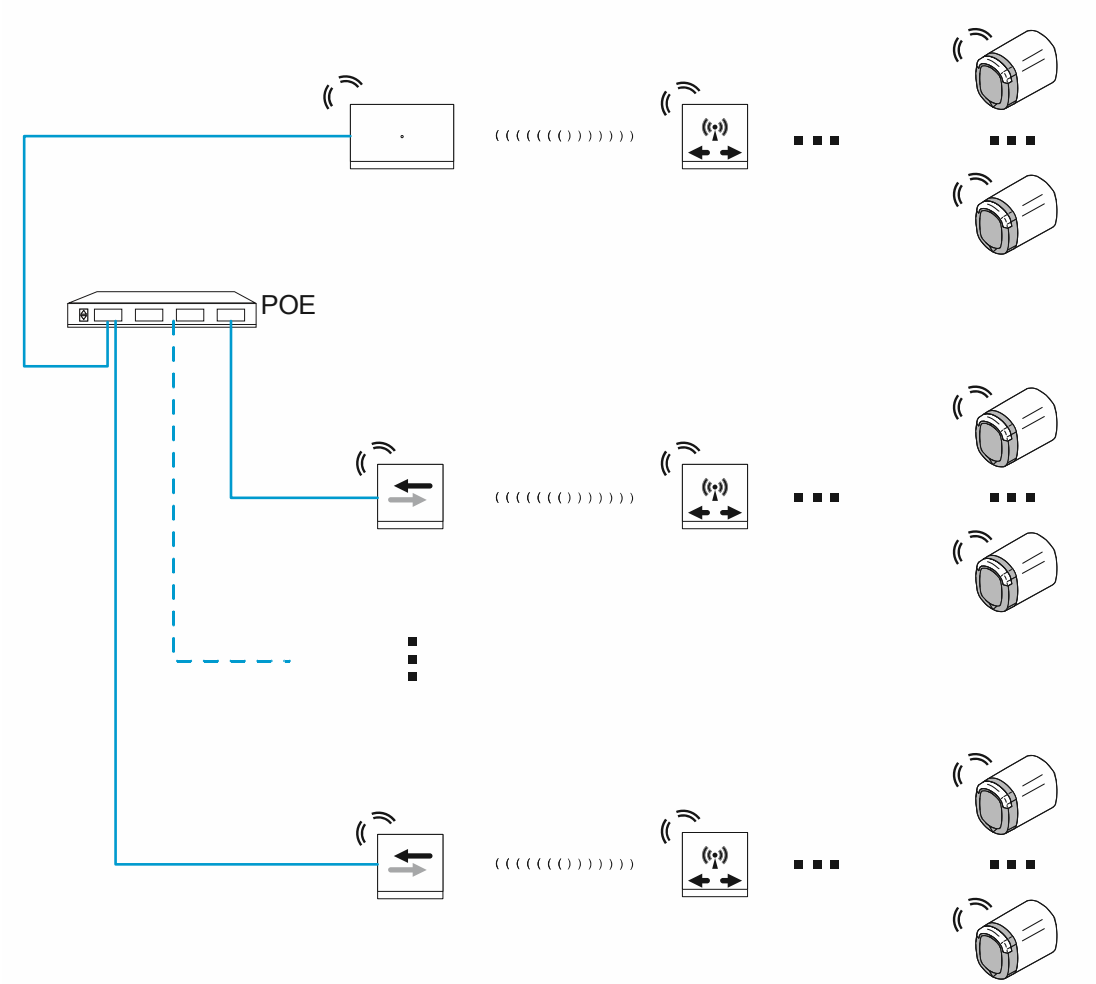


Fig. 53: Total capacity and total transmission range

Up to 64 "RF/IP Gateway" can be activated from a "Smart Access Point Pro". From these up to 16 "Electronic cylindrical lock" can be activated in an independent radio line in addition to the "Smart Access Point Pro". This results in a theoretical total capacity of 1040 „Electronic cylindrical lock“ in one system.Therefore, the total number of all devices in a system ("Electronic cylindrical lock", "RF Repeater". etc.) must not exceed 600.

The maximum transmission range of 40 meters in a single radio line is often insufficient. In this case the more remotely located devices are activated via "RF/IP Gateway" with independent radio lines. The transmission range that can be implemented within a "ABB-AccessControl" system is therefore only limited via th transmission range of the IP network.

– For the details of the transmission range that can be implemented within an IP network see chapter 1.5 “Fundamentals of structured cabling“ on page 9.

Notice

- If thick walls are located within the planned radio line, the attainable transmission ranges are greatly reduced. In this case it would be practical to split the radio line via several "RF/IP Gateway".
- The same applies to connections on other floors where the radio signals must pass through floor ceilings. Here it would be practical to plan a separate "RF/IP Gateway" for every floor.

4.3 Case studies

4.3.1 One-family house

In a "ABB-AccessControl" system the main entrance in a one-family house is equipped with a "Electronic cylindrical lock".

Aside from the "Electronic cylindrical lock" a "Smart Access Point Pro" is necessary for the user management.

– The "ABB-AccessControl" system in this example is not networked with other systems. The use of a PoE switch is not planned, and that is why the "Smart Access Point Pro" a separate 24 V power supply.

The distances are within the radio range of around 10 meters. That is why additional devices to increase the range are not required.

Up to 16 "Electronic cylindrical lock" can be activated via a "Smart Access Point Pro". If the total number of the "Electronic cylindrical lock" is smaller, additional devices to increase the capacity are not required.

Detailed information about the capacity and network planning is available at: see chapter 4.2 “Capacity / Transmission range“ on page 65

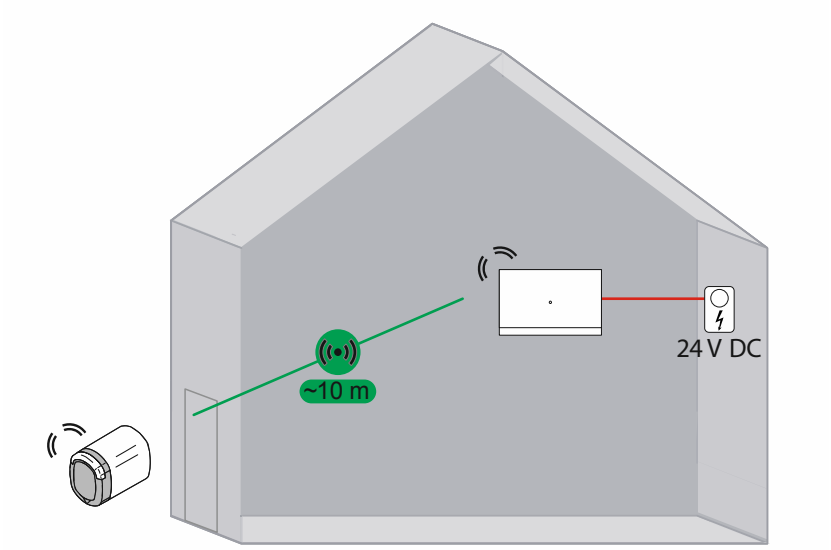


Fig. 54: Overview: One-family house with an "Electronic cylindrical lock"

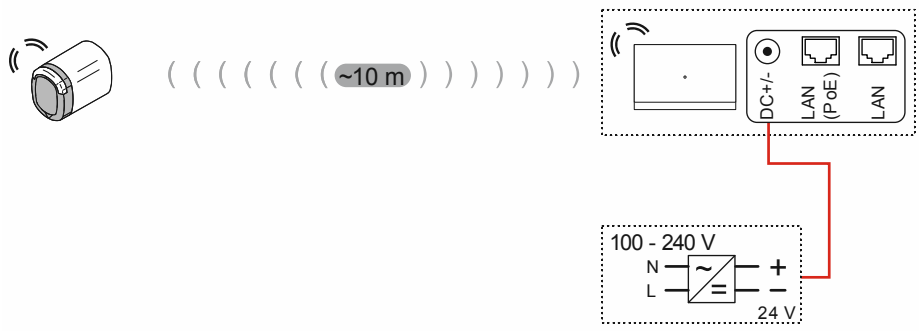


Fig. 55: Connection: One-family house with a "Electronic cylindrical lock"

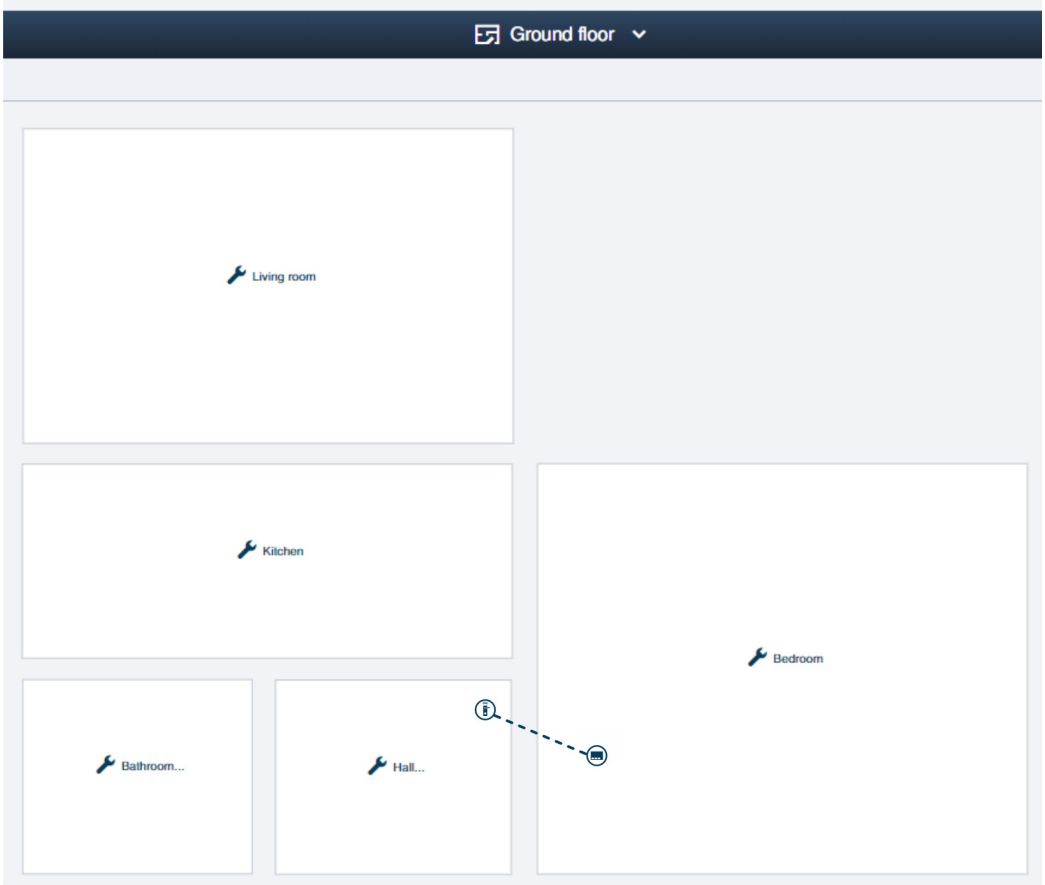


Fig. 56: Building structure: One-family house with a "Electronic cylindrical lock"

Example of the setup of the ground floor of a one-family house in the management software of the "Smart Access Point Pro". The "Electronic cylindrical lock" is connected with the "Smart Access Point Pro".

– Information for the creation of a building structure: see chapter 5.2 “Building structure“ on page 95

4.3.2 Multifamily house with one floor

In a "ABB-AccessControl" system the main entrance and the entrances to the apartments in a multifamily house are equipped with "Electronic cylindrical lock"

Aside from the "Electronic cylindrical lock" a "Smart Access Point Pro" is necessary for the user management.

– The "ABB-AccessControl" system in this example is not networked with other systems. The use of a PoE switch is not planned, and that is why the "Smart Access Point Pro" a separate 24 V power supply.

The distances are within the radio range of around 10 meters. That is why additional devices to increase the range are not required.

Up to 16 "Electronic cylindrical lock" can be activated via a "Smart Access Point Pro". If the total number of the "Electronic cylindrical lock" is smaller, additional devices to increase the capacity are not required.

Detailed information about the capacity and network planning is available at: see chapter 4.2 “Capacity / Transmission range“ on page 65

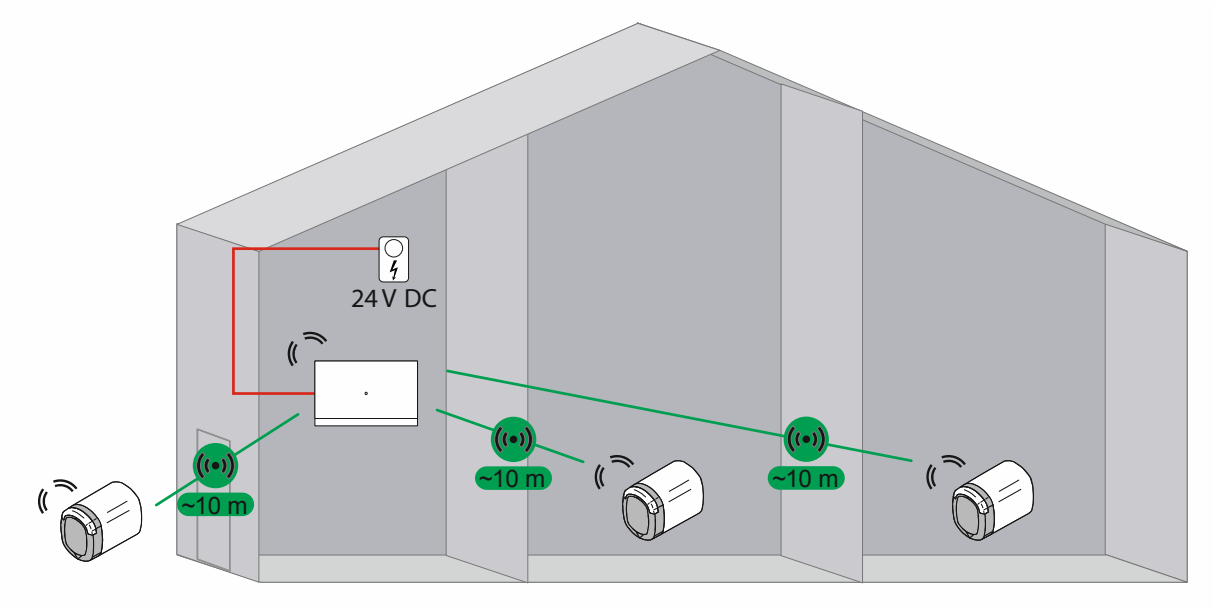


Fig. 57: Overview: Multifamily house with 3 "Electronic cylindrical lock"

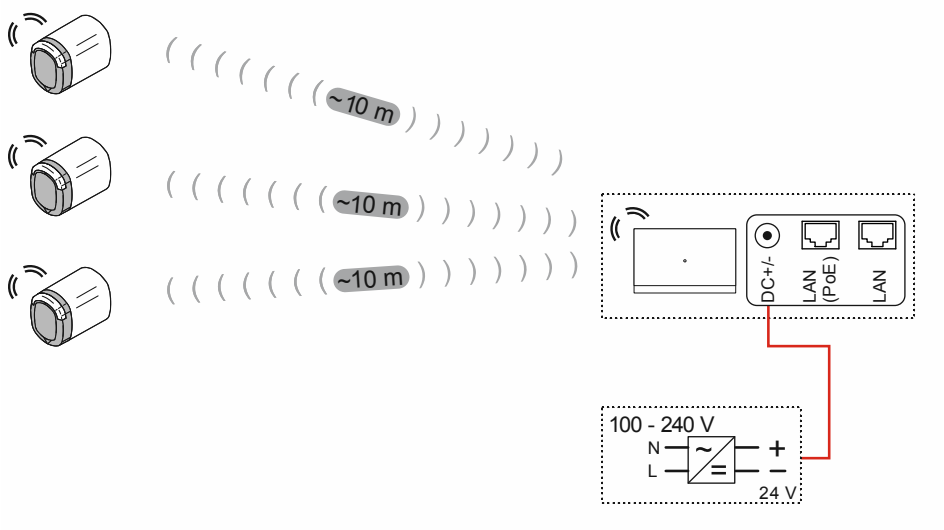


Fig. 58: Connection: Multifamily house with 3 "Electronic cylindrical lock"

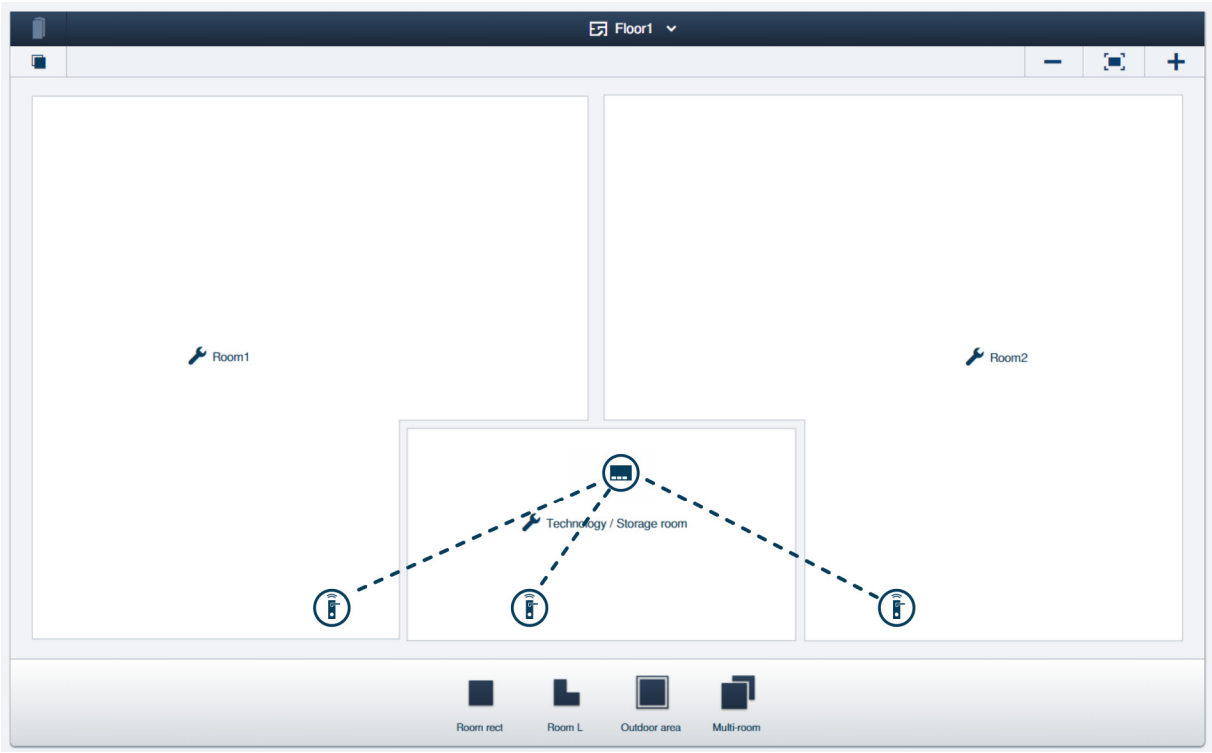


Fig. 59: Building structure: Multifamily house with 3 "Electronic cylindrical lock"

Example of a setup of a floor with 2 apartments in the management software of the "Smart Access Point Pro". The "Electronic cylindrical lock" are connected with the "Smart Access Point Pro".

– Information for the creation of a building structure: see chapter 5.2 “Building structure“ on page 95

4.3.3 Multifamily house with several floors

In a "ABB-AccessControl" system the main entrance and the entrances to the apartments in a multifamily house are equipped with "Electronic cylindrical lock"

Aside from the "Electronic cylindrical lock" a "Smart Access Point Pro" is necessary for the user management.

The ceiling of the floor greatly reduces the transmission range of the radio signals. That is why the additional use of an "RF/IP Gateway" is required for the distribution of data for each additional floor.

– The "ABB-AccessControl" system in this example is not networked with other systems. A PoE switch is required for the use of an "RF/IP Gateway". The power for the "Smart Access Point Pro" and the "RF/IP Gateway" is supplied via the PoE switch.

The distances within a floor are within the radio range of around 10 meters. That is why additional devices to increase the range are not required within the floors.

Detailed information about the capacity and network planning is available at: see chapter 4.2 “Capacity / Transmission range“ on page 65

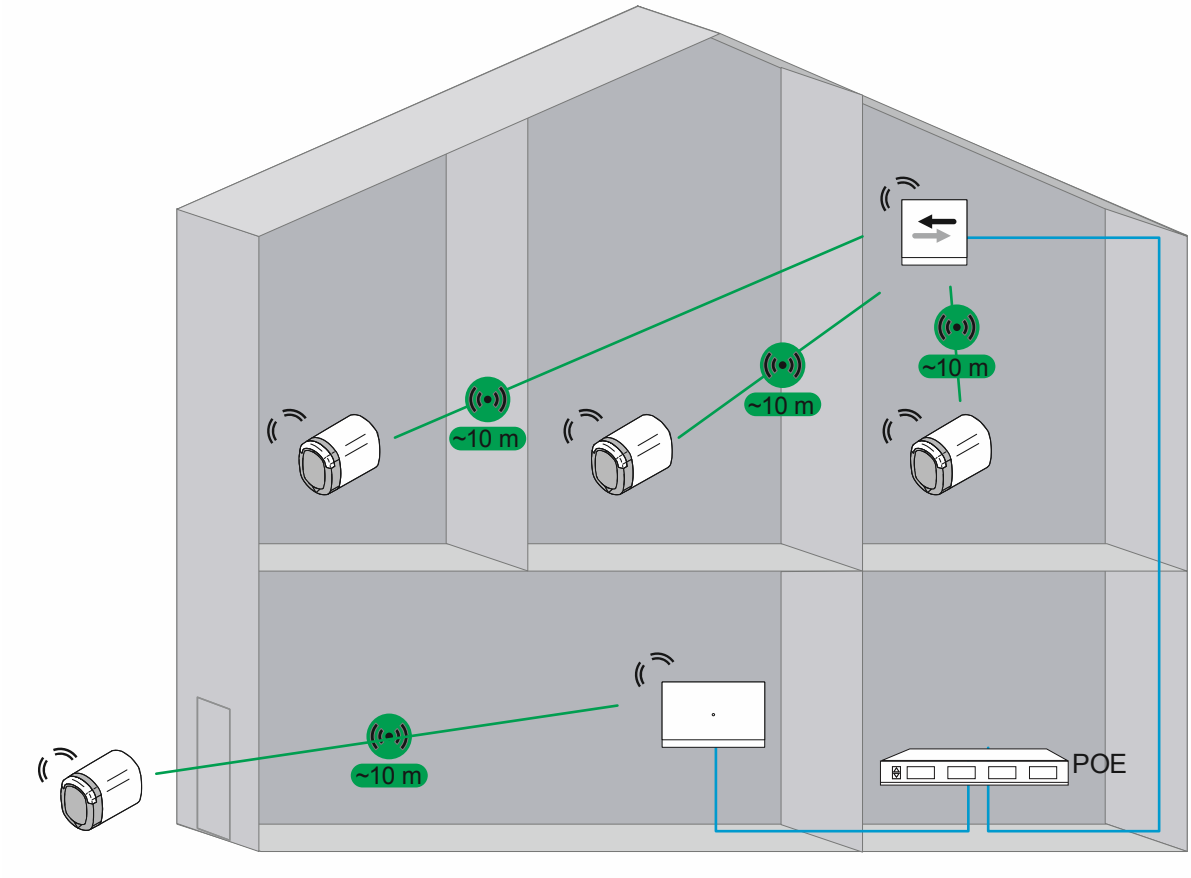


Fig. 60: Overview: Multifamily house with 4 "Electronic cylindrical lock"

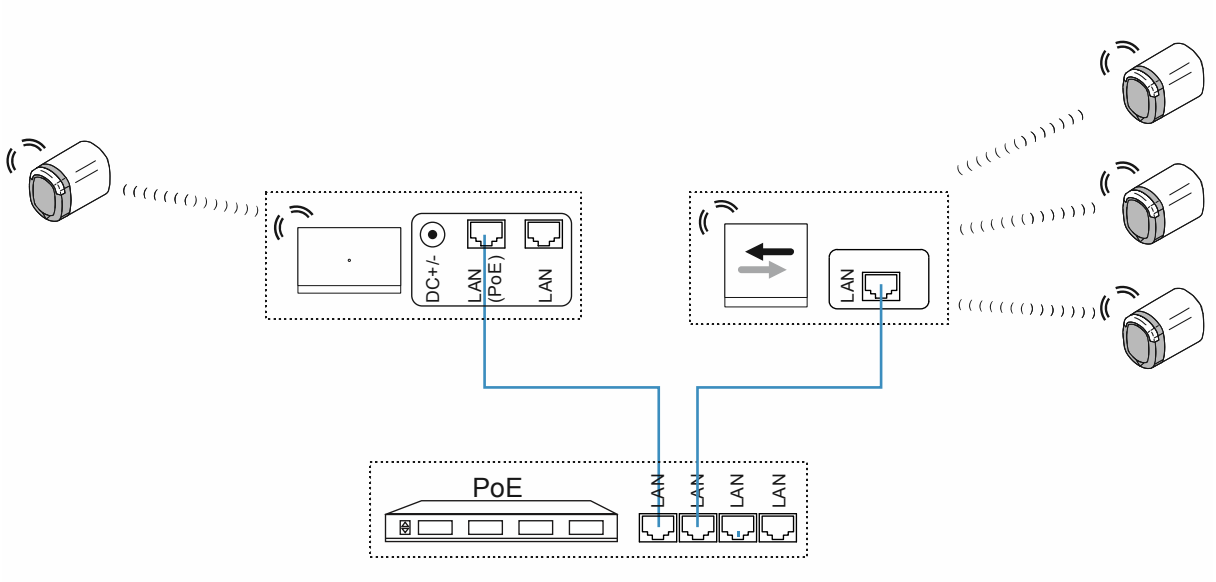


Fig. 61: Connection: Multifamily house with 4 "Electronic cylindrical lock"

Fig. 62: Building structure: Multifamily house with 4 "Electronic cylindrical lock"

Example of a setup of the apartments of a multifamily house in the management software of the "Smart Access Point Pro".

– Information for the creation of a building structure: see chapter 5.2 “Building structure“ on page 95

Floor 1:

The "Electronic cylindrical lock" is connected with the "Smart Access Point Pro".

Floor 2:

The "Electronic cylindrical lock" are connected with the "RF/IP Gateway".

4.3.4 Multifamily house with a medical practice

In a "ABB-AccessControl" system the main entrance and the entrances to the apartments in a multifamily house are equipped with "Electronic cylindrical lock"

The building contains a medical practice. The archive in the basement should also be equipped with an "Electronic cylindrical lock" for the medical practice. There is no radio connection to this room.

Aside from the "Electronic cylindrical lock" a "Smart Access Point Pro" is necessary for the user management.

The ceiling of the floor greatly reduces the transmission range of the radio signals. That is why the additional use of an "RF/IP Gateway" is required for the distribution of data for each additional floor.

– In this example the "Smart Access Point Pro" is already available (e.g. in a "ABB-Welcome IP"). That is why it is also being used. The power for the "Smart Access Point Pro" and the "RF/IP Gateway" is supplied via the PoE switch.

Upper building:

The distances within a floor are within the radio range of around 10 meters. That is why additional devices to increase the range are not required within the floors.

Detailed information about the capacity and network planning is available at: see chapter 4.2 “Capacity / Transmission range“ on page 65

Basement with archive:

The installation of an increase of the transmission range into the basement is not available.

Since there is no radio connection between the "Electronic cylindrical lock" and the "Smart Access Point Pro", the emergency function must in this case be set up in the user management for the necessary "Electronic cylindrical lock" and the associated transponder key. The emergency function allows the archive then to be opened and closed without a radio connection to the "Smart Access Point Pro".

– To set up the emergency function an initial radio connection of the "Electronic cylindrical lock" to the "Smart Access Point Pro" is required. E.g. by dismantling the reading head from the "Electronic cylindrical lock". To set up the emergency function the reading head is then positioned in close proximity of the "Smart Access Point Pro".
– To set up the emergency function in the management software of the "Smart Access Point Pro" see chapter 5.3.3 “"Electronic cylindrical lock" Settings – Emergency function“ on page 107

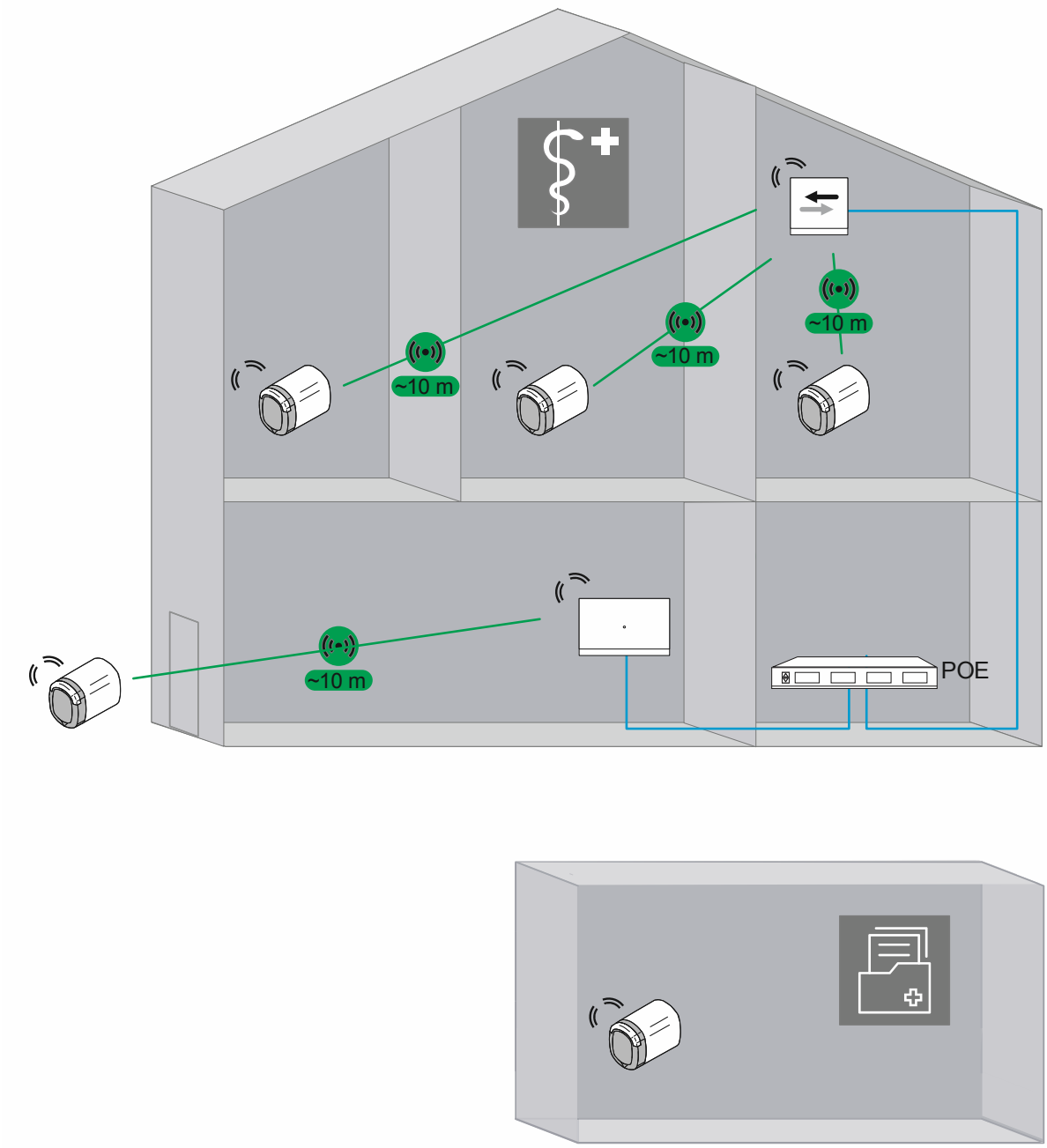


Fig. 63: Overview: Multifamily house with medical practice and archive

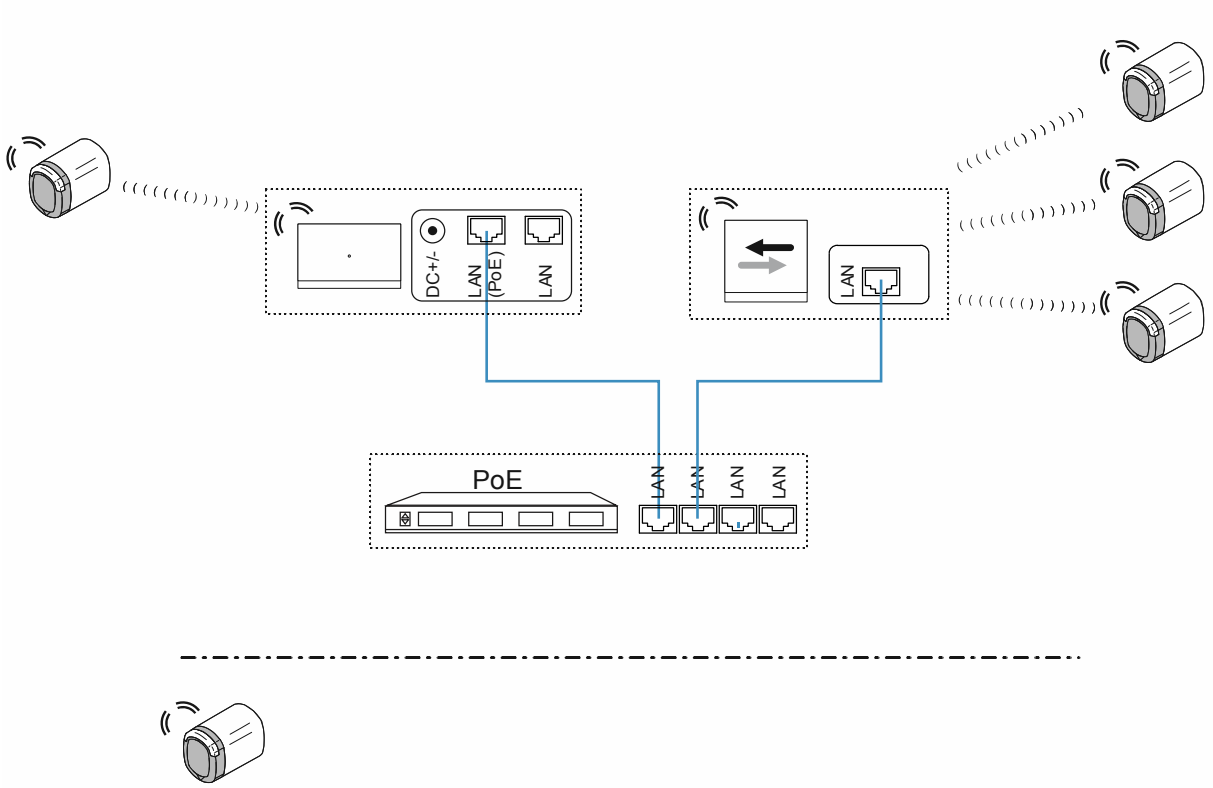


Fig. 64: Connection: Multifamily house with medical practice and archive

Fig. 65: Building structure: Multifamily house with 4 "Electronic cylindrical lock"

Example of a setup of the apartments of a multifamily house in the management software of the "Smart Access Point Pro".

– Information for the creation of a building structure: see chapter 5.2 “Building structure“ on page 95

Floor :1

The "Electronic cylindrical lock" are connected with the "Smart Access Point Pro".

– The "Electronic cylindrical lock" for the archive is marked as device with missing connection as soon as it is outside the transmission range of the "Smart Access Point Pro" for its use.

Floor :2

The "Electronic cylindrical lock" are connected with the "RF/IP Gateway".

4.3.5 Residential building with a longer floor

In a "ABB-AccessControl" system the main entrance and the entrances to the apartments in a single-floor residential building are equipped with "Electronic cylindrical lock"

Aside from the "Electronic cylindrical lock" a "Smart Access Point Pro" is necessary for the user management.

Fire walls greatly reduce the transmission range of the radio signals. That is why the additional use of an "RF/IP Gateway" is required for the distribution of data for each area between the fire walls.

– The "ABB-AccessControl" system in this example is not networked with other systems. A PoE switch is required for the use of an "RF/IP Gateway". The power for the "Smart Access Point Pro" and the "RF/IP Gateway" is supplied via the PoE switch.

The distances within an area are within the radio range of around 10 meters. That is why additional devices to increase the range are not required within these areas.

Detailed information about the capacity and network planning is available at: see chapter 4.2 “Capacity / Transmission range“ on page 65

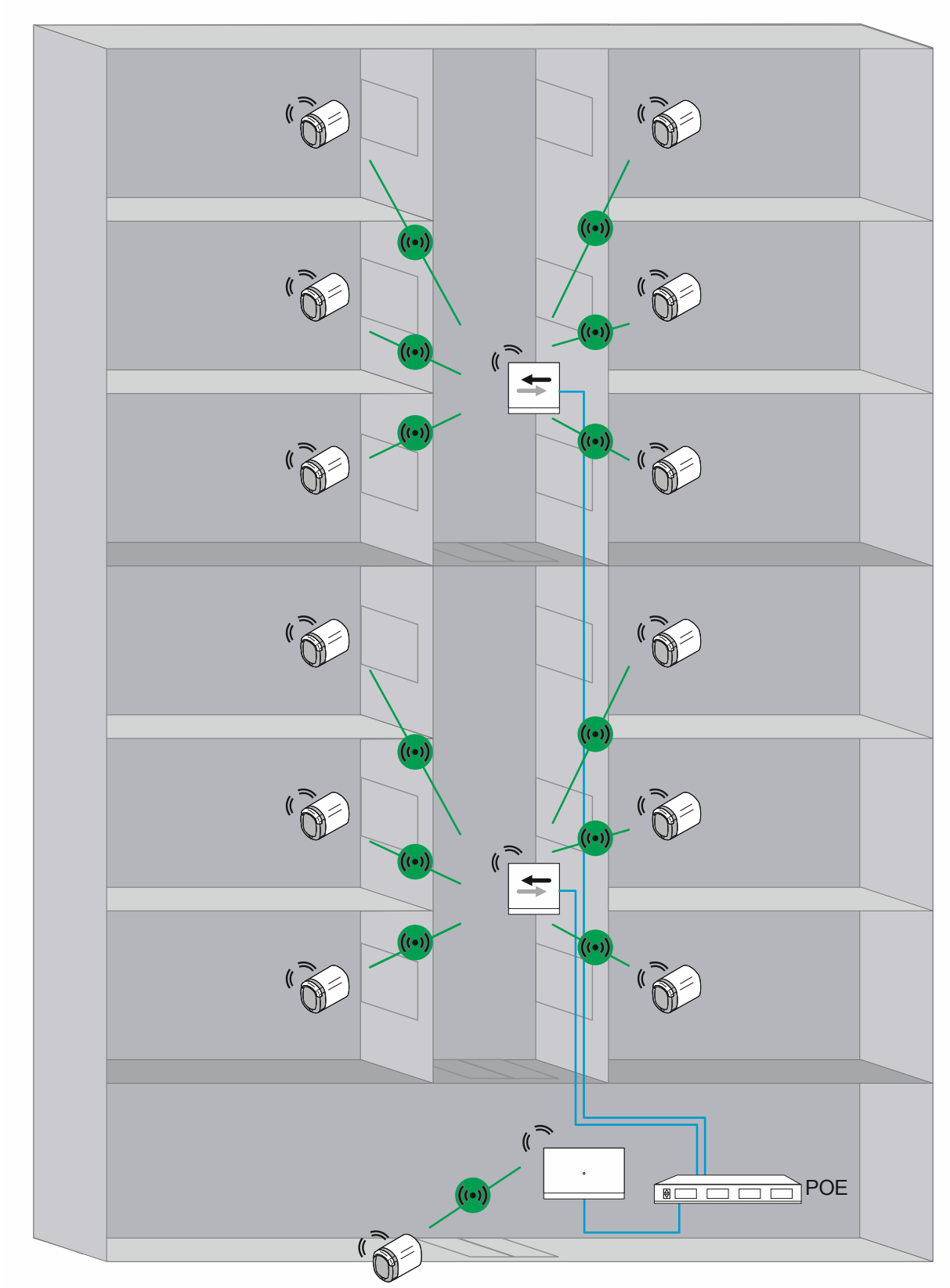


Fig. 66: Overview (top view): Residential building with more than 10 meters transmission route and radio signal inhibition through fire walls

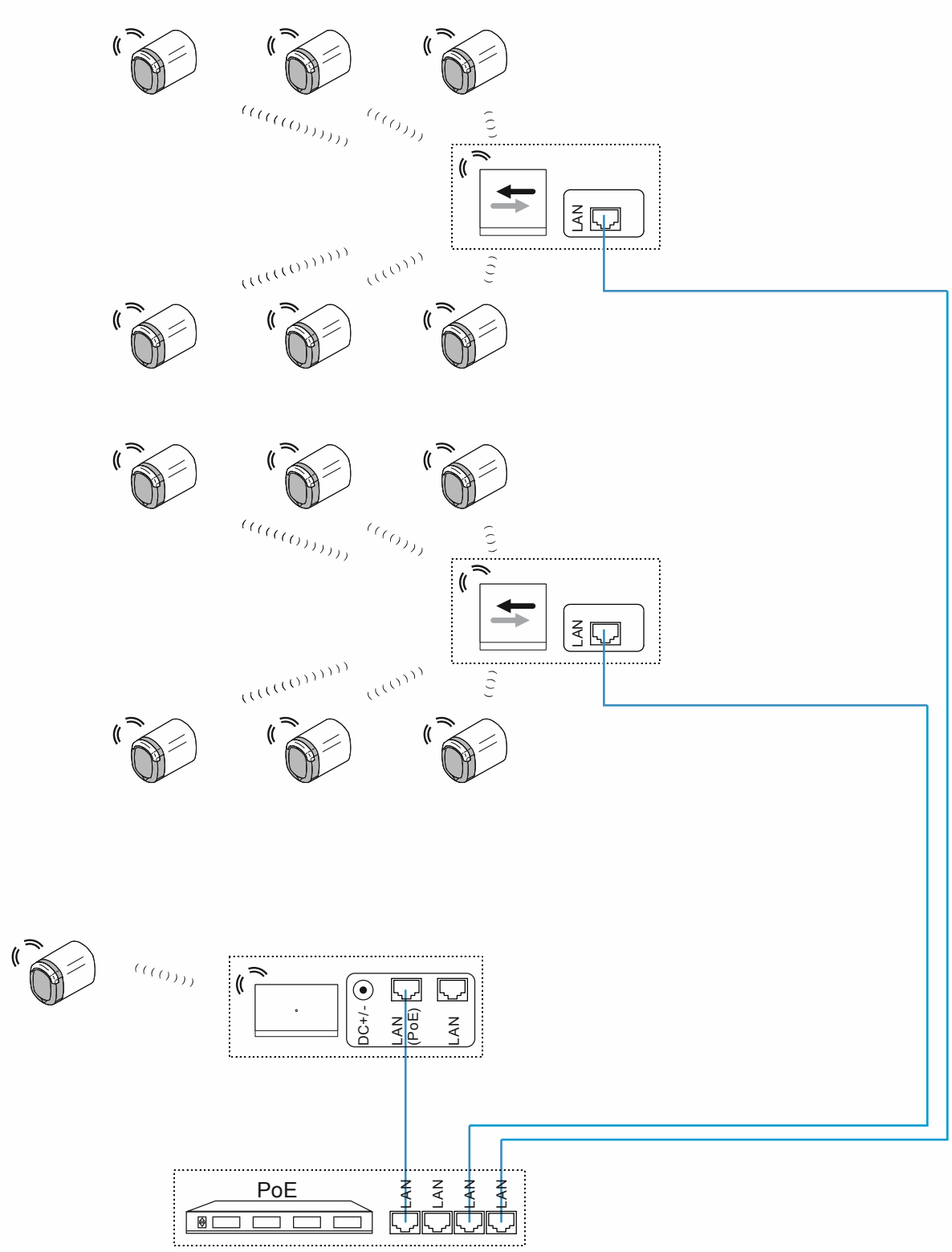


Fig. 67: Connection: Residential building with more than 10 meters transmission route and radio signal inhibition through fire walls

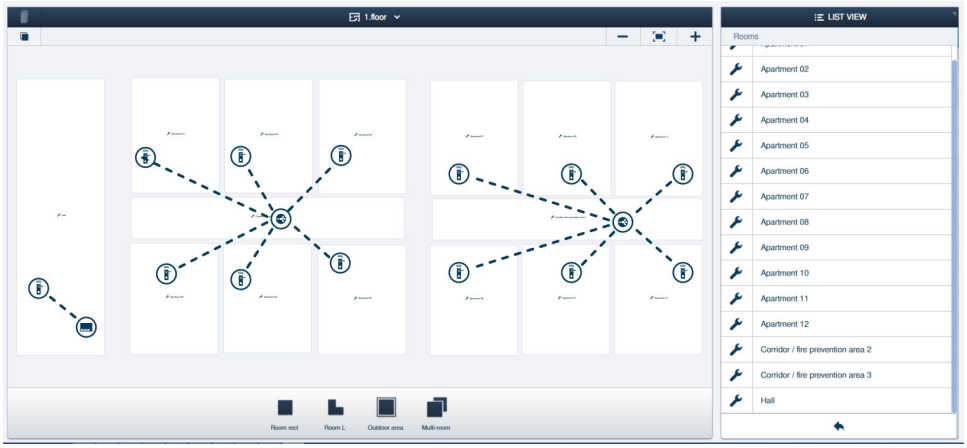


Fig. 68: Building structure: Residential building with more than 10 meters transmission route and radio signal inhibition through fire walls

Example of a setup of the apartments of a multifamily house in the management software of the "Smart Access Point Pro".

– Information for the creation of a building structure: see chapter 5.2 “Building structure“ on page 95

Main entrance:

The "Electronic cylindrical lock" is connected with the "Smart Access Point Pro".

Fire protection areas:

The "Electronic cylindrical lock" are connected with the "RF/IP Gateway".

4.3.6 Residential buildings with several floors

In a "ABB-AccessControl" system the main entrance and the entrances to the apartments in a multi-floor residential building are equipped with "Electronic cylindrical lock"

Aside from the "Electronic cylindrical lock" a "Smart Access Point Pro" is necessary for the user management.

The ceiling of the floor greatly reduces the transmission range of the radio signals. That is why the additional use of an "RF/IP Gateway" is required for the distribution of data for each additional floor.

– The "ABB-AccessControl" system in this example is not networked with other systems. A PoE switch is required for the use of an "RF/IP Gateway". The power for the "Smart Access Point Pro" and the "RF/IP Gateway" is supplied via the PoE switch.

The distances within a floor are above the radio range of around 10 meters. Therefore, "RF Repeater" are used to increase the transmission range.

– The "RF Repeater" are not PoE-capable. They require a separate 24 V power supply.

Detailed information about the capacity and network planning is available at: see chapter 4.2 “Capacity / Transmission range“ on page 65

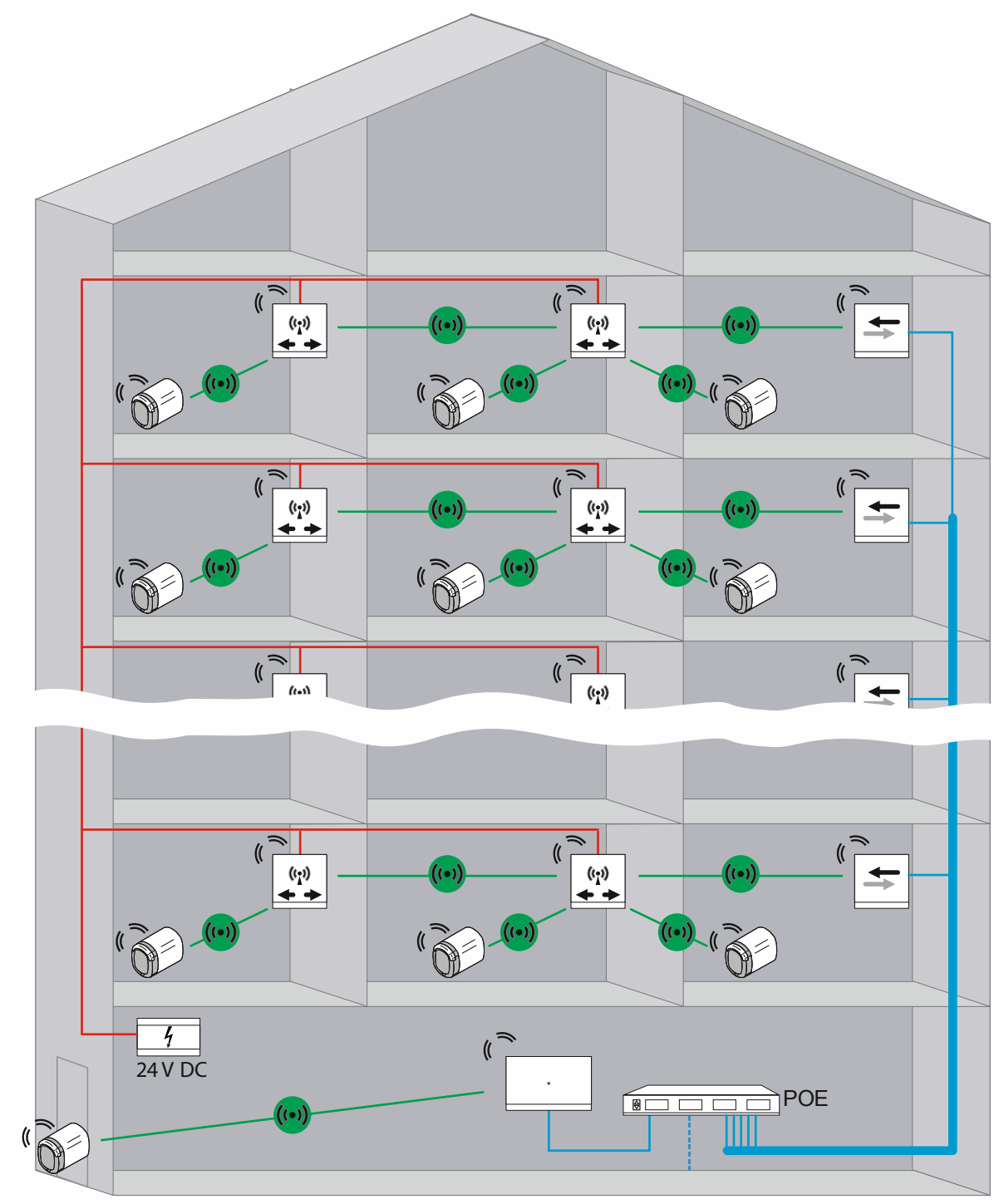


Fig. 69: Overview: Multi-floor residential building with more than 10 meters transmission route

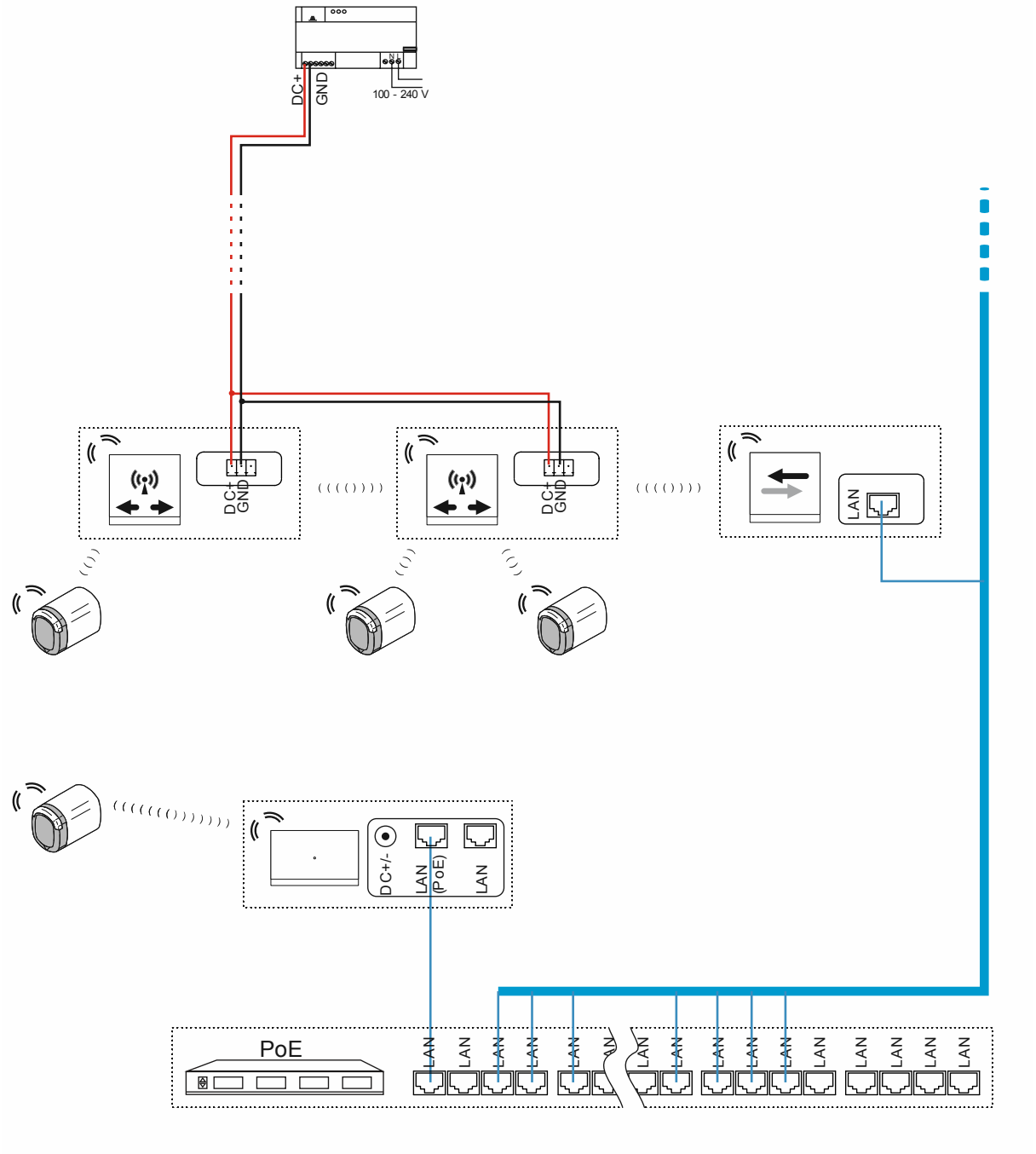


Fig. 70: Connection: Multi-floor residential building with more than 10 meters transmission route

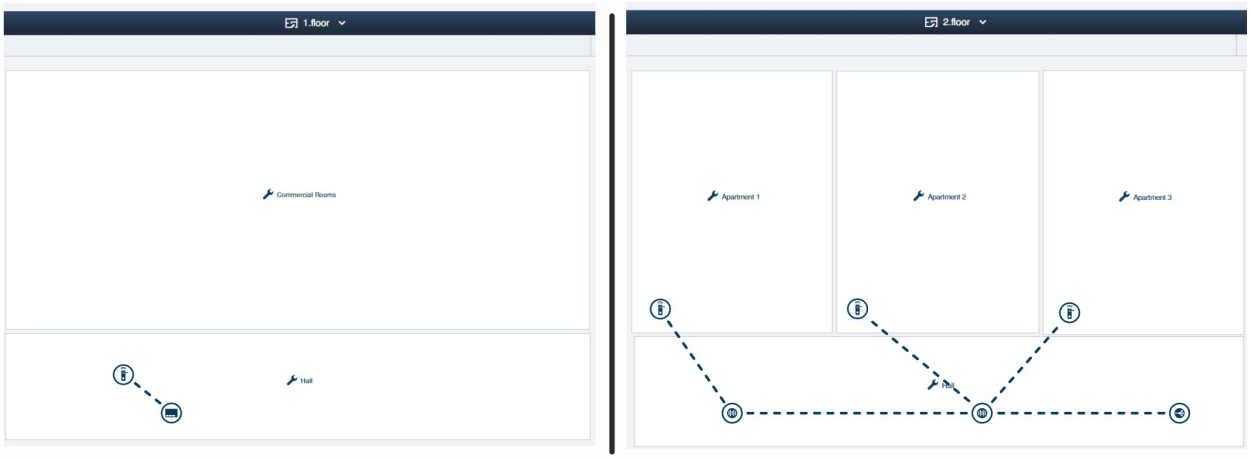


Fig. 71: Building structure: Multi-floor residential building with more than 10 meters transmission route

Example of a setup of the apartments of a multi-floor multifamily house with a transmission route of more than 10 meters within a floor in the management software of the "Smart Access Point Pro".

– Information for the creation of a building structure: see chapter 5.2 “Building structure“ on page 95

Floor :1

The "Electronic cylindrical lock" is connected with the "Smart Access Point Pro".

Floor 2 and additional floors:

The "Electronic cylindrical lock" are connected with the "RF/IP Gateway" via "RF Repeater".

4.3.7 Perimeter

An installation with a perimeter is illustrated in the following example. The perimeter comprises two houses and associated parking garage.

In a "ABB-AccessControl" system the residential buildings and parking garages are equipped with "Electronic cylindrical lock".

Next to the "Electronic cylindrical lock" a "Smart Access Point Pro" is necessary for the user management.

The distribution of signals in the additional buildings and the respective floors is taken over by "RF/IP Gateway".

A LAN network is required for the connection between the different buildings. The power for the devices used in this example is therefore supplied via PoE.

– In this example there are no further IP devices in operation in the parking garage. The "RF/IP Gateway" can therefore be operated without a separate PoE switch.

Detailed information about the capacity and network planning is available at: Chapter 4.2 “Capacity / Transmission range“ on page 65

Notice

It is absolutely essential that the houses are always connected with glass fibre cables.

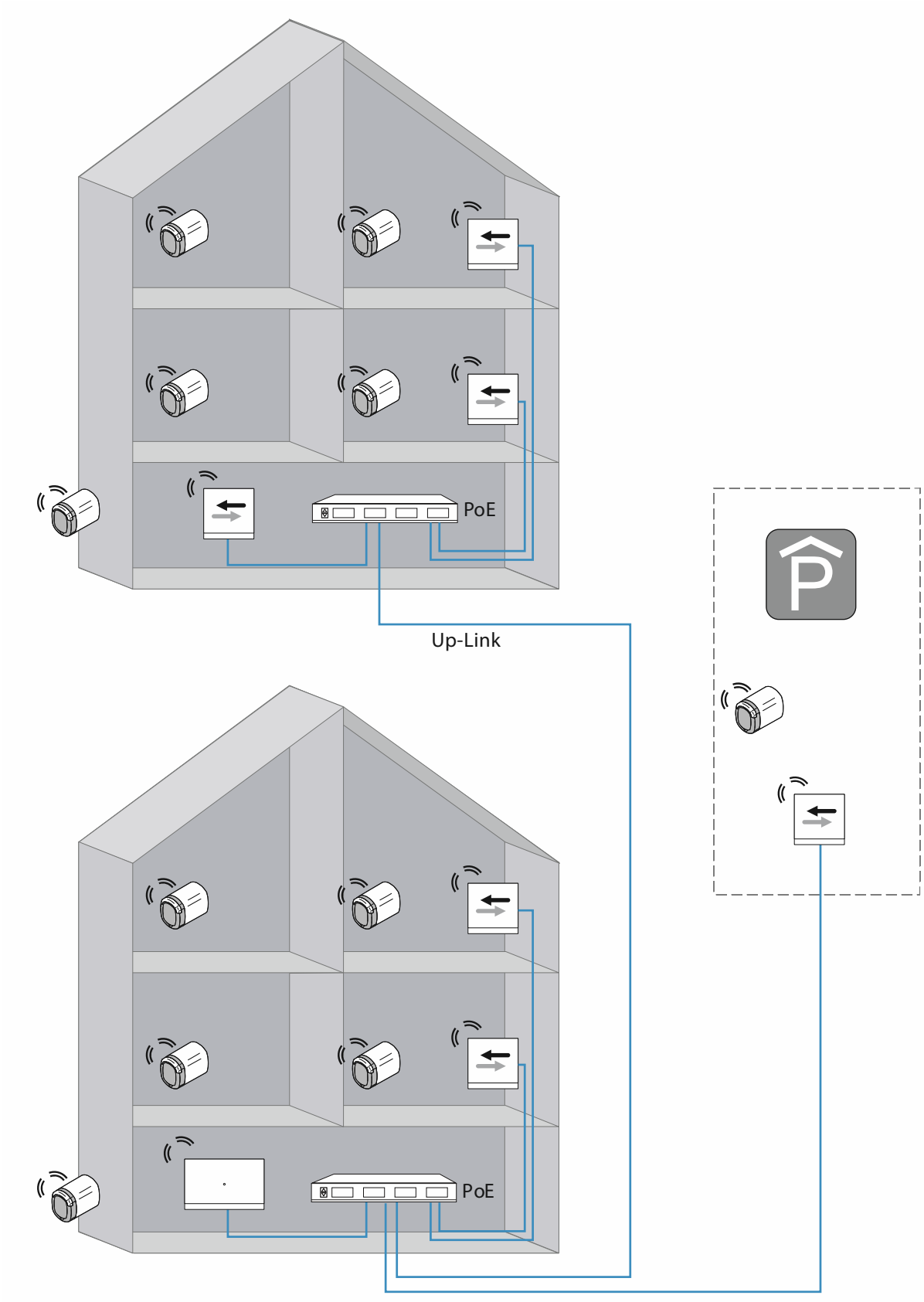


Fig. 72: Overview: Perimeter with more than 40 meters transmission route and less than 16 "Electronic cylindrical lock".

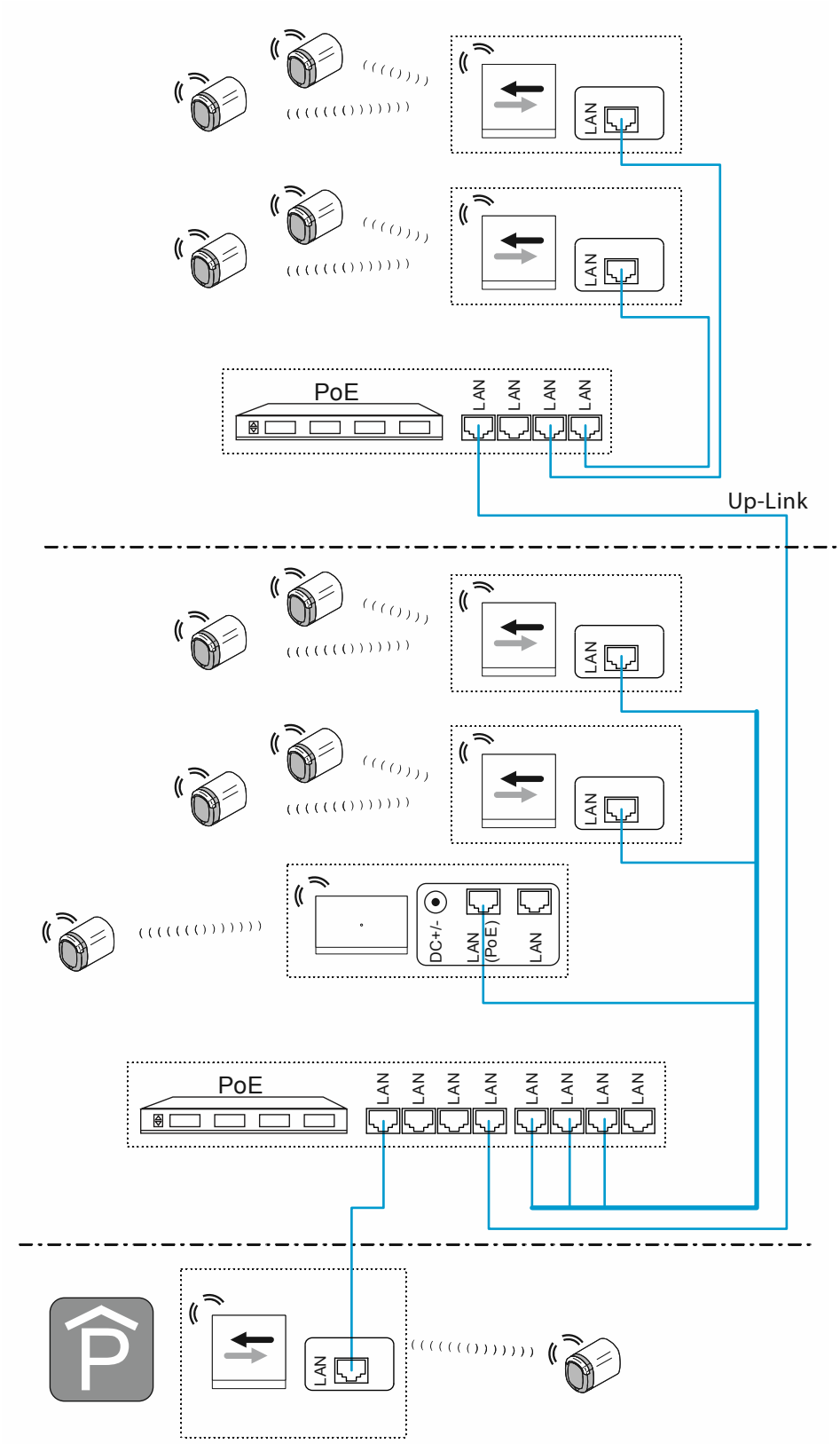


Fig. 73: Connection: Perimeter with more than 40 meters transmission route and less than 16 "Electronic cylindrical lock".

UP-link connection for the cascading (series switching) of switches:

– When the switch has an up-link connection:

  Connect the up-link connection with a normal LAN cable with a LAN connection of the next switch.

– When the switch has no up-link connection:

  Connect a LAN connection with a crossover cable with a LAN connection of the next switch.

Attention!

Malfunctions

– For building-interlinking cabling, observe the specifications of the structured cabling (glass fibre line), see chapter 1.5 “Fundamentals of structured cabling“ on page 9.

Fig. 74: Building structure: Perimeter with more than 40 meters transmission route and less than 16 "Electronic cylindrical lock".

Example of a system setup with several buildings including parking garage in the management software of the "Smart Access Point Pro".

– Information for the creation of a building structure: see chapter 5.2 “Building structure“ on page 95

Building 1 Floor 1:

The "Electronic cylindrical lock" is connected with the "RF/IP Gateway".

Building 1 Floor 2:

The "Electronic cylindrical lock" are connected with the "RF/IP Gateway".

Building 2 Floor 1:

The "Electronic cylindrical lock" is connected with the "Smart Access Point Pro".

Building 2 Floor 2:

The "Electronic cylindrical lock" are connected with the "RF/IP Gateway".

Parking garage:

The "Electronic cylindrical lock" is connected with the "RF/IP Gateway".

4.4 Sources of interference

Errors between transponder key and reading head

The connection between the reading head of the "Electronic cylindrical lock" and the transponder key is triggered via RFID technology by induction.

If during the switching process of the reading head the transponder key is located next to other transponder keys or RFID cards, this can cause mutual influences.

– E.g. when the transponder key is kept in the purse with other RFID cards and the purse is held in front of the reading head.

Such influences do not cause damage. However, it is possible that then the reading head does not switch.

Errors of communication of the reading head with the management software of the "Smart Access Point Pro"

The communication between the reading head and the management software of the "Smart Access Point Pro" is carried out via the frequencies of Bluetooth.

- Errors during installation:
  – The normal transmission range of 10 meters between the individual devices of the "ABB-AccessControl" is influenced by the building structure. If the radio signals must pass through a reinforced concrete wall, the transmission range can be reduced.
- Errors during running operation:
  – The devices of the "ABB-AccessControl" are permanently installed. This causes no problems due to changes of location.
  – Errors can be caused when foreign devices near the communication process send on the same frequencies. E.g. wireless telephones or microwaves. The reading head may then not switch. If the source of the error in the area is rectified, everything will function again as usual.

Newly installed "Electronic cylindrical lock" cannot be operated

- The "Electronic cylindrical lock" is being operated in a location different to the area of application stored in the management software. That is why the communication path no longer harmonizes with the original one. The "Electronic cylindrical lock" must be coupled anew, see chapter 5.4.4 “Coupling the "Electronic cylindrical lock" with the "Smart Access Point Pro"“ on page 122.
- The "Electronic cylindrical lock" was put into operation on a different "Smart Access Point Pro".
  – The "Electronic cylindrical lock" must be uncoupled on the original "Smart Access Point Pro" and then put into operation on the current "Smart Access Point Pro".

5 Management software in the "Smart Access Point Pro"

5.1 Overview

For the setup and management of the "ABB-AccessControl" access system the following areas are significant in the management software of the "Smart Access Point Pro".

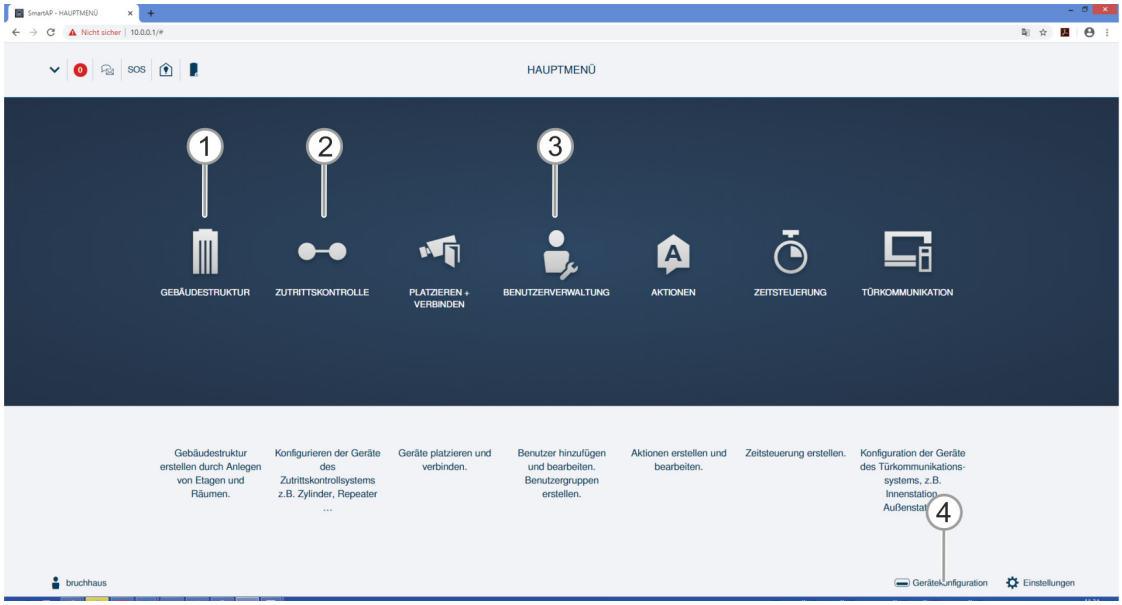


Fig. 75: Main menu "Overview"

1 Building structure
   - A building structure that has been set up is a prerequisite for the placement and coupling of devices of the "ABB-AccessControl" system.
   - For the functions in the "Building structure" area, see chapter 5.2 “Building structure“ on page 95.

2 Access control
   - The devices of the "ABB-AccessControl" are placed and coupled with each other in the "Access control" area.
   - For the functions in the "Access control" area, see chapter 5.4 “Access control“ on page 113.

3 User management
   - The locking rights of persons are assigned and managed in the "User management" area".
   - For the functions in the "User management" area, see chapter 5.5 “User management“ on page 131.

4 Device configuration
   - In the "Device configuration" area the devices of the "ABB-AccessControl" system are added in the management software of the "Smart Access Point Pro".
   - After being added, the devices of the "ABB-AccessControl" system are placed and coupled in the respective other areas in the building structure and then the locking rights are assigned.
   - For the functions in the "Device configuration" area, see chapter 5.3 “Device configuration“ on page 103.

5.2 Building structure

The buildings, floors and rooms are created via menu item "Building structure" in the main menu of the "Smart Access Point Pro".

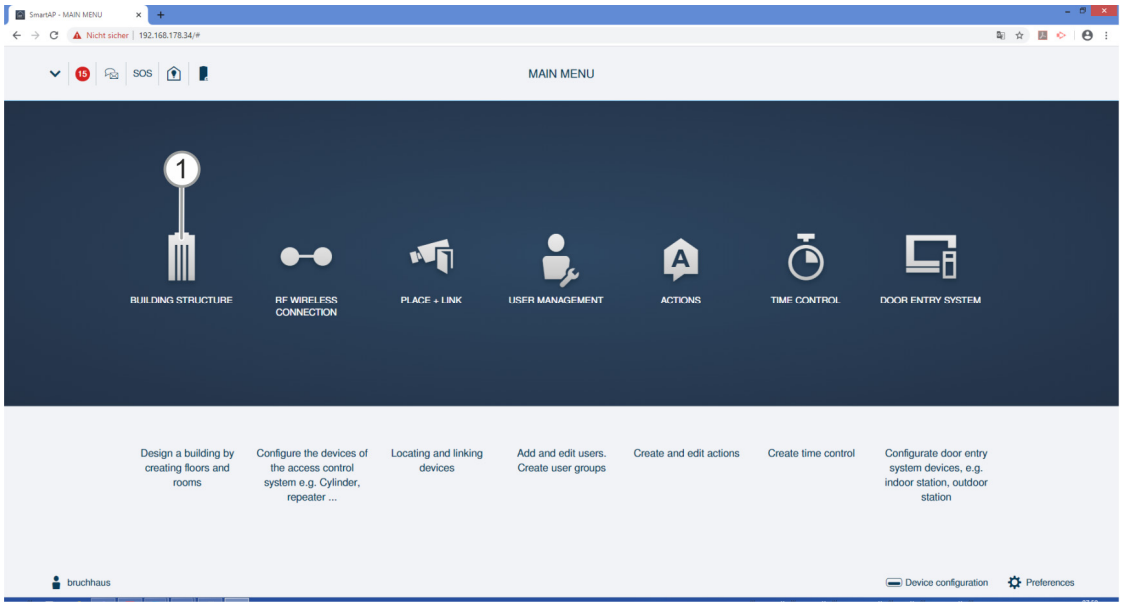


Fig. 76: "Building structure" menu

The following settings are made in menu item "Building structure":

- Add buildings
- Add floors
- Add rooms

5.2.1 Creating buildings

To create the building, perform the following steps:

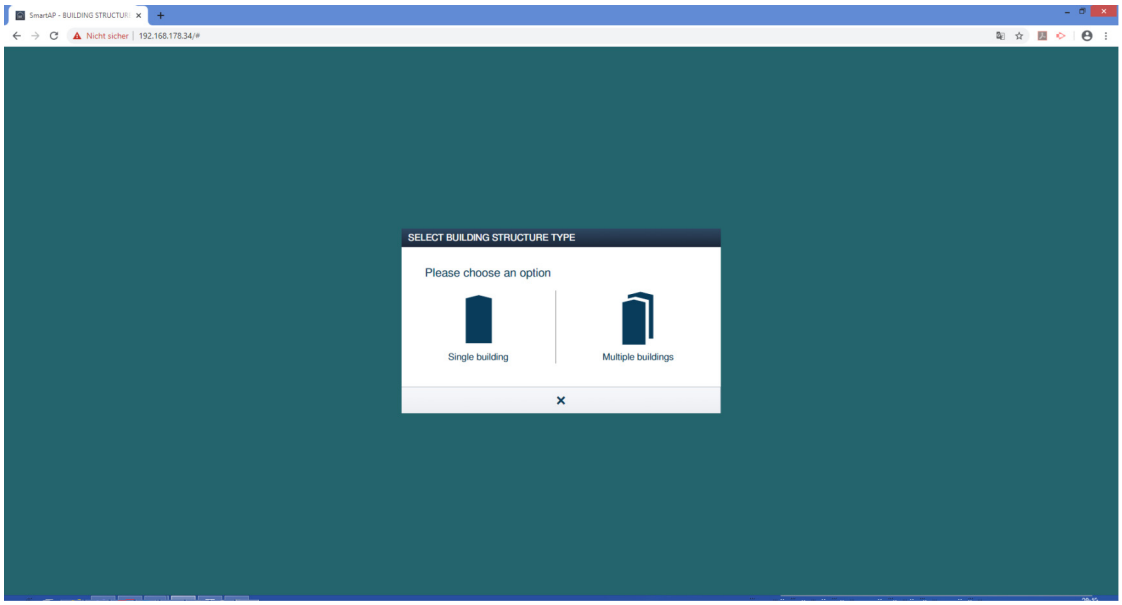


Fig. 77: Selecting the building structure type

1. In the "Building structure type" window select whether it is a "Single building" or "Several buildings".

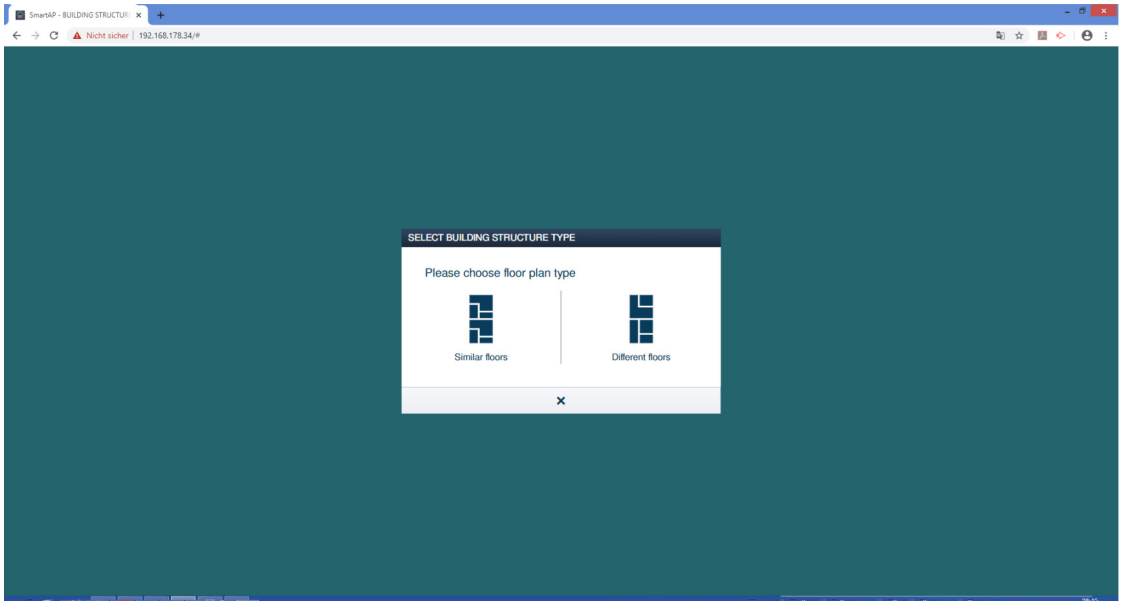


Fig. 78: Selecting the floor plan type

2. In the "Floor plan type" select whether the floors exhibit a similar or different floor plan.

Fig. 79: Selecting the building form

3. Select the suitable building form in the list [1] and pull it onto the working area [2].

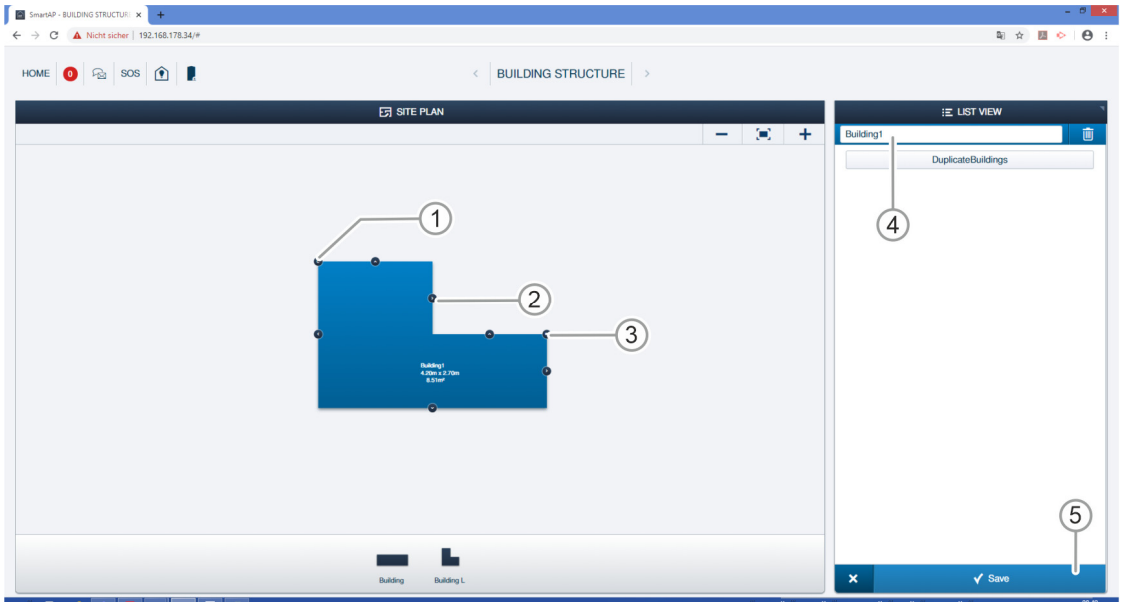


Fig. 80: Adjusting the building form

4. Click on the building.
   - The building gets a blue background. Buttons appear at the edge of the building with which the form and size of the building can be adjusted.
     - The building is turned with button [1].
     - The position of the individual edges is changed with button [2].
     - The size of the building is enlarged or reduced with button [3].
5. Enter the name of the building in field [4].
6. Click on the "Save" button [5].

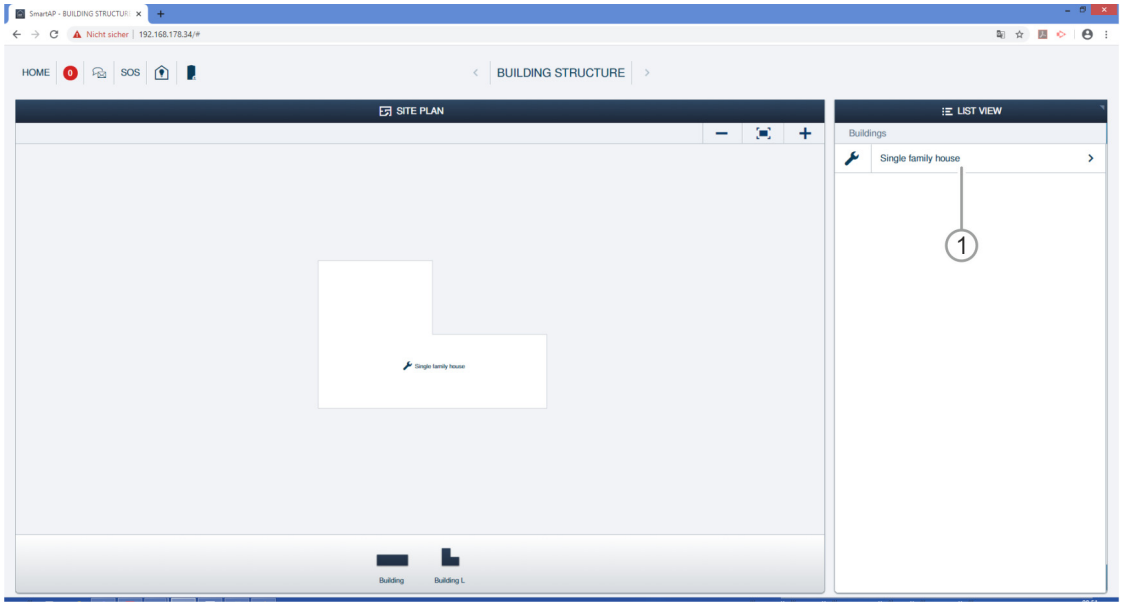


Fig. 81: Selecting a building for further editing.

– Click on the building name in the list [1] to select the building for further editing.

5.2.2 Creating floors

To create the floors, perform the following steps:

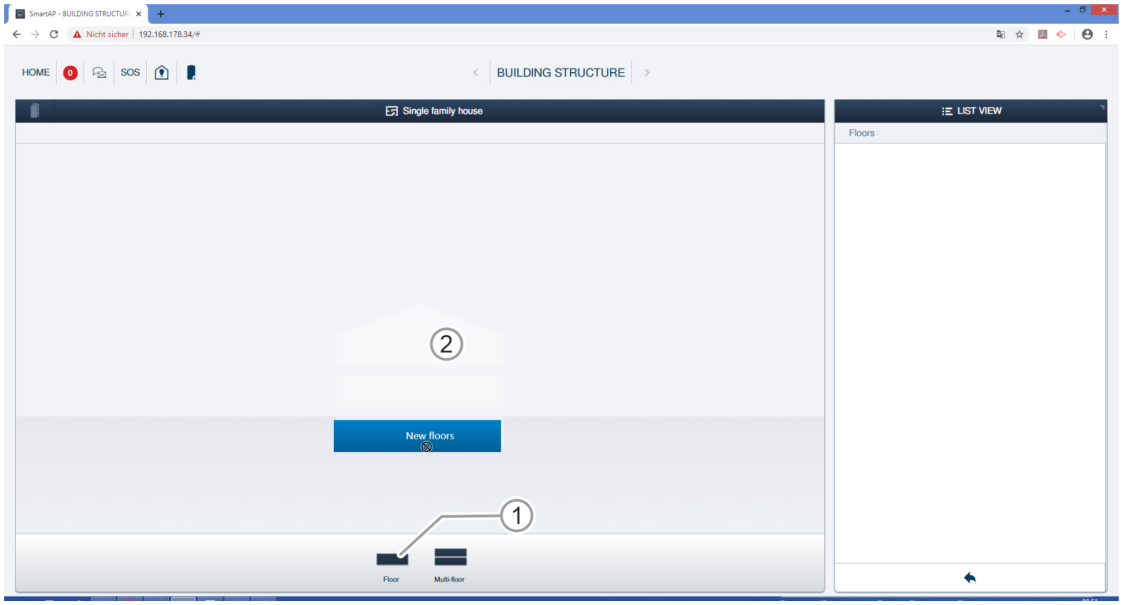


Fig. 82: Selecting the floor version

1. Select the floor versions from the list [1] and pull it onto the building [2].

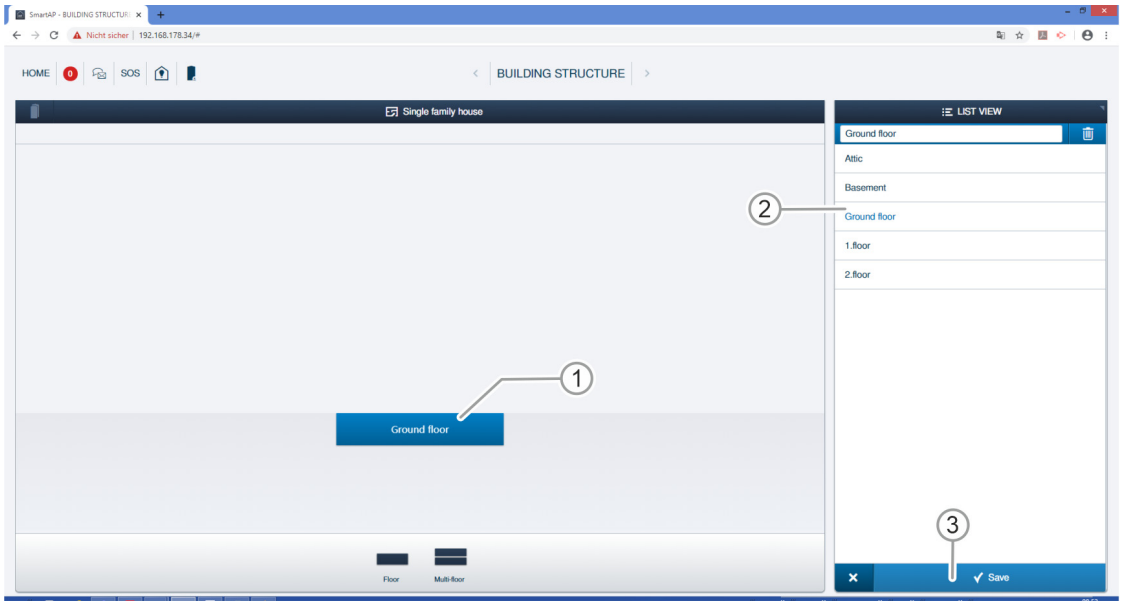


Fig. 83: Floor characteristics

2. Click on the floor [1].
3. Select the floor type from the list [2] and click on the "Save" [3] button.
4. Add additional floors if required.

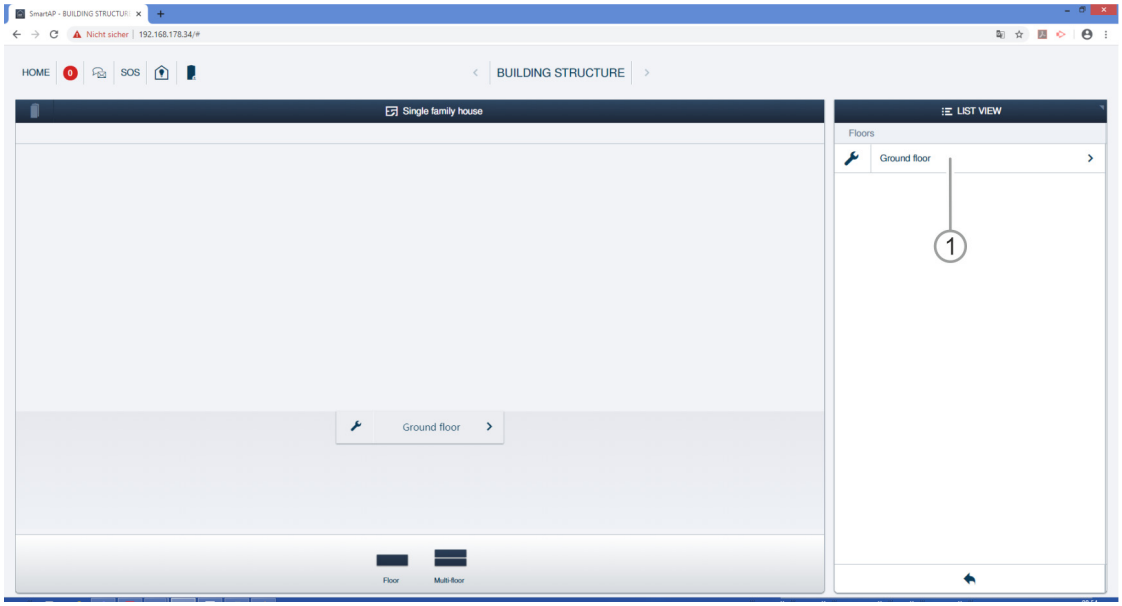


Fig. 84: Selecting a floor for further editing.

5. Click on a floor in the list [1] to select it for further editing.

5.2.3 Creating rooms

To create the rooms, perform the following steps:

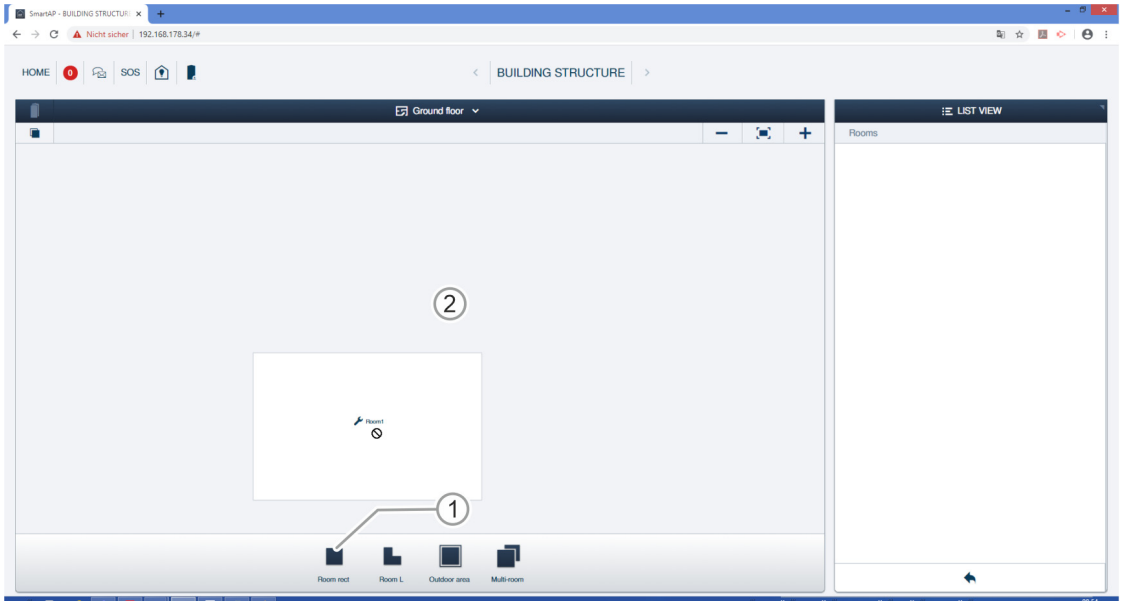


Fig. 85: Selecting the room version

1. Select the room version from the list [1] and pull it onto the working area [2].

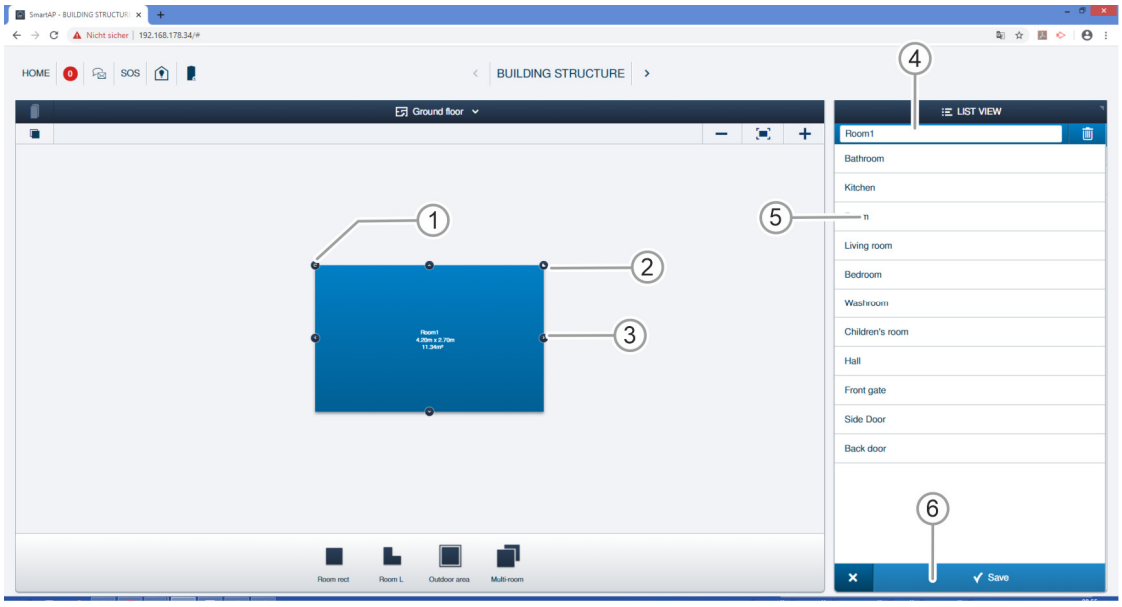


Fig. 86: Edit room

2. Click on the room.
   - The room gets a blue background. Buttons appear at the edge of the room with which the form and size of the room can be adjusted.
     - The room is turned with button [1].
     - The size of the room is enlarged or reduced with button [2].
     - The position of the individual edges is changed with button [3].
3. Enter the name of the room in field [4] or select an available room name from the list [5].

4. Click on the "Save" button [6].

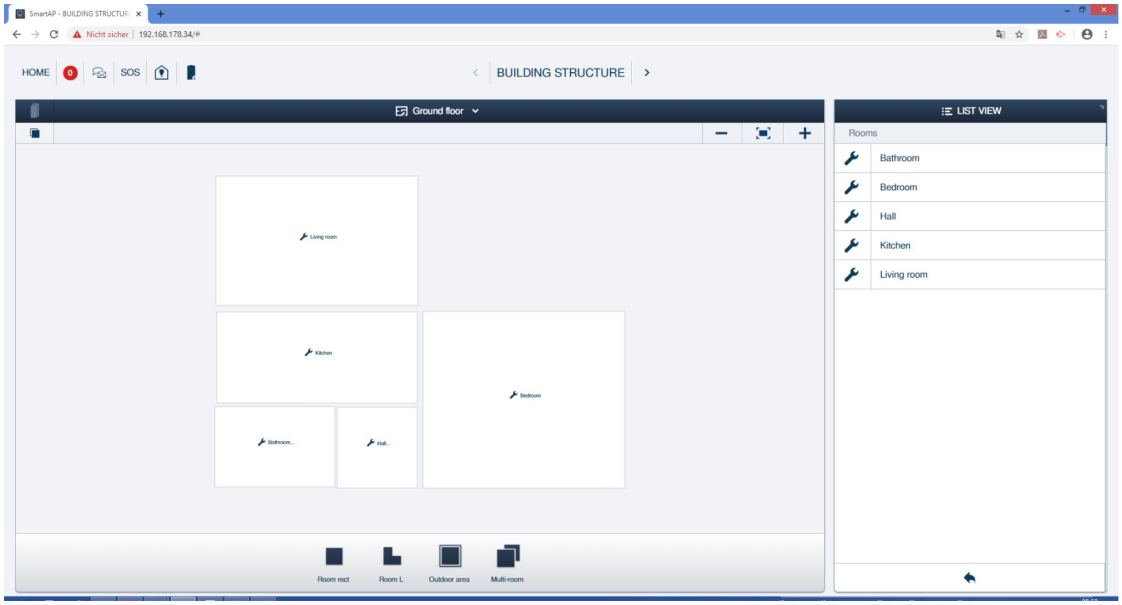


Fig. 87: Creating additional rooms

5. Repeat the working steps until the floor plan of the floor has been fully created.

5.3 Device configuration

Devices are added via menu item "Device configuration" in the main menu of the "Smart Access Point Pro".

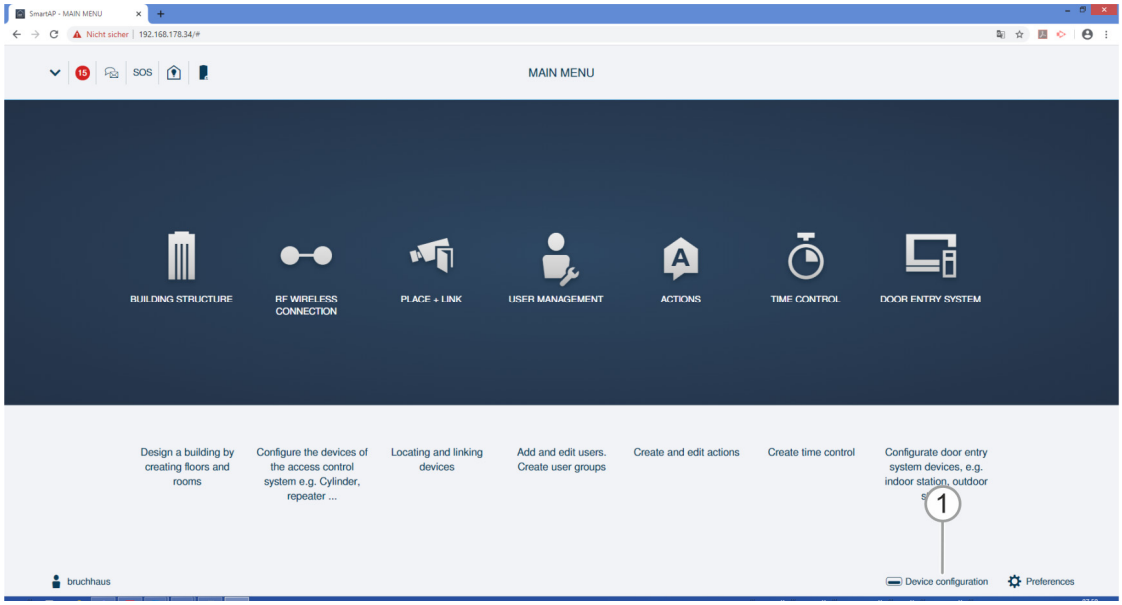


Fig. 88: Menu "Device configuration"

The following settings are made in menu item "Device configuration" [1]:

– Add devices,
– Delete devices from the system,
– Change device properties.

5.3.1 Add "Smart Access Point Pro"

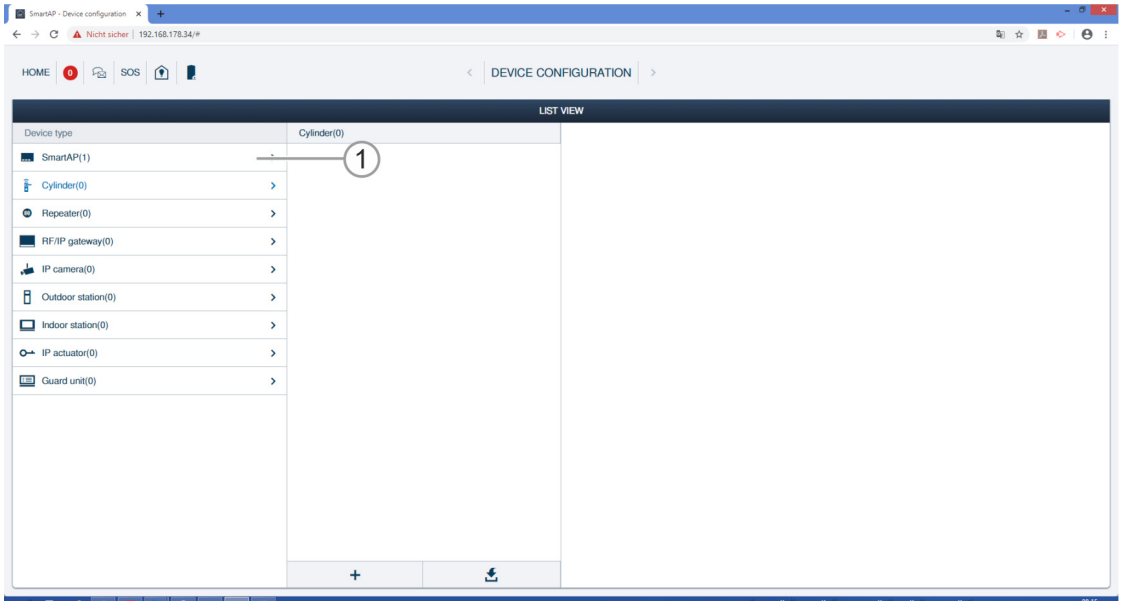


Fig. 89: "Smart Access Point Pro" in the list of available devices

The "Smart Access Point Pro" is not added. After initial commissioning the "Smart Access Point Pro" automatically in the list of available devices [1].

5.3.2 Add "Electronic cylindrical lock"

To add a "Electronic cylindrical lock", perform the following steps:

Fig. 90: Add "Electronic cylindrical lock"

1. Click on the "Cylinder" button [1].

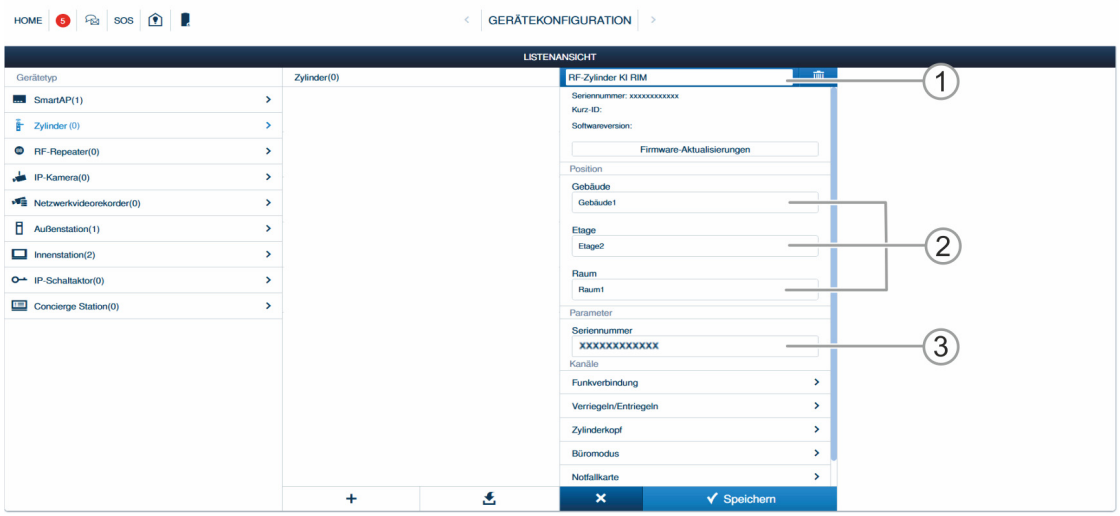


Fig. 91: Enter "Electronic cylindrical lock" data

2. Enter the name of the "Electronic cylindrical lock" in field [1].
3. Assign the "Electronic cylindrical lock“ to the building structure [2] (building, floor, room).
   – The assignment to the building structure can also be made later, see chapter 5.2 “Building structure“ on page 95.
4. Enter the serial number [3] of the "Electronic cylindrical lock".
   – The serial number is located on the type plate in the battery compartment, see chapter 3.2.1 ““Electronic cylindrical lock"“ on page 51.
5. Click on the "Save" button.

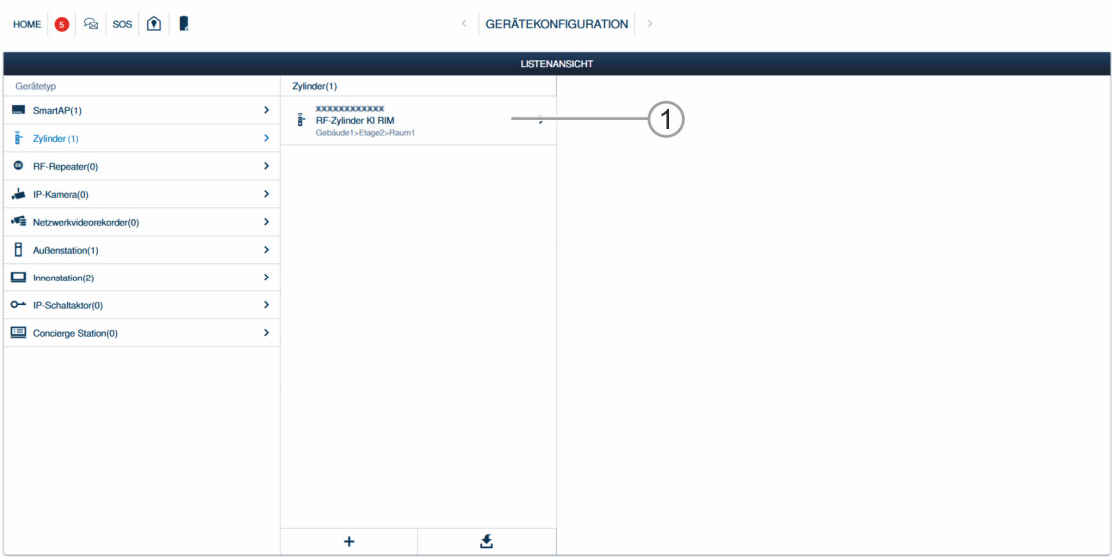


Fig. 92: "Electronic cylindrical lock" created

The created "Electronic cylindrical lock" is displayed in the "Cylinder" field [1].

5.3.3 "Electronic cylindrical lock" Settings – Emergency function

In the setting area of the "Electronic cylindrical lock" various device statuses can be viewed and settings made.

A prerequisite for some areas is that the "Electronic cylindrical lock" has already been coupled and a user with a transponder card has a closing right for the "Electronic cylindrical lock".

The following example lists the setup of the emergency situation for a transponder key. With this emergency card the selected "Electronic cylindrical lock" can also be opened when the "Electronic cylindrical lock" has no radio connection to the "Smart Access Point Pro". This, for example, is the case during a power failure of the "Smart Access Point Pro" or in a room to which a radio connection has not been set up.

Use the following steps to set up the emergency card for a "Electronic cylindrical lock":

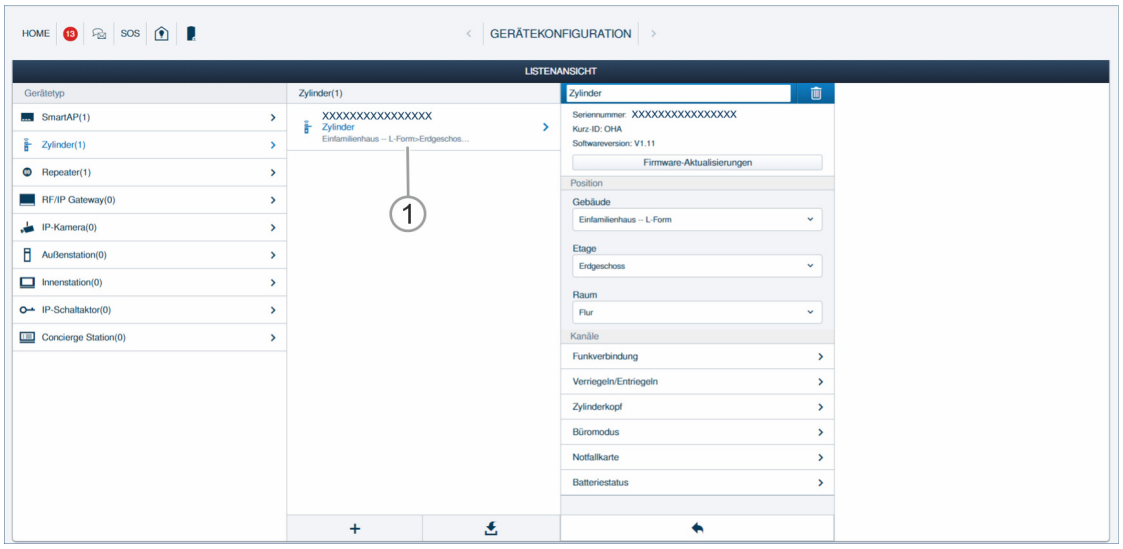


Fig. 93: Setting area of the "Electronic cylindrical lock"

1. Display the setting area of the "Electronic cylindrical lock".
   – For this, click on the desired "Electronic cylindrical lock" [1].

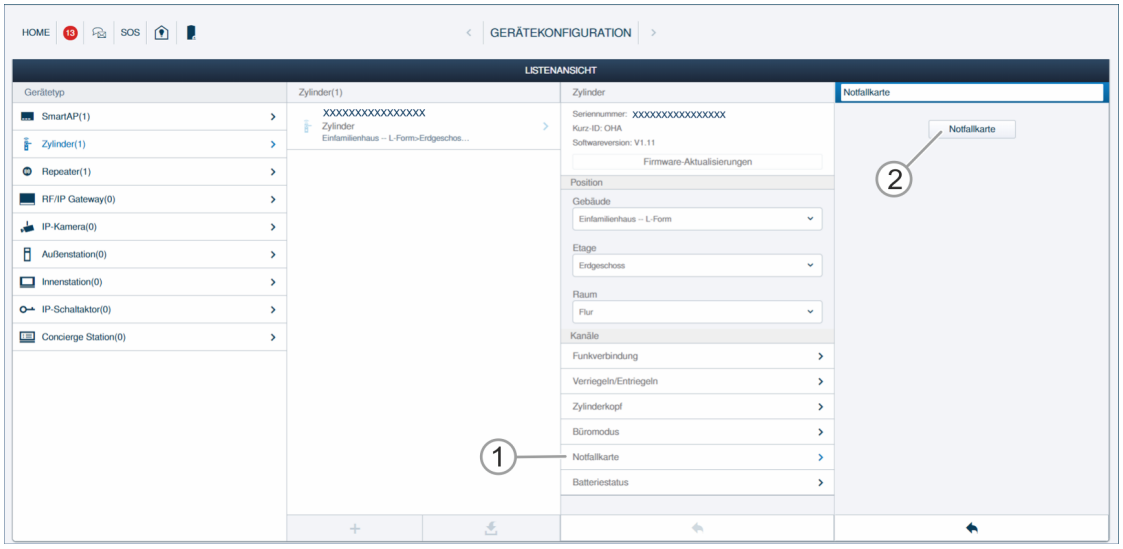


Fig. 94: "Electronic cylindrical lock" emergency function setting

2. Select the "Emergency card" setting [1].
3. Open the "Emergency card" function [2].

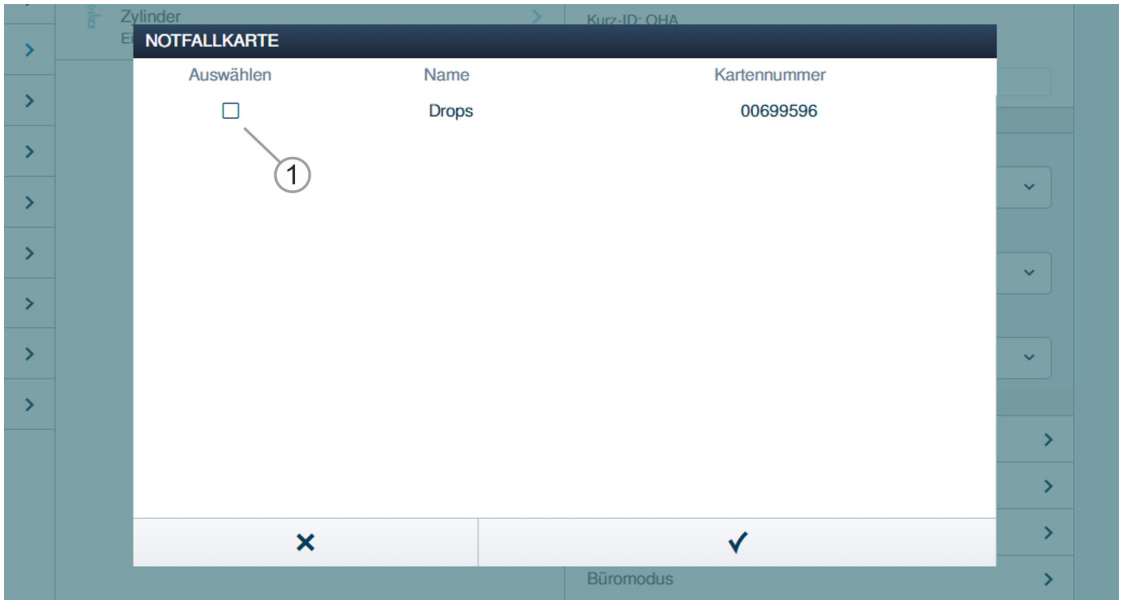


Fig. 95: Set up the "Electronic cylindrical lock"

4. Select the desired transponder key in the list [1].
   - All transponder keys that are stored via the authentication in the system are shown in the list, see chapter 5.5.3 “Add authentication“ on page 138.
   - The emergency function can be set up for every listed transponder key. This turns the transponder key into an emergency card.
5. Confirm the selection.
   - The emergency function for the transponder key has been set up.
   - The selected "Electronic cylindrical lock" can be opened with this emergency card even during a non-existing radio connection to the "Smart Access Point Pro".

5.3.4 Add "RF/IP Gateway"

To add a "RF/IP Gateway", perform the following steps:

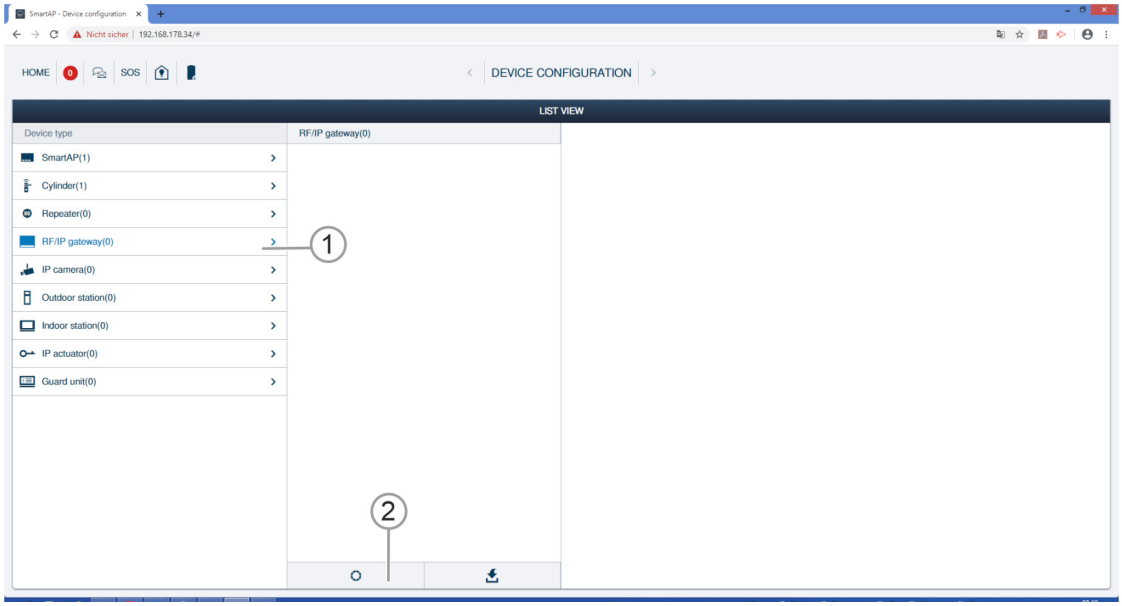


Abb. 96: Add "RF/IP Gateway"

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

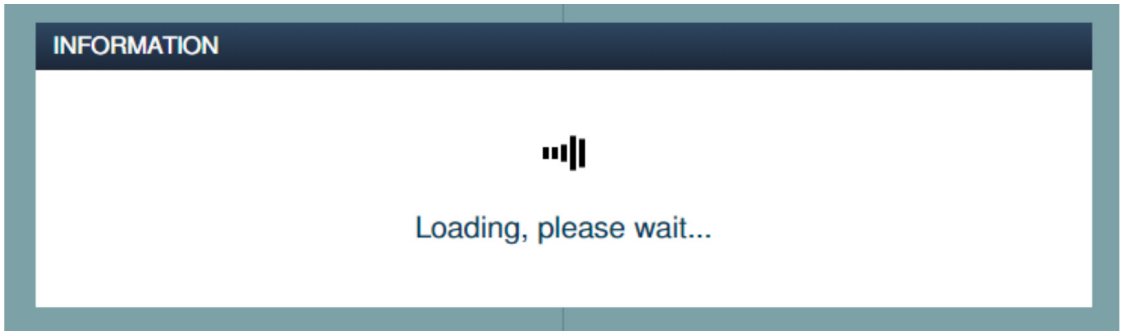


Fig. 97: Search for "RF/IP Gateway"

– The system searches for reachable "RF/IP Gateway".

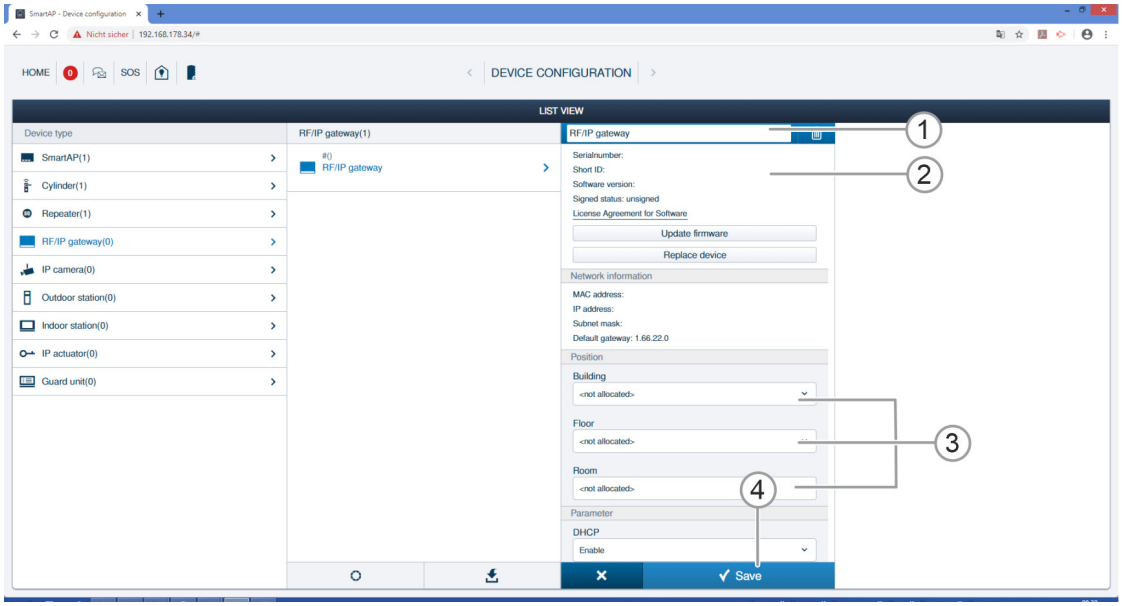


Fig. 98: "RF/IP Gateway" characteristics

– All "RF/IP Gateway" found are displayed in the list view.

3. Enter the name of the "RF/IP Gateway" in field [1].
4. Enter the serial number [2] of the "RF/IP Gateway".
5. Assign the "RF/IP Gateway“ to the building structure [3] (building, floor, room).
   – The assignment to the building structure can also be made later, see chapter 5.2 “Building structure“ on page 95.
6. Click on the "Save" button [4].

The "RF/IP Gateway" has been created.

5.3.5 Add "RF Repeater"

To add a "RF Repeater", perform the following steps:

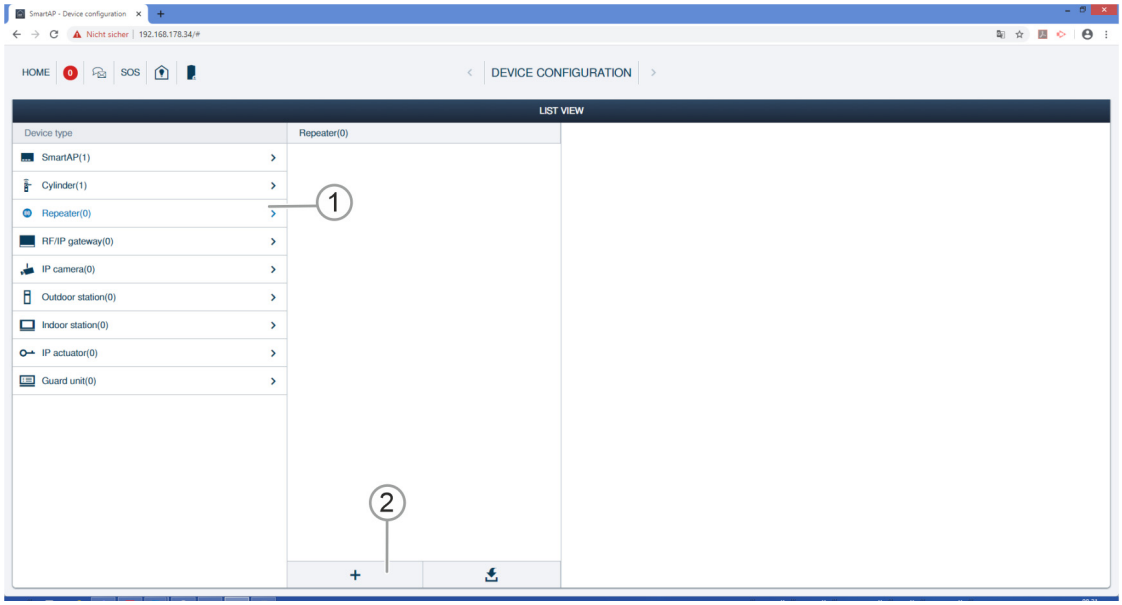


Abb. 99: Add "RF Repeater"

1. Click on the "RF Repeater" button [1].
2. Click on the "Add user" button [2].

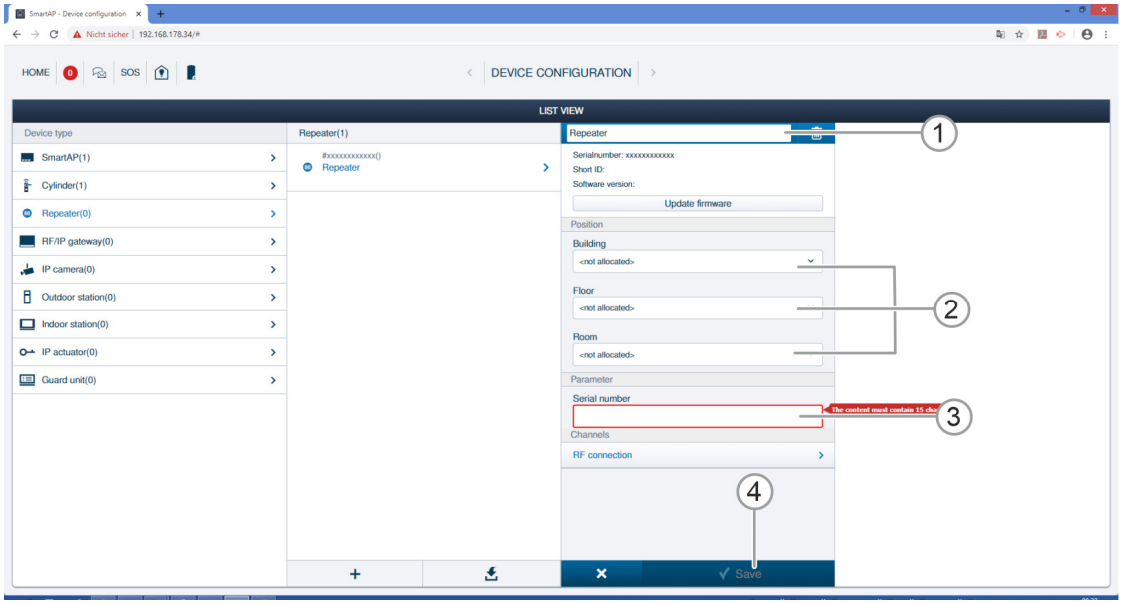


Fig. 100: "RF Repeater" characteristics

3. Enter the name of the "RF Repeater" in field [1].
4. Assign the "RF Repeater" to the building structure [2] (building, floor, room).
   – The assignment to the building structure can also be made later, see chapter 5.2 “Building structure“ on page 95.

5. Enter the serial number [3] of the "RF Repeater".
6. Click on the "Save" button [4].

The "RF Repeater" has been created.

5.4 Access control

In menu item "Access control" [1] in the main menu of the "Smart Access Point Pro" the devices of the "ABB-AccessControl" system are distributed to the individual rooms and floors in the building structure. Also the coupling of the devices of the "ABB-AccessControl".

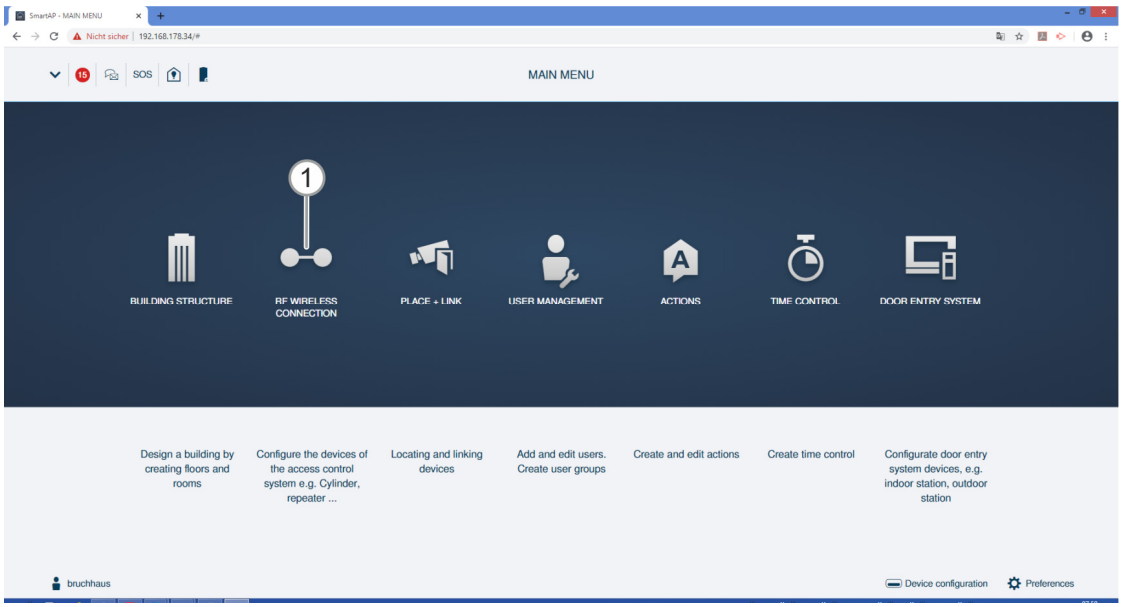


Fig. 101: Menu "Access control"

5.4.1 Placing the "Smart Access Point Pro"

To place a "Smart Access Point Pro", perform the following steps:

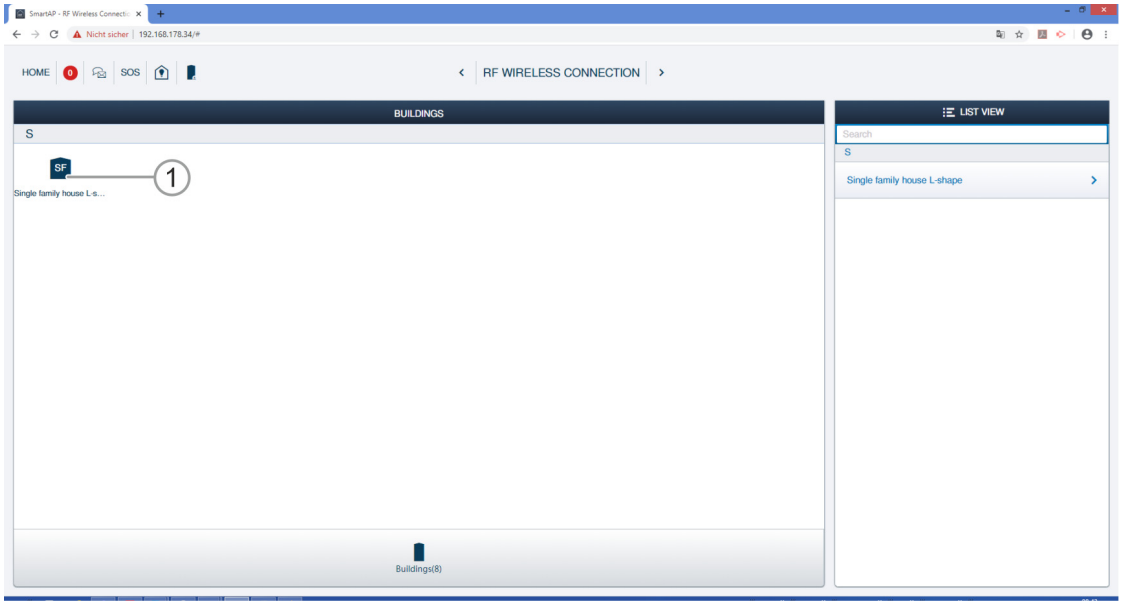


Fig. 102: Selecting the building

1. Select the desired building [1].

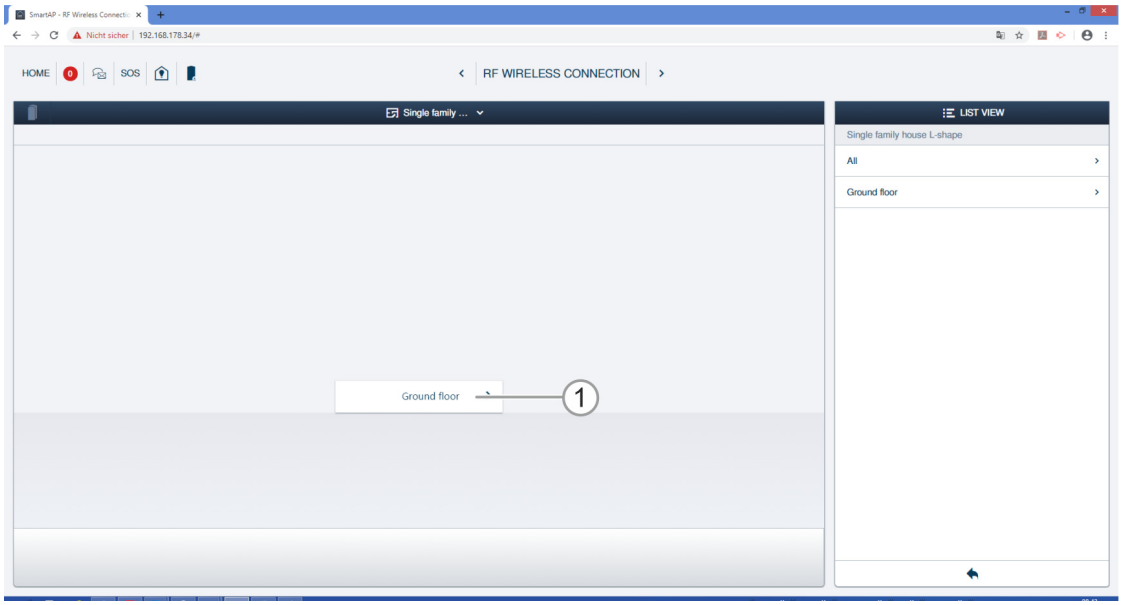


Fig. 103: Selecting the floor

2. Select the desired floor [1].

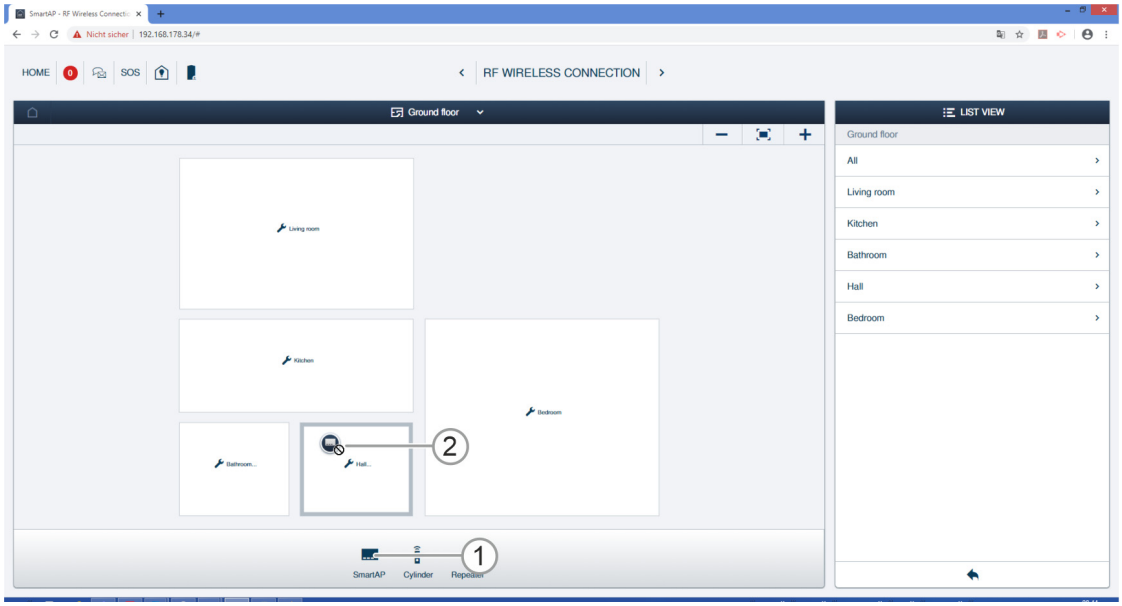


Abb. 104: Pulling the "Smart Access Point Pro" onto the room

3. Pull the "Smart Access Point Pro" [1] onto the desired room [2].

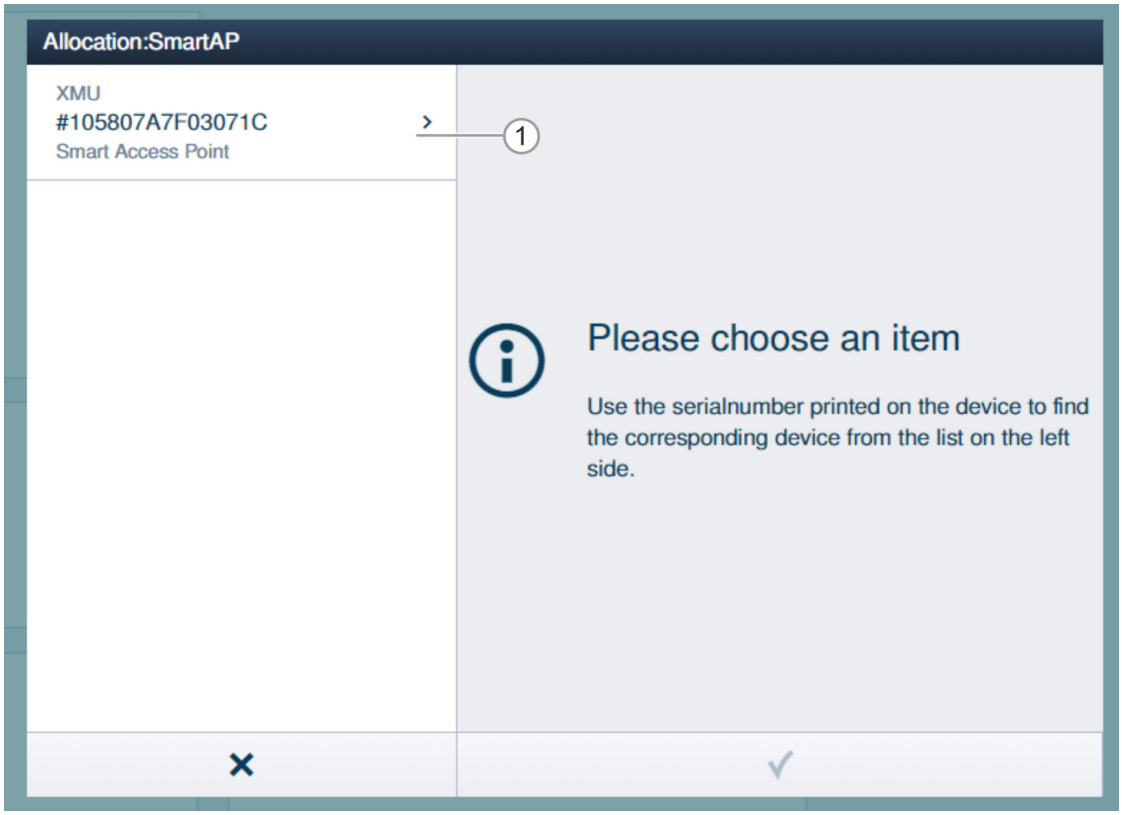


Fig. 105: Allocation of "Smart Access Point Pro"

4. Select "Smart Access Point Pro" from the list [1].

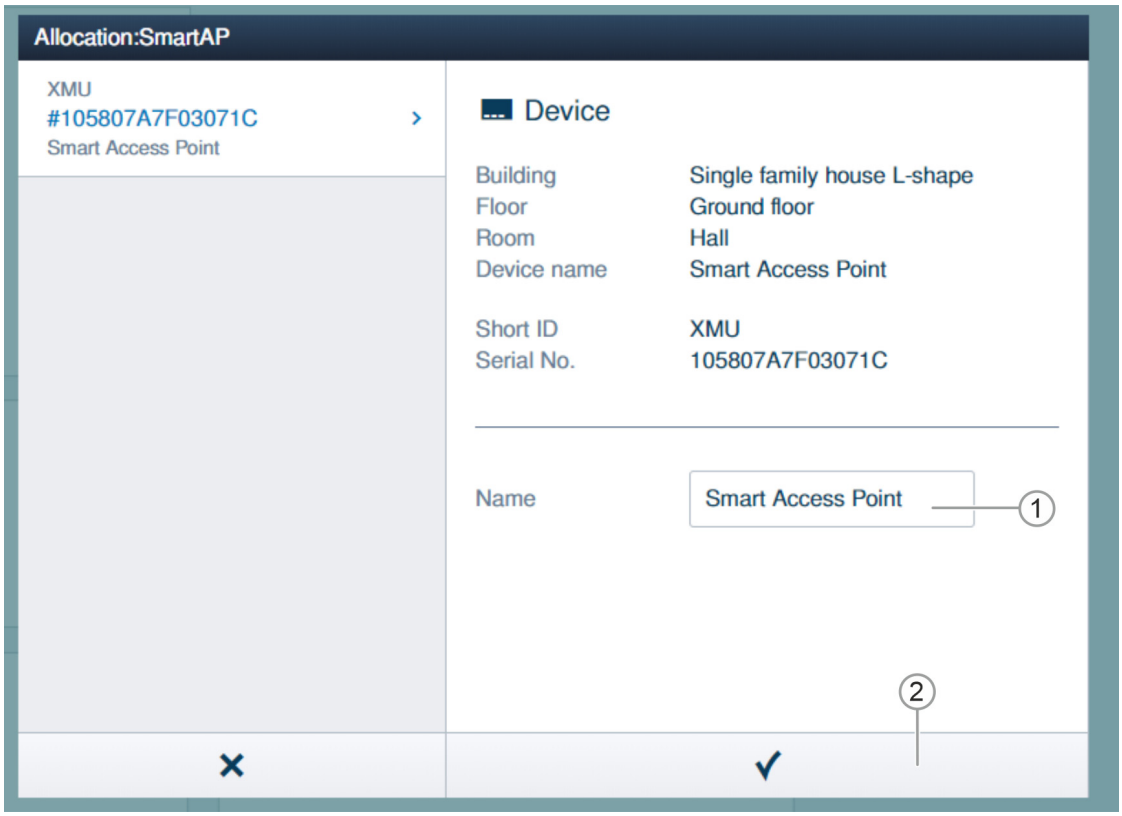


Fig. 106: Allocation of "Smart Access Point Pro" - Details

5. Enter the desired designation for "Smart Access Point Pro" in field [1].
6. Click on the "Save" button [2].

5.4.2 Placing the "RF/IP Gateway"

To place a "RF/IP Gateway", perform the following steps:

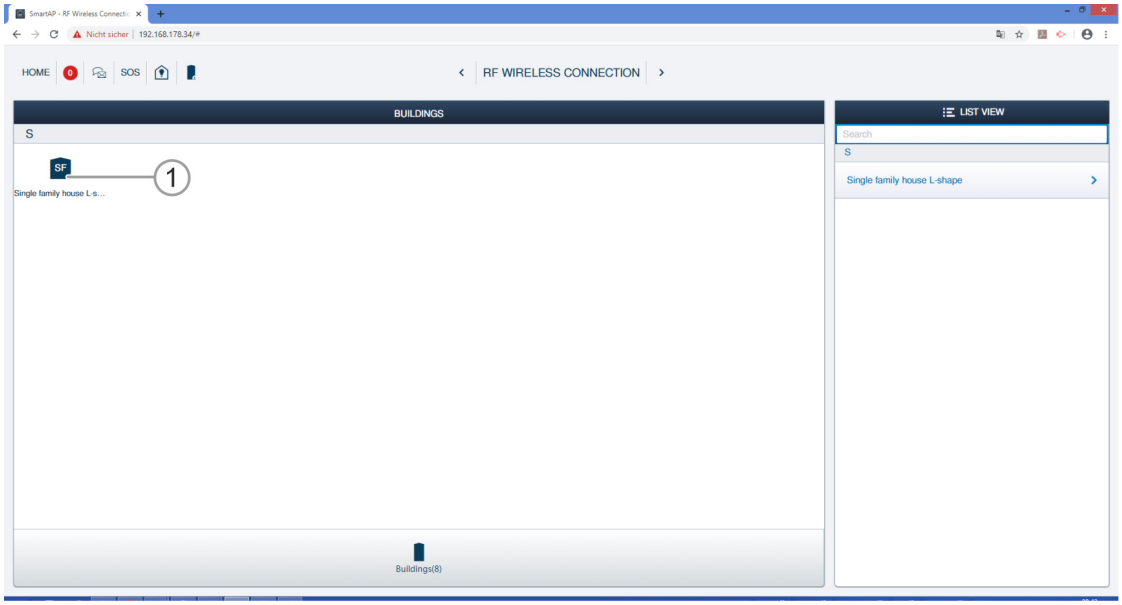


Fig. 107: Selecting the building

1. Select the desired building [1].

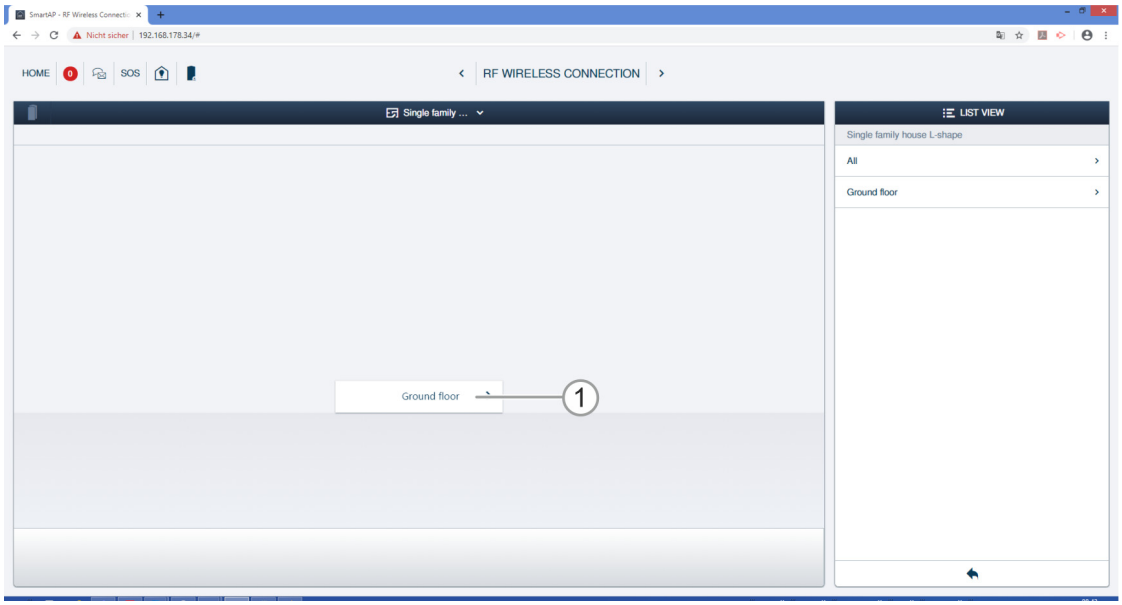


Fig. 108: Selecting the floor

2. Select the desired floor [1].

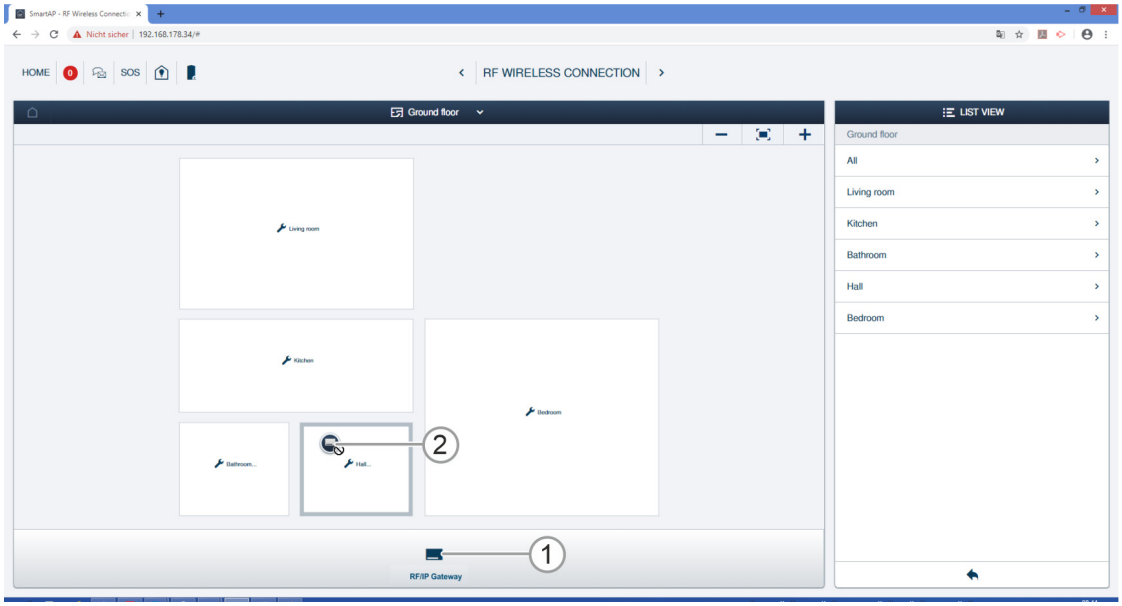


Abb. 109: Pulling the "RF/IP Gateway" onto the room

3. Pull the "RF/IP Gateway" [1] onto the desired room [2].

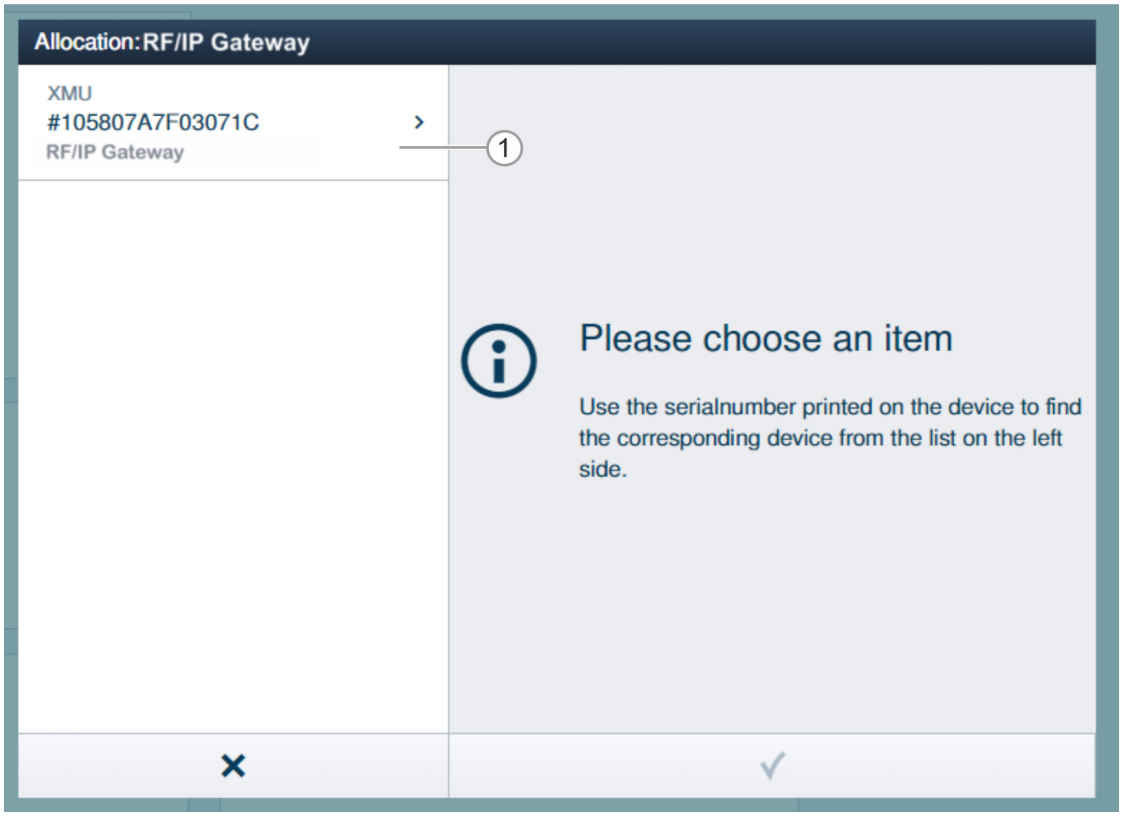


Fig. 110: Allocation of "RF/IP Gateway"

4. Select "RF/IP Gateway" from the list [1].

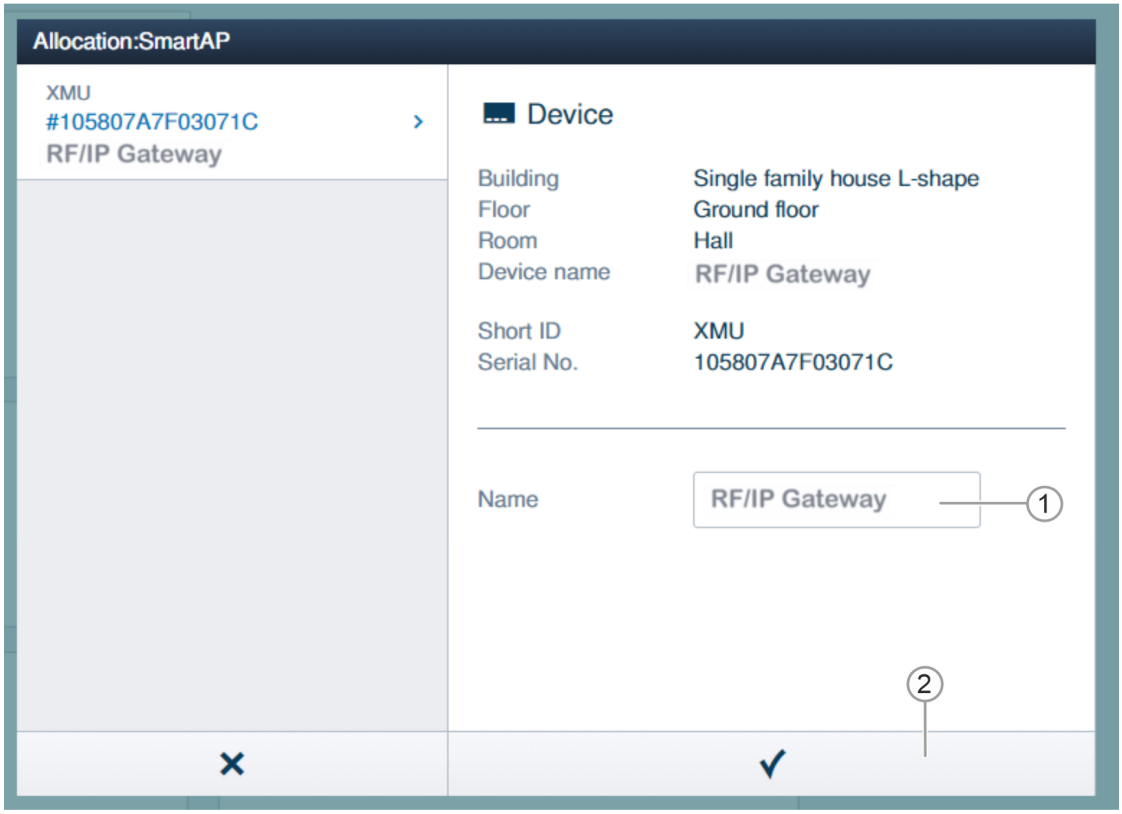


Fig. 111: Allocation of "RF/IP Gateway" - Details

5. Enter the desired designation for "RF/IP Gateway" in field [1].
6. Click on the "Save" button [2].

5.4.3 Placing the "Electronic cylindrical lock"

To place a "Electronic cylindrical lock", perform the following steps:

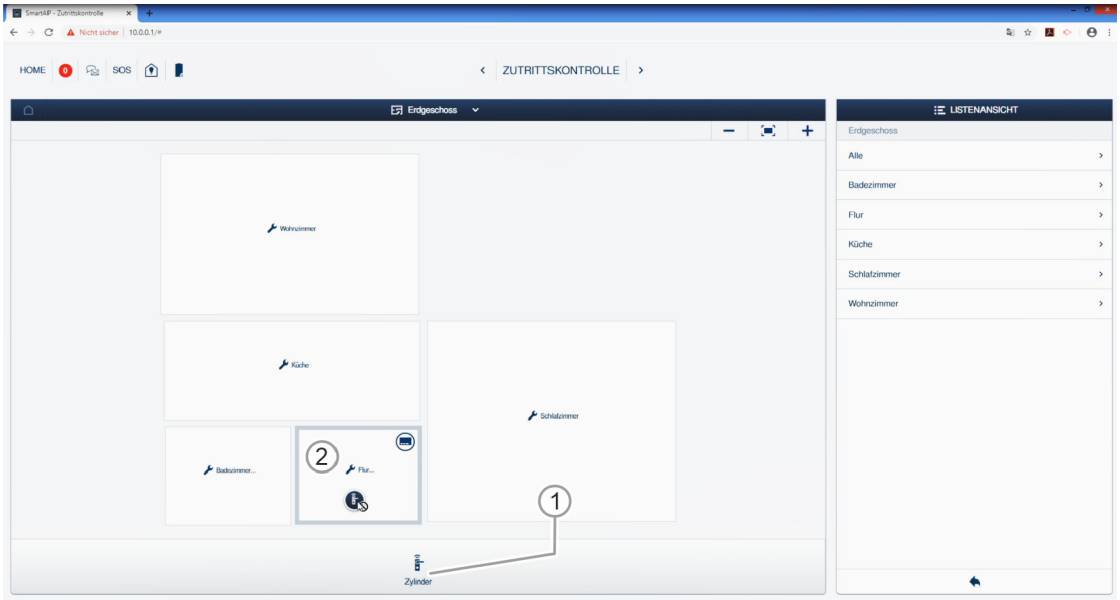


Fig. 112: Pulling the "Electronic cylindrical lock" onto the room

1. Pull the "Electronic cylindrical lock" from the list [1] onto the desired room [2].

Fig. 113: Allocation of "Electronic cylindrical lock" 1.

2. Select the "Electronic cylindrical lock" from the list.

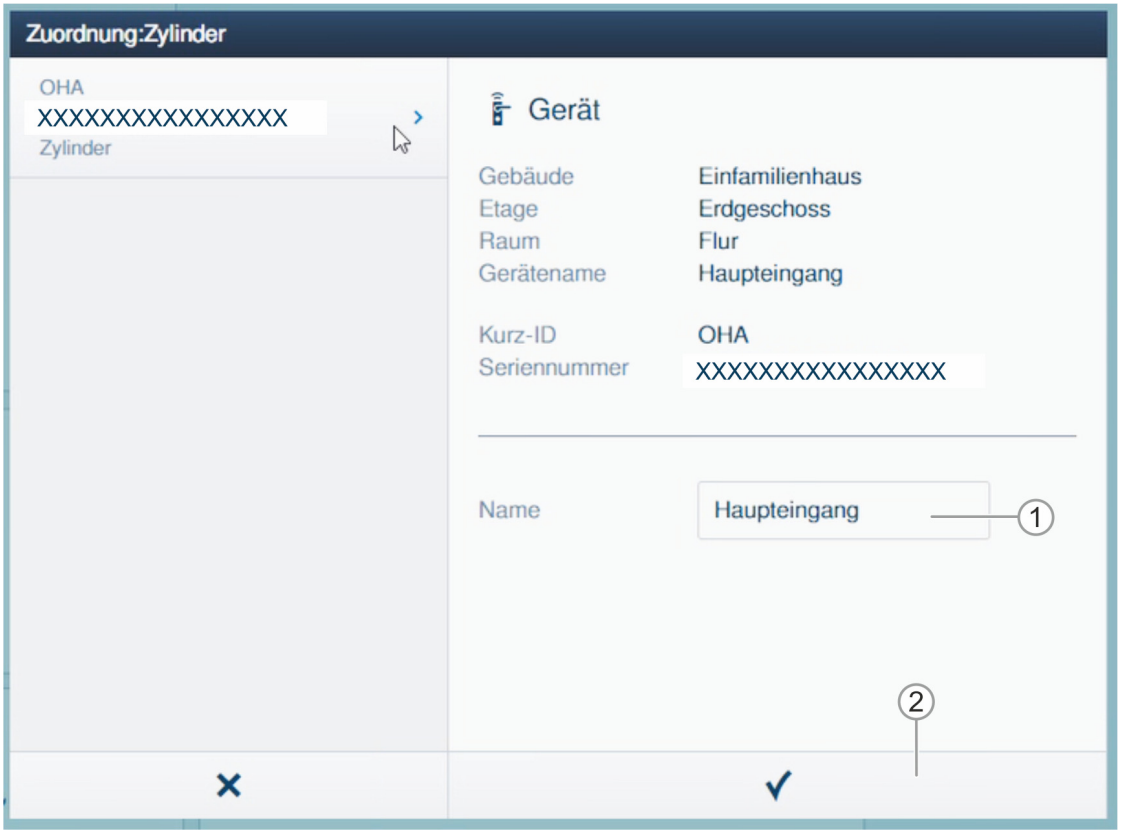


Fig. 114: Allocation of "Electronic cylindrical lock" 2.

3. Enter a name for the "Electronic cylindrical lock" and click on the "Save" button.

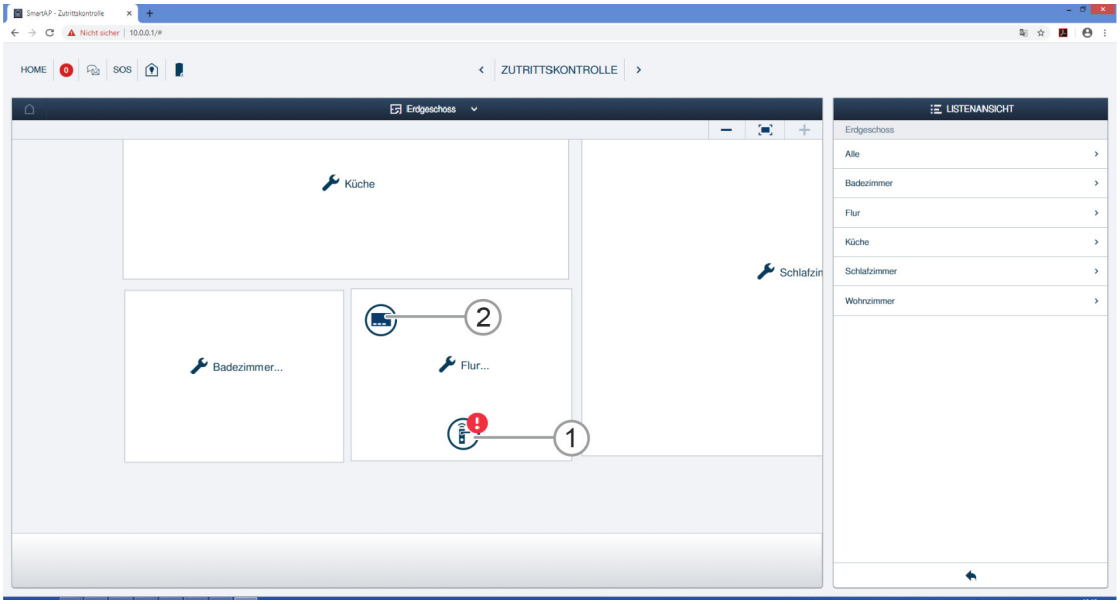


Fig. 115: "Electronic cylindrical lock" in the room

The newly created "Electronic cylindrical lock" [1] and the "Smart Access Point Pro" [2] are displayed in the room.

The icon "!" and the missing connecting line show that there is yet no connection between the two devices.

5.4.4 Coupling the "Electronic cylindrical lock" with the "Smart Access Point Pro"

Attention! Loss of data

If no backup is available and the data in the "Smart Access Point" are lost, the battery-operated access systems can no longer be uncoupled for re-commissioning. The old data remain in the reading heads. Since these are locking systems, access from outside is not possible. This could be an unauthorized access.

– The battery-operated access systems must then be reset in the manufacturer's factory.
  – Make absolutely certain that you have a backup of the data of the "Smart Access Point".

The newly created "Electronic cylindrical lock" must now be linked (coupled) with the "Smart Access Point Pro".

Use the following steps to couple the "Electronic cylindrical lock" with the "Smart Access Point Pro":

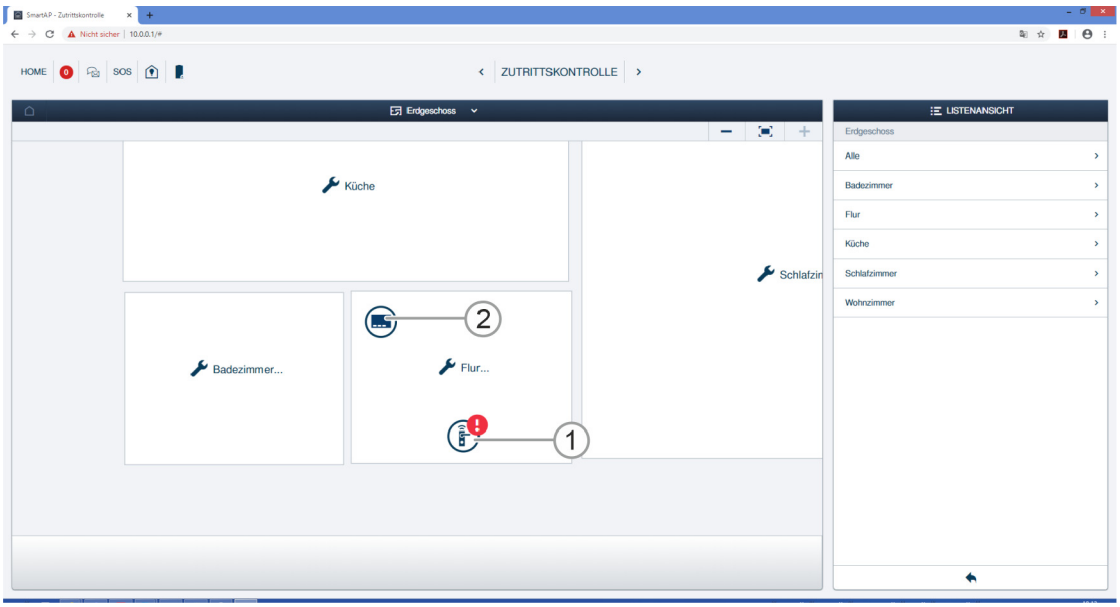


Fig. 116: Coupling the "Electronic cylindrical lock" with the "Smart Access Point Pro"

1. Click on the "Electronic cylindrical lock" [1].
2. Click on the "Smart Access Point Pro" [2].

Fig. 117: Coupling process 1/3

3. Follow the instructions on the display and hold the maintenance card in front of the "Electronic cylindrical lock".

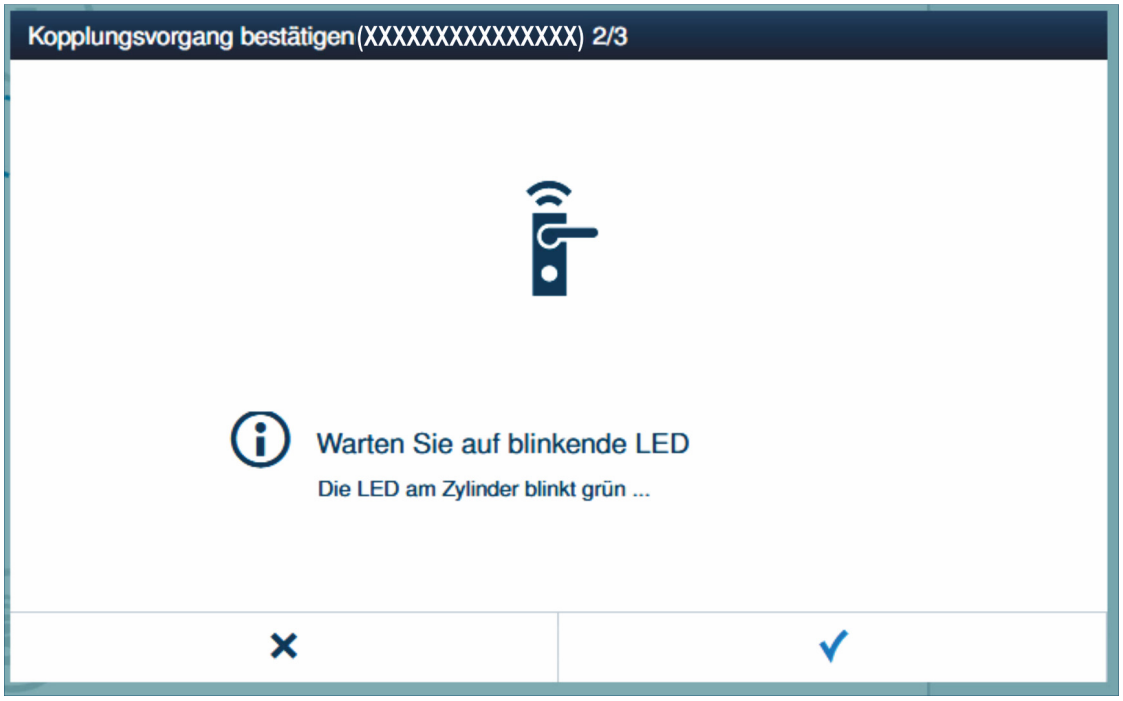


Fig. 118: Coupling process 2/3

4. Hold the maintenance card in front of the "Electronic cylindrical lock" until the LED flashes green.

Fig. 119: Coupling process 3/3

The "Electronic cylindrical lock" is now coupled with the "Smart Access Point Pro".

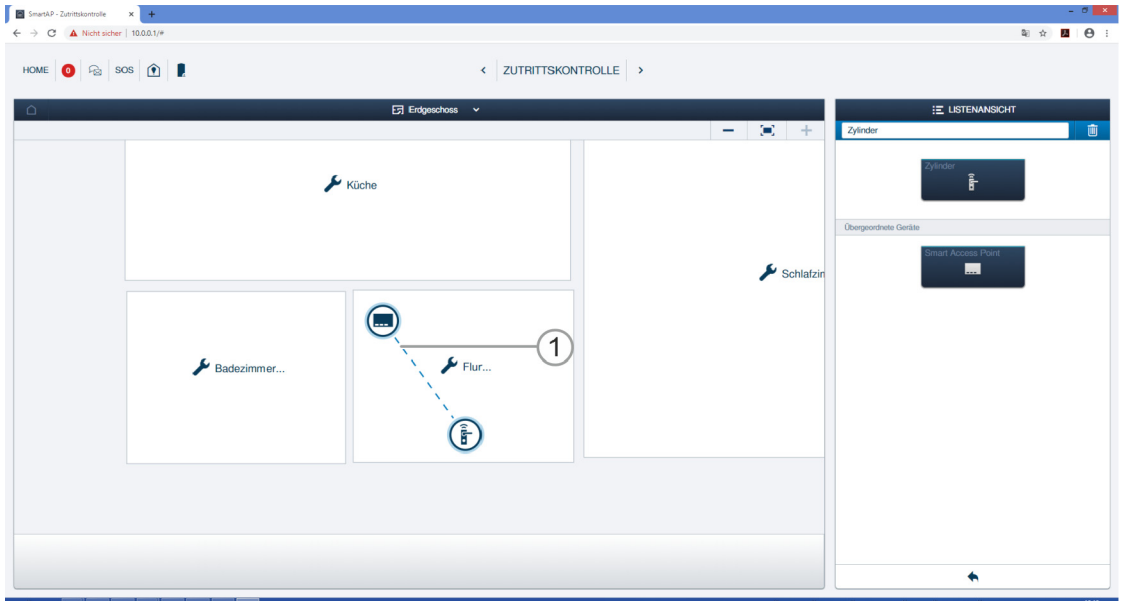


Fig. 120: "Electronic cylindrical lock" created

The successful coupling of both devices is displayed with a broken line [1].

The "Electronic cylindrical lock" is ready for operation and can be occupied with locking rights via the user management, see chapter 5.5 “User management“ on page 131.

Notice

This example describes the direct coupling to the "Smart Access Point Pro". Depending on the area of application, the "Electronic cylindrical lock" is coupled

to the last interconnected "RF Repeater" or to a "RF/IP Gateway" (also with or without interconnected "RF Repeater"). The coupling method is always the same.

For different coupling situations, see chapter 4.3 “Case studies“ on page 69.

5.4.5 Placing the "RF Repeater"

To place a "RF Repeater", perform the following steps:

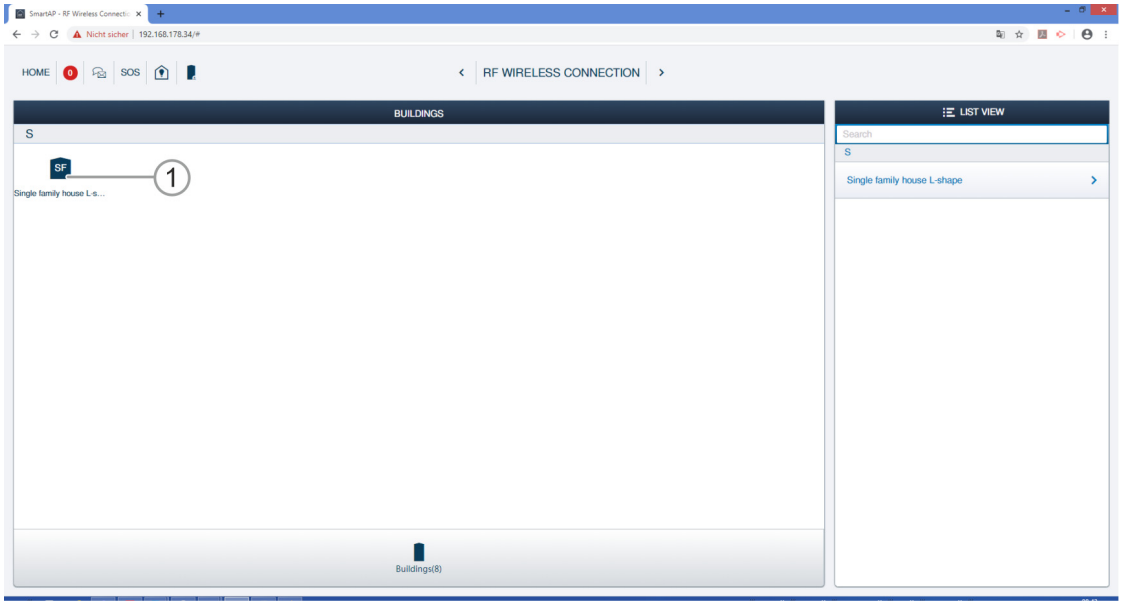


Fig. 121: Selecting the building

1. Select the desired building [1].

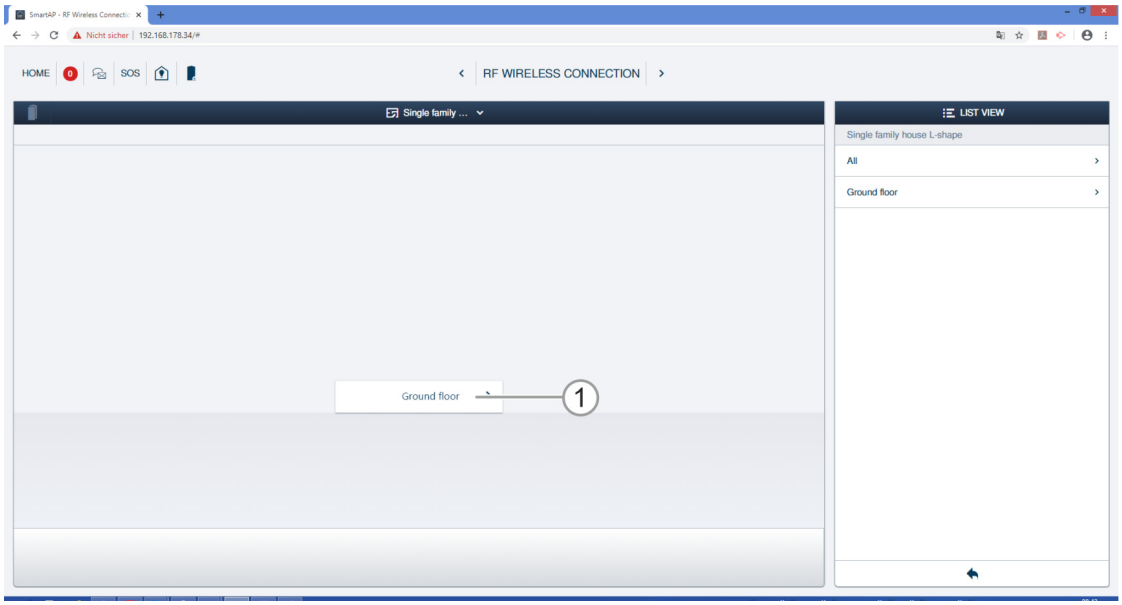


Fig. 122: Selecting the floor

2. Select the desired floor [1].

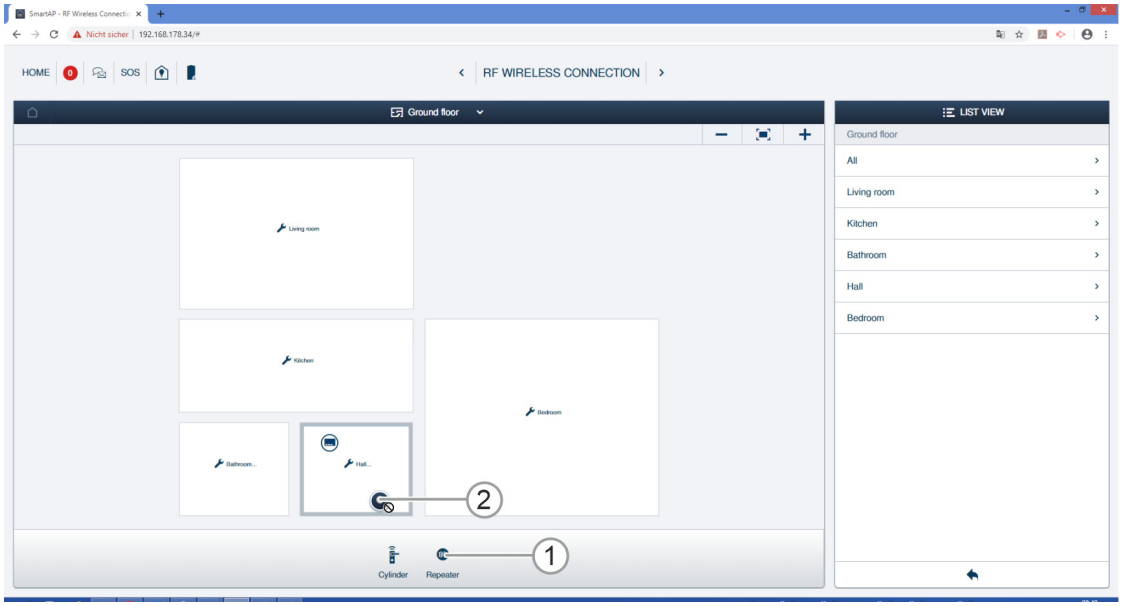


Abb. 123: Pulling the "RF Repeater" onto the room

3. Pull the "RF Repeater" [1] onto the desired room [2].

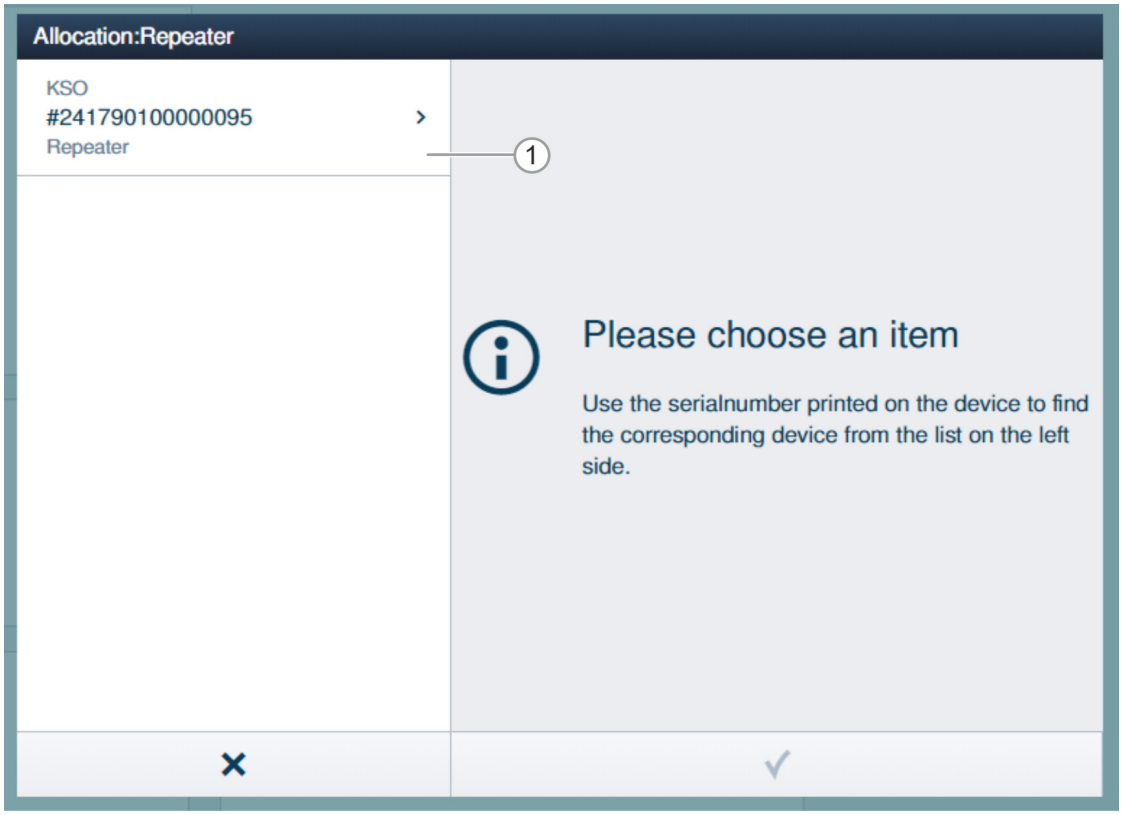


Fig. 124: Allocation of "RF Repeater"

4. Select "RF Repeater" from the list [1].

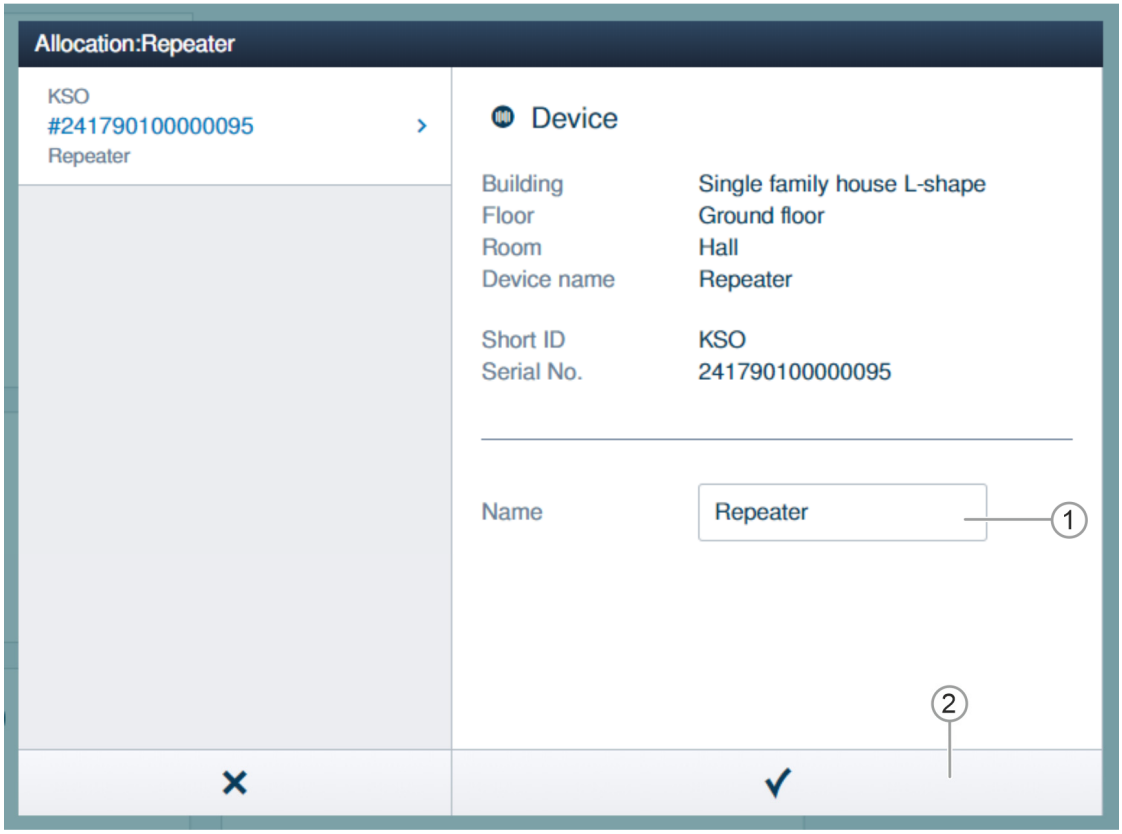


Fig. 125: Allocation of "RF Repeater" - Details

5. Enter the desired designation for "RF Repeater" in field [1].
6. Click on the "Save" button [2].

5.4.6 Coupling the "RF Repeater"

Use the following steps to couple the "RF Repeater" with the "Smart Access Point Pro":

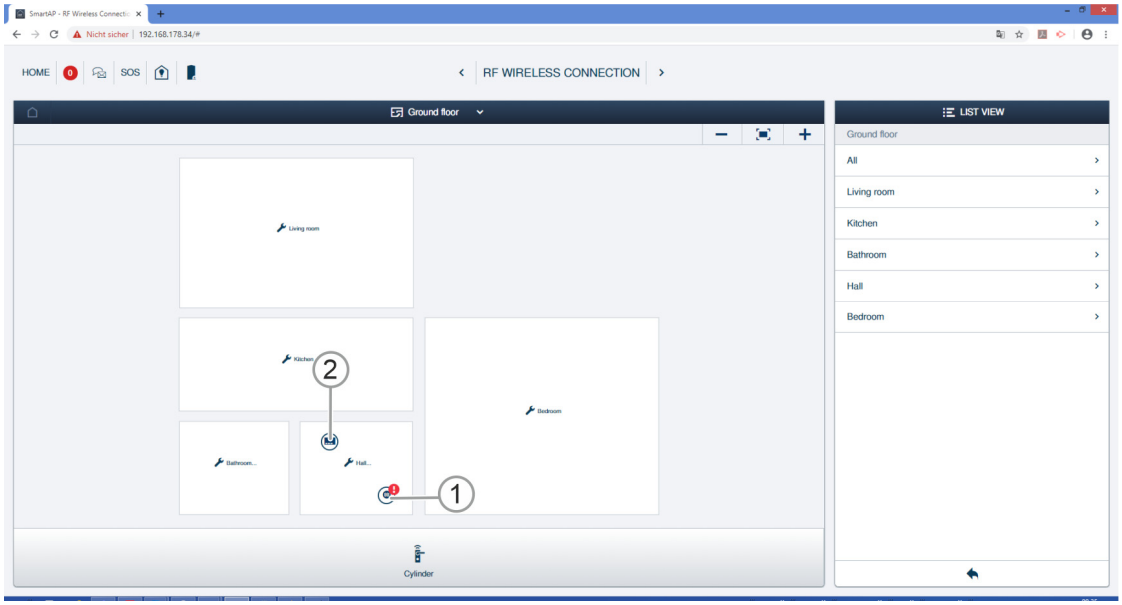


Fig. 126: Coupling the "RF Repeater" with the "Smart Access Point Pro"

1. Pull the "RF Repeater" [1] from the list into the desired room.
2. Click on the "RF Repeater" [1].
3. Click on the "Smart Access Point Pro" [2].

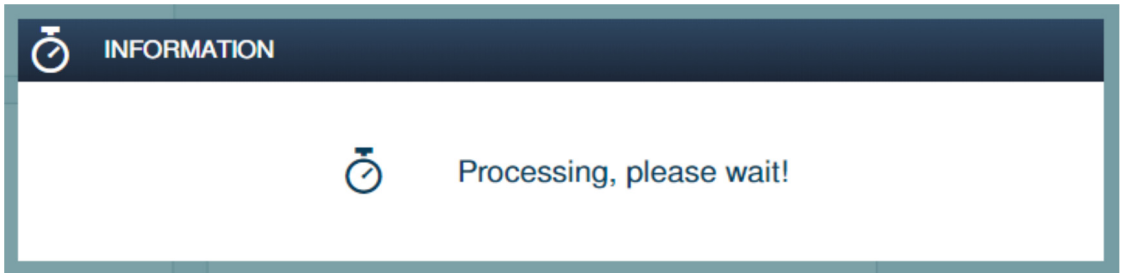


Fig. 127: Coupling process

– The progress of the coupling process is displayed in the window

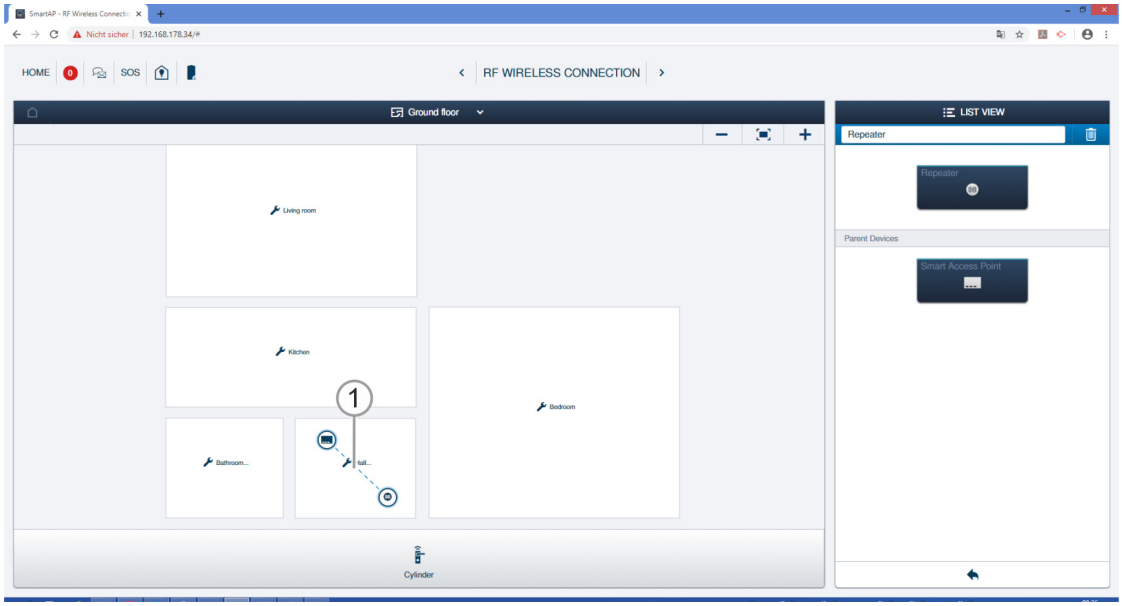


Fig. 128: "RF Repeater" coupled with "Smart Access Point Pro"

– The "RF Repeater" is now coupled with the "Smart Access Point Pro". The successful coupling of both devices is displayed with a broken line [1].

Notice

If several "RF Repeater" have been coupled consecutively in a radio line, one device will always be coupled with the next one. Finally the "Electronic cylindrical lock" is coupled with the last "RF Repeater" in the radio line.

5.5 User management

The management of the users, transponder keys and locking rights for the "Electronic cylindrical lock" is carried out via menu item "User management" [1] in the main menu of the "Smart Access Point Pro".

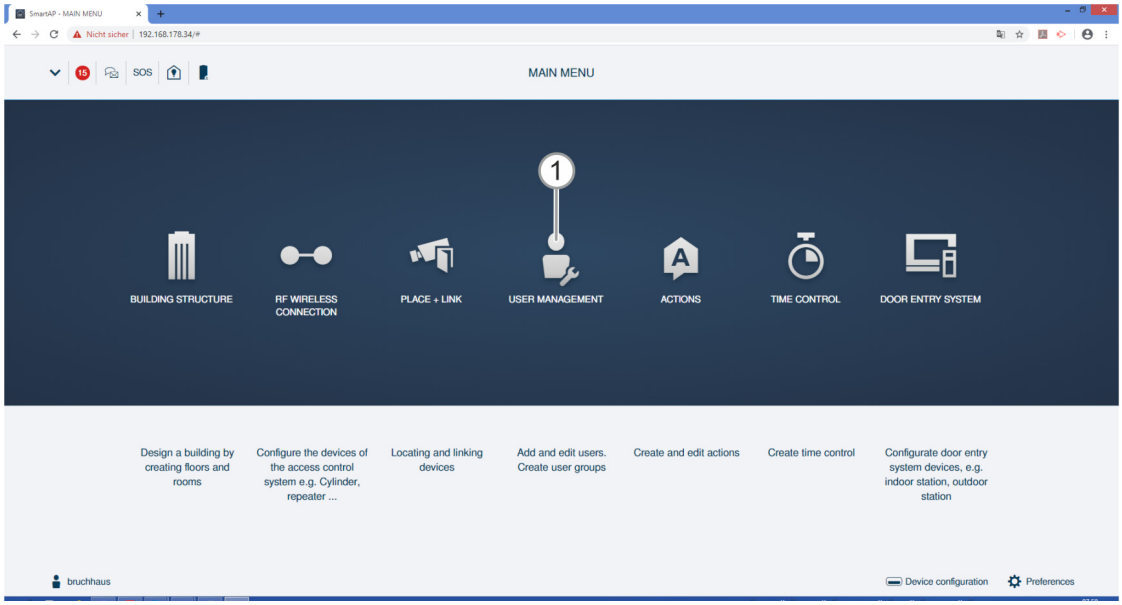


Fig. 129: Menu item "User management"

The following settings are made in menu item "User management" [1]:

- Create new users.
- Create new user groups.
- Create transponder keys.
- Create transponder keys and assign to a user (authentication).
- Assign and manage locking rights for users.

The following steps are required to assign locking rights:

1. Create user, see chapter 5.5.1 “Create user “ on page 132.
2. Assign transponder key to a user and read the data of the transponder key into the management software of the "Smart Access Point Pro"(authentication), see chapter 5.5.3 “Add authentication“ on page 138
3. Assigning users the locking rights to a "Electronic cylindrical lock", see chapter 5.5.4 “Assigning locking rights“ on page 143

5.5.1 Create user

To add a user, perform the following steps:

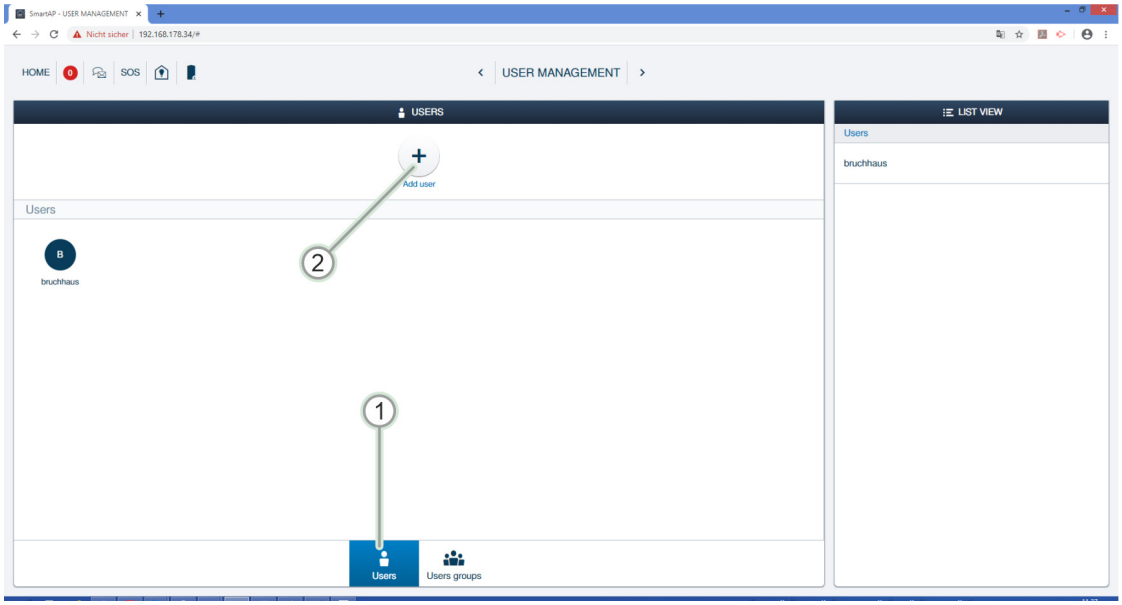


Fig. 130: Adding users

1. Click on the "Users" button [1].
2. Click on the "Add user" button [2].

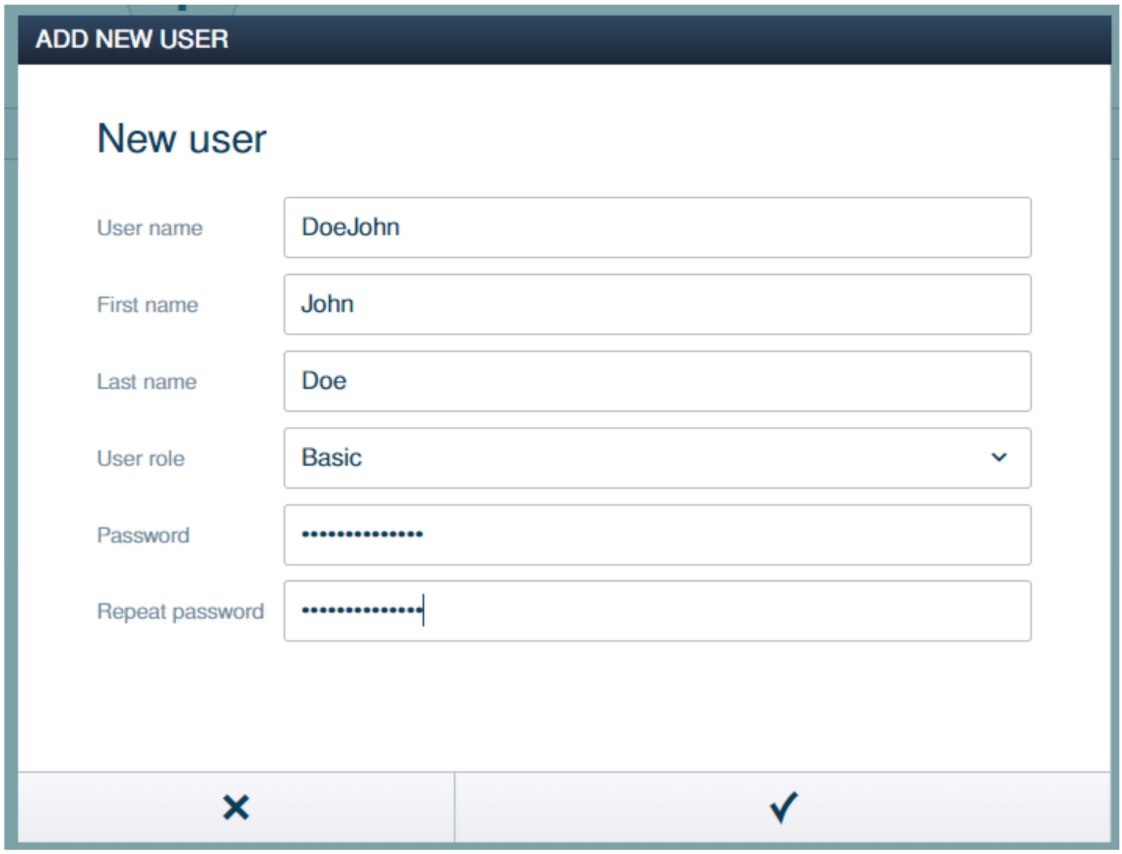


Fig. 131: User: Enter data

3. Enter the data for the new user.
4. Confirm the entries.
   – The new user has been created.

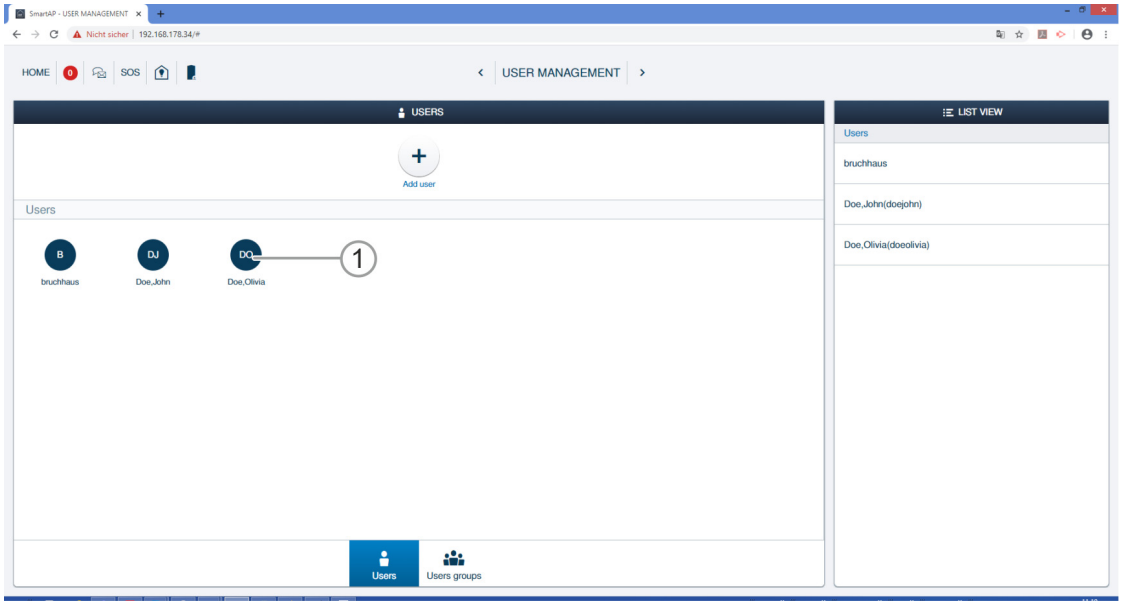


Fig. 132: Selecting user

5. Select the desired user [1] from the list for further editing.

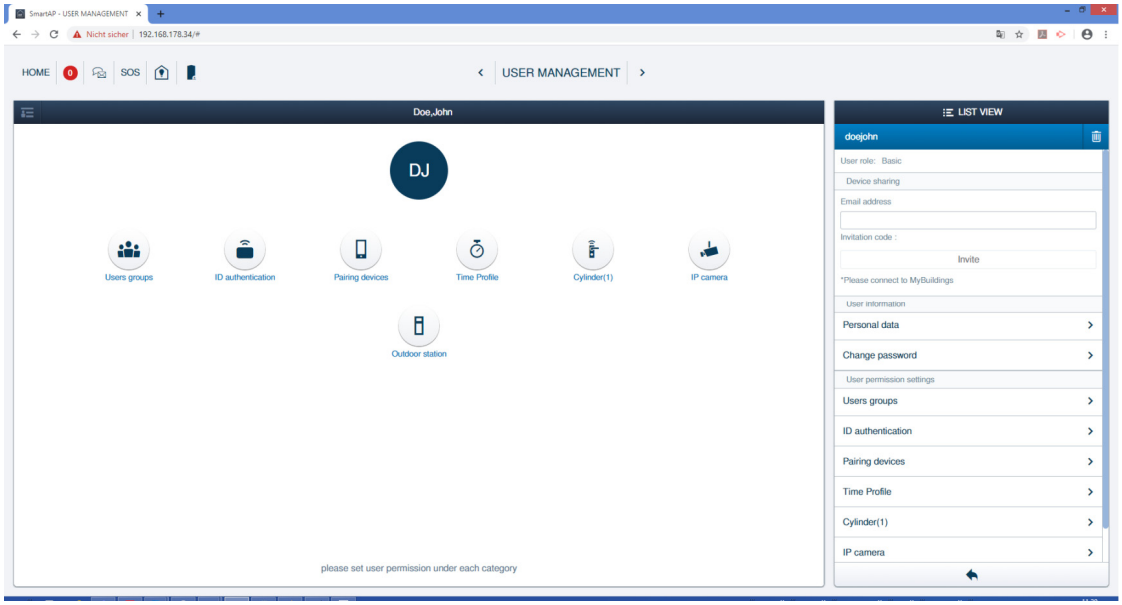


Fig. 133: Editing users

6. Enter the data (e.g. rights groups, password, e-mail address and user role) in the parameter fields.

Notice
The precise descriptions of the user parameters are available in the product manuals of the respective devices.

5.5.2 Creating user groups

User groups facilitate the management of the rights of users. If, for example, the allocation of a locking right to a specific room is issued to a user group, all members of this group automatically have the locking right. The locking right must not be assigned separately to each individual user.

To add a user group, perform the following steps:

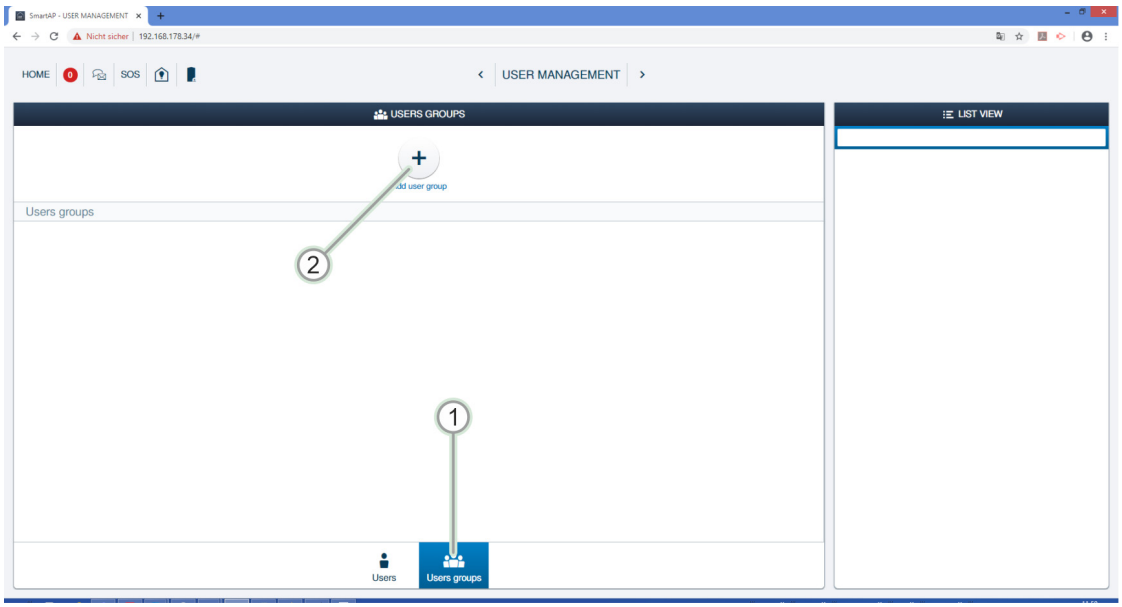


Fig. 134: Creating a user group

1. Click on the "User groups" button [1].
2. Click on the "Add user groups" button [2].

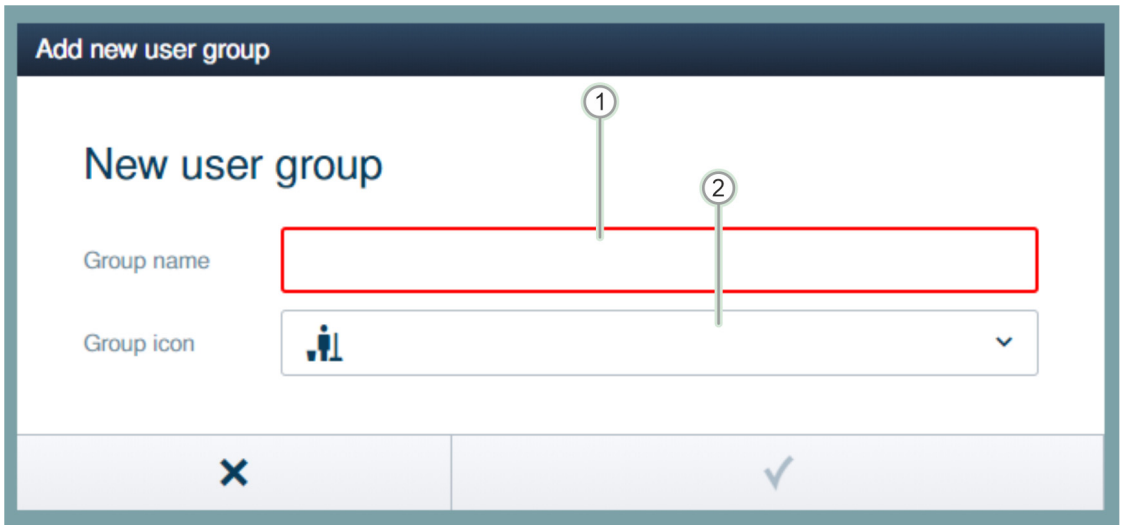


Fig. 135: Data input of user group

3. Assign a name for the user group [1].

4. Select an icon for the user group [2].
5. Confirm the selection.
   – The new user group has been created.

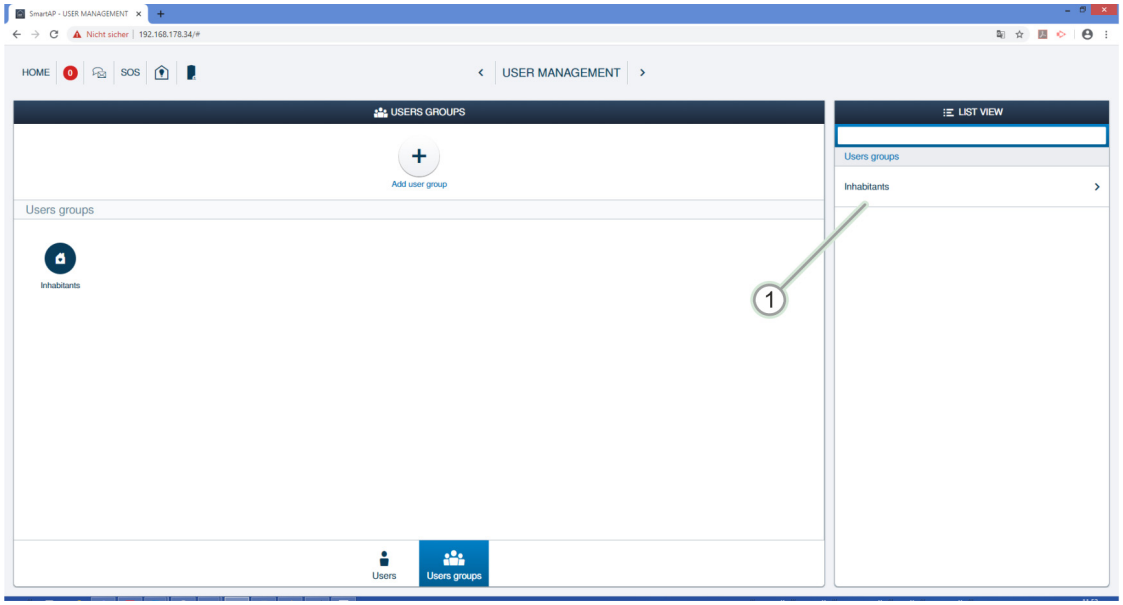


Fig. 136: Selecting a user group

6. Select the desired user group [1] from the list for further editing.

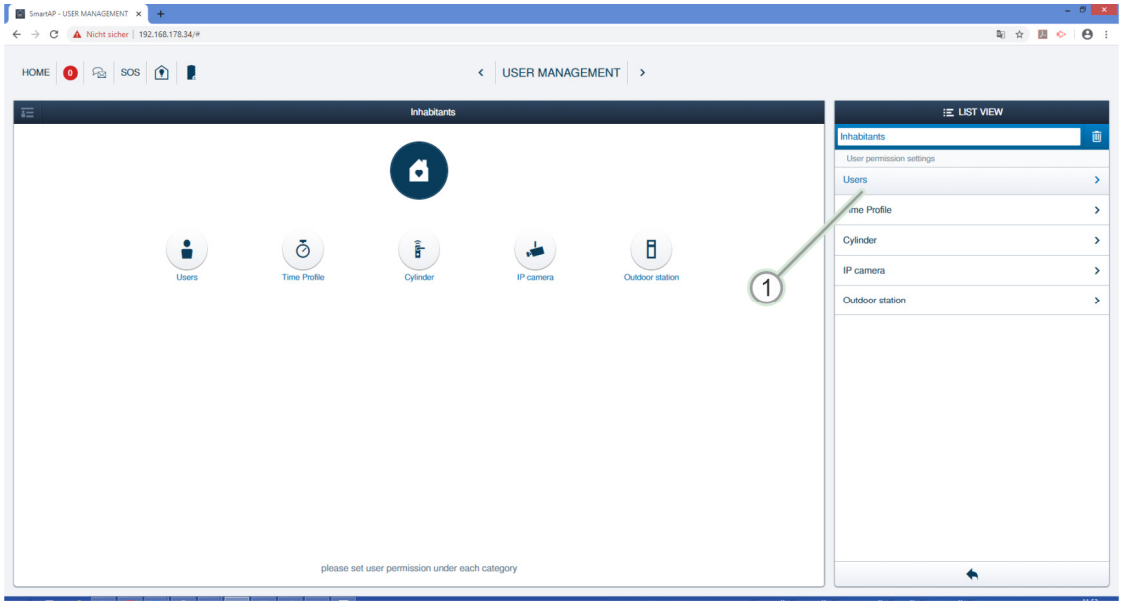


Fig. 137: User group: Selecting rights / characteristics

7. Select the desired rights / characteristics [1] from the list for further editing.
   – If users are to be taken into the group, select the "Users" area [1].

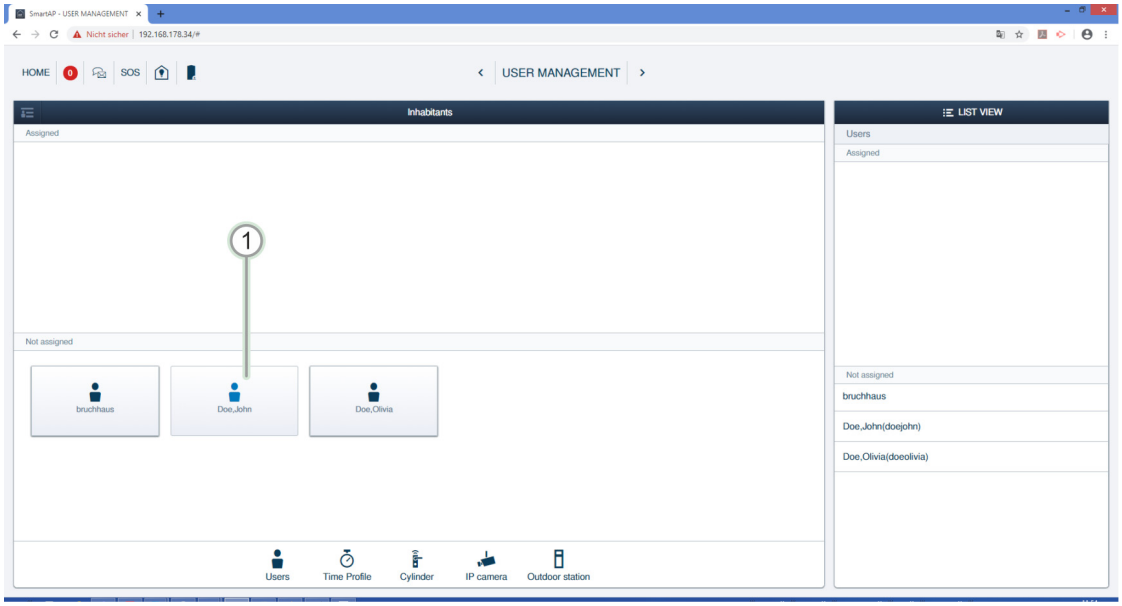


Fig. 138: User group: Adding users

8. To add a user, click on the available user [1] and confirm the selection.

5.5.3 Add authentication

The term "Authentication" includes all available transponder keys in the system and their allocation to the created users / user groups and "Electronic cylindrical lock".

For each transponder key in the system, an authentication must be created in the "Smart Access Point Pro".

To add an authentication, perform the following steps:

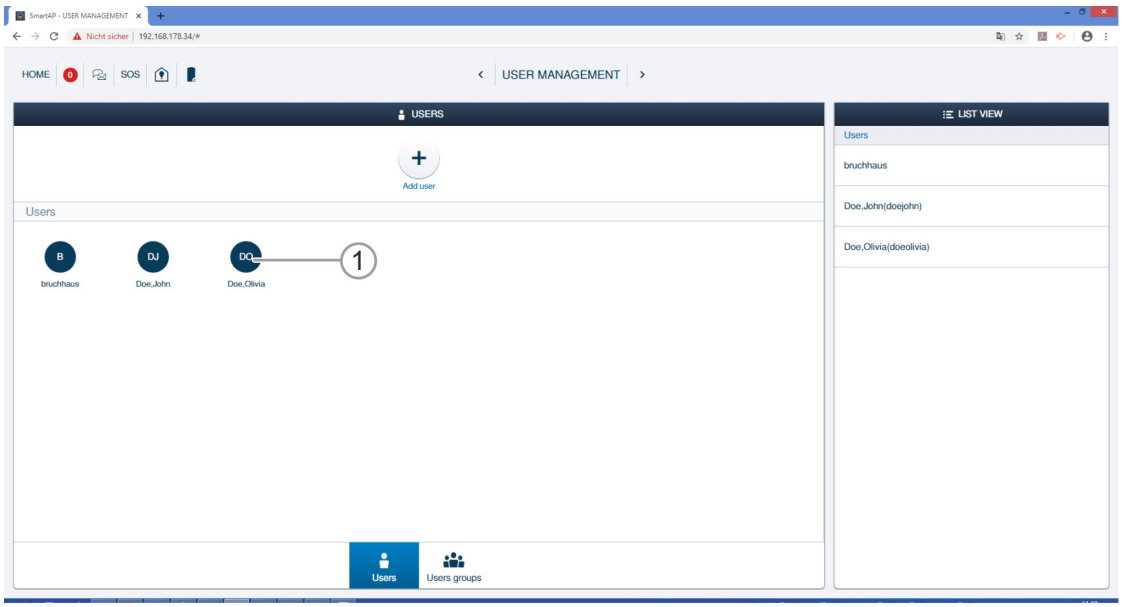


Fig. 139: Selecting user.

1. Select the desired user for the new transponder key in the list [1].

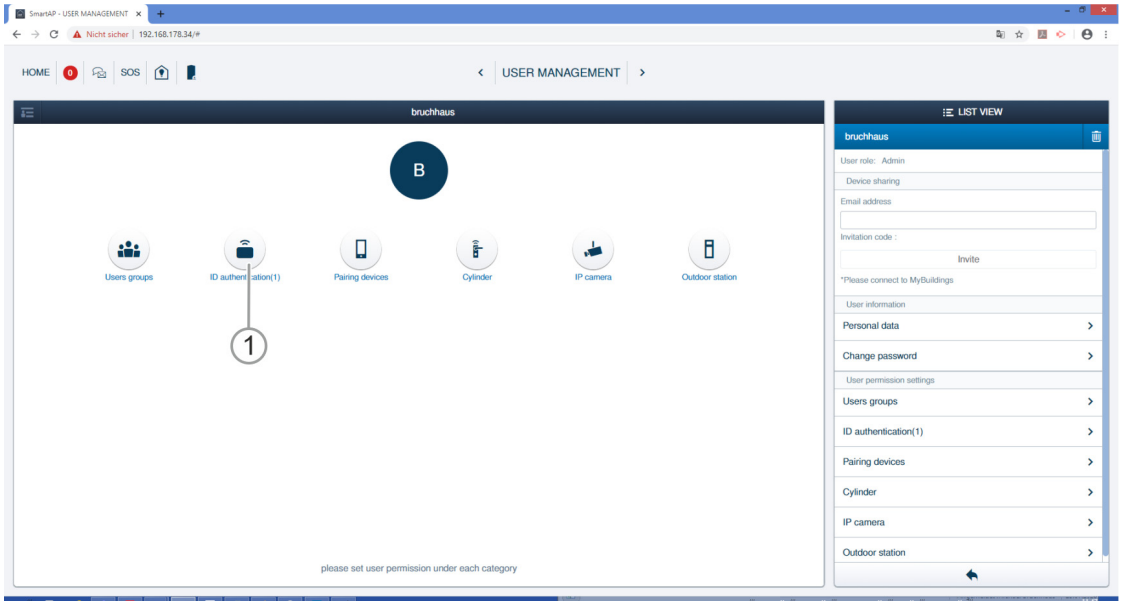


Fig. 140: Selecting the ID authentication

2. Click on the "ID authentication" button [1].

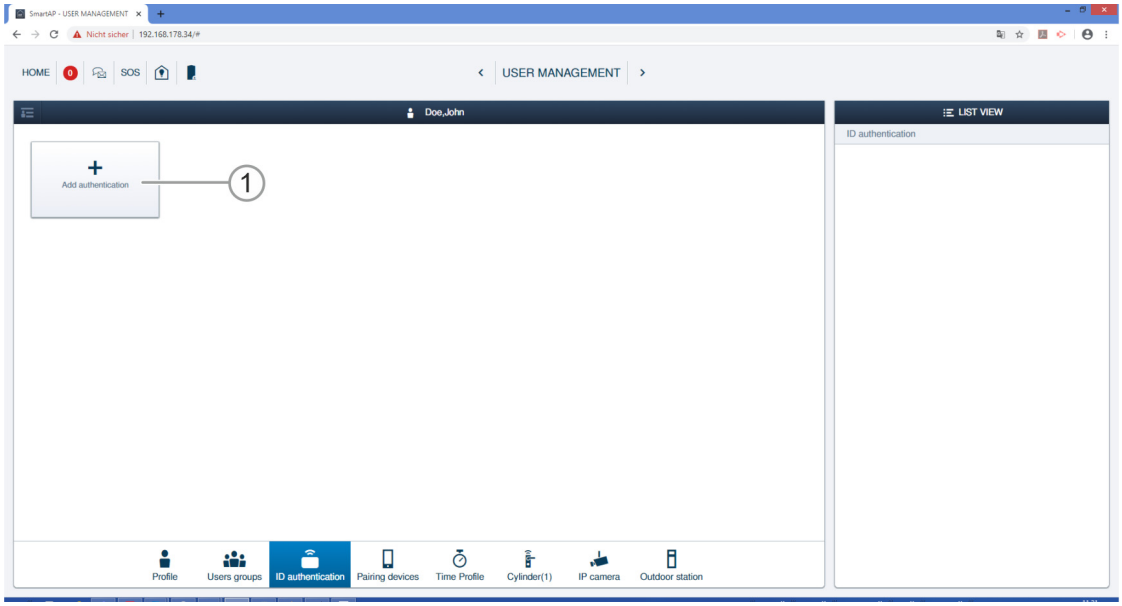


Fig. 141: Adding authentication

3. Click on the "Add authentication" button [1]

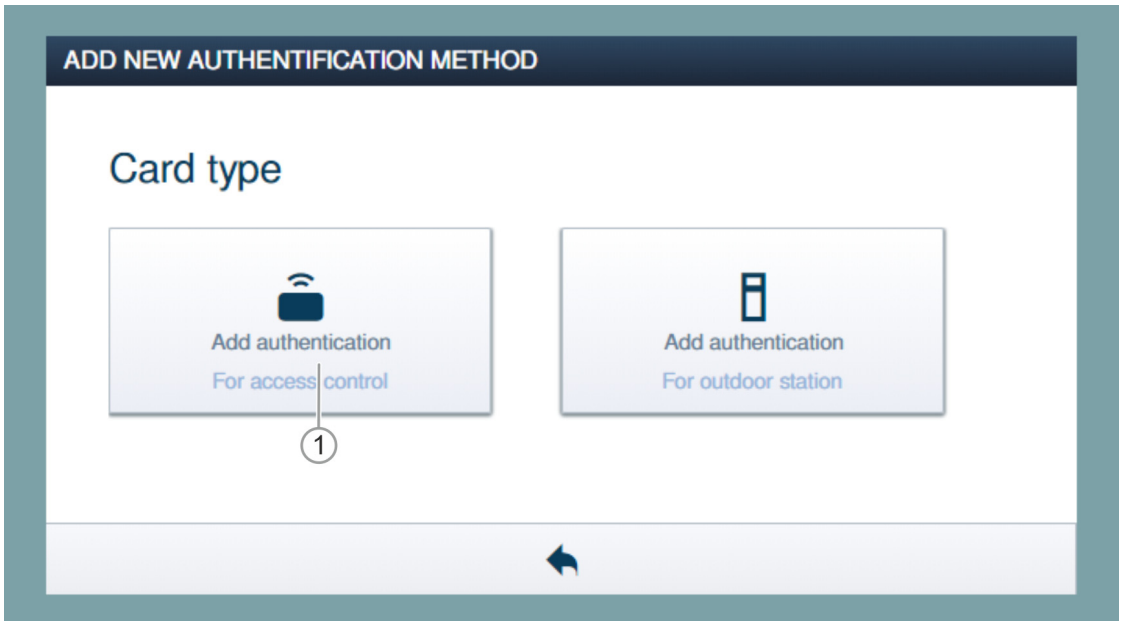


Fig. 142: "Add authentication for access control" button

4. Click on the "Add authentication for access control" button [1].

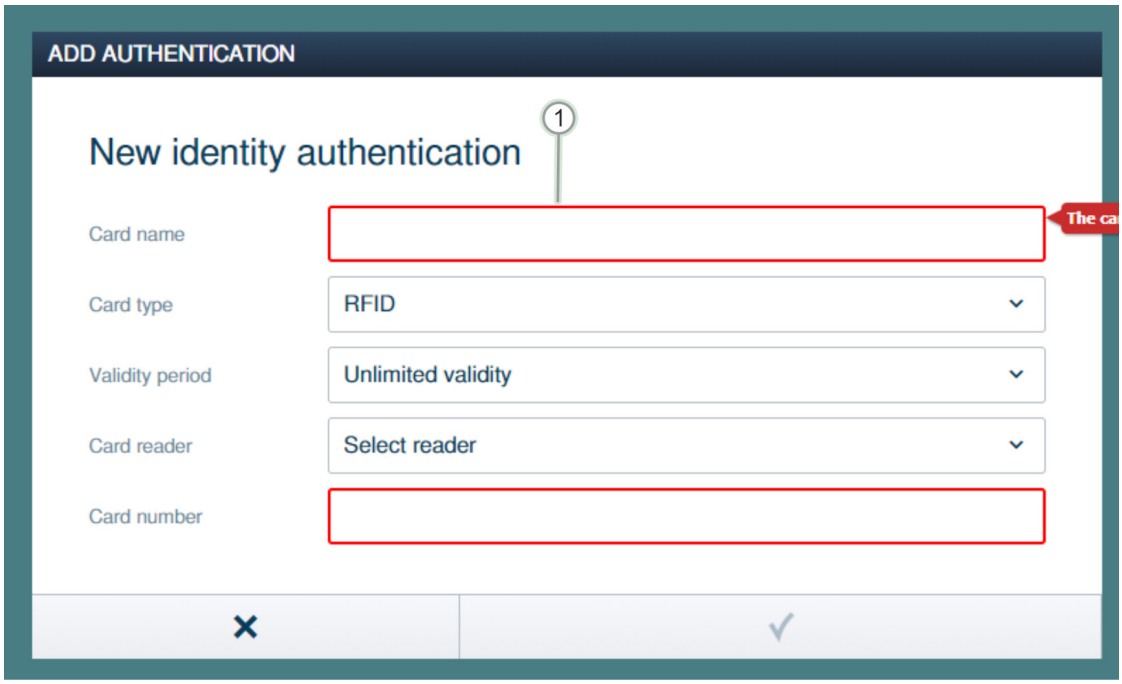


Fig. 143: New authentication

5. Enter a clearly identifiable name in field "Card name" [1] for the new transponder key.

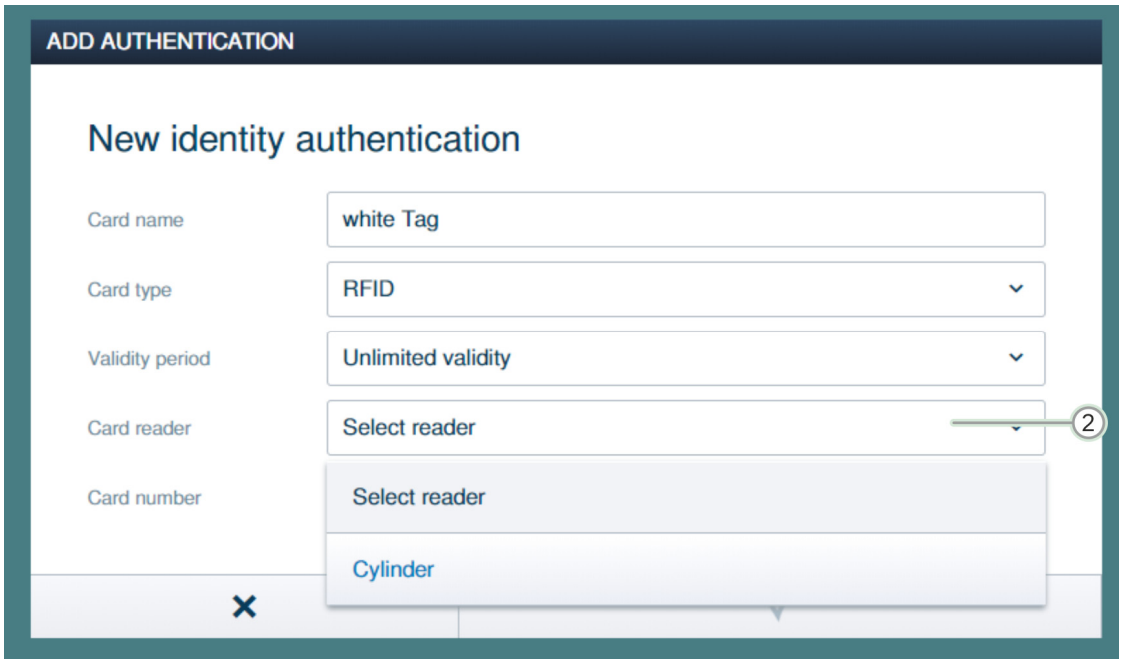


Fig. 144: Select "Electronic cylindrical lock"

6. Select any "Electronic cylindrical lock" in field "Card reading device" [2].
   – This selected "Electronic cylindrical lock" merely serves for reading the data of the transponder key into the management software. No locking rights are assigned.

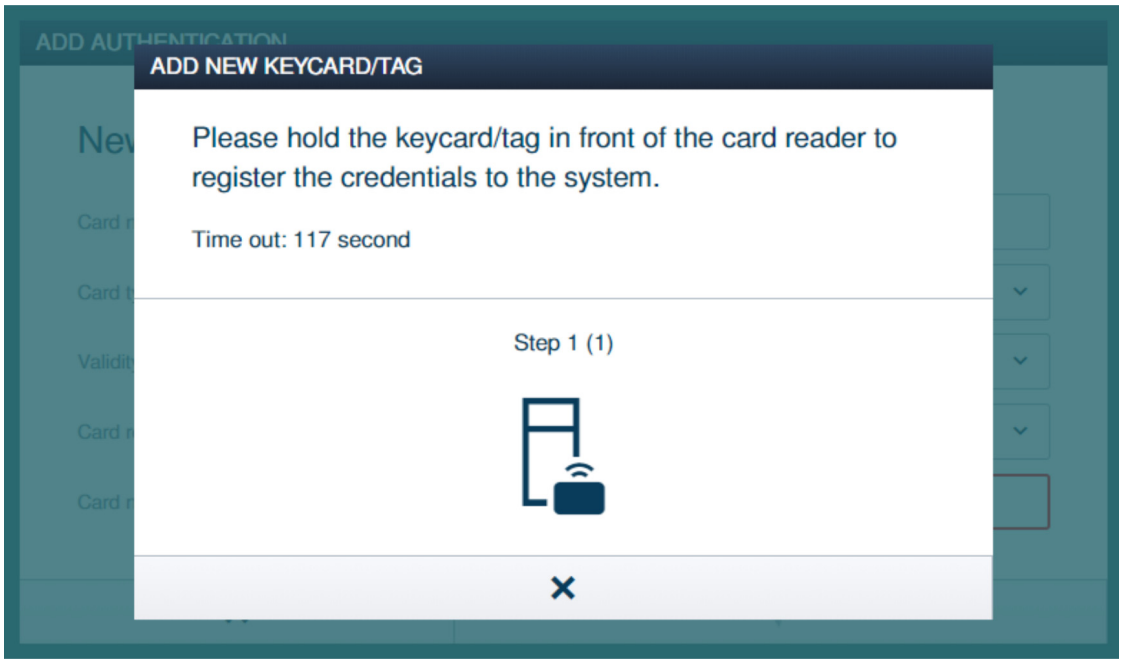


Fig. 145: Holding the transponder keys in front

7. Follow the instructions on the display and hold the transponder key in front of the selected "Electronic cylindrical lock".
   – The card number of the transponder key is automatically entered.
   – The transponder key of the user is now carried in the system.

Notice
Then the user must still be assigned the locking right for the desired "Electronic cylindrical lock".

5.5.4 Assigning locking rights

All created "Electronic cylindrical lock" are displayed in area "Not assigned" [1].

The user does not yet have locking rights. This locking right must now be assigned to him.

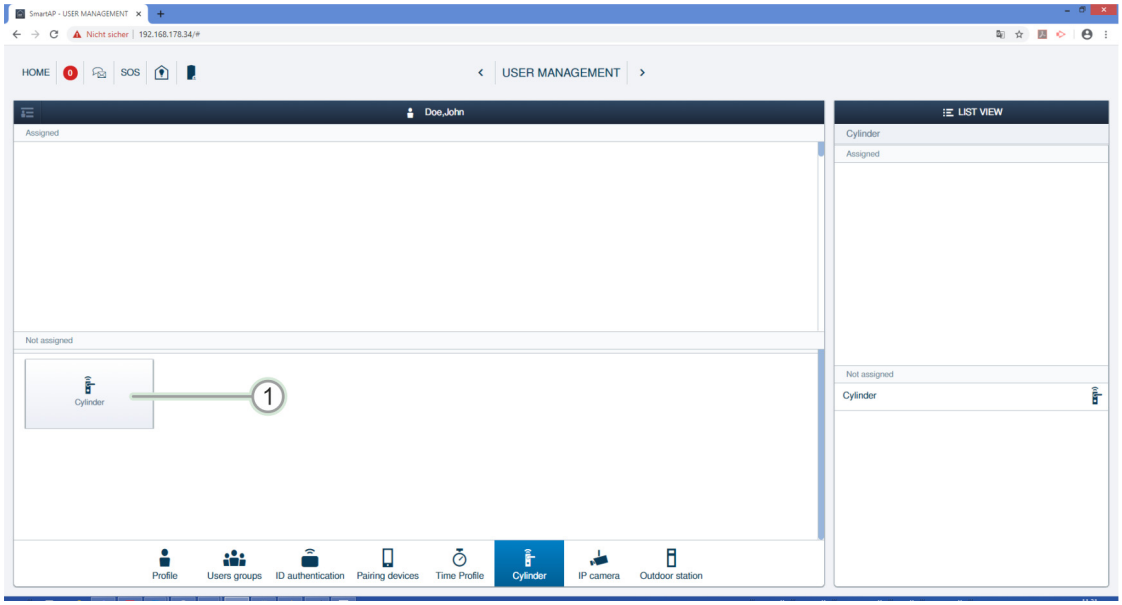


Fig. 146: "Electronic cylindrical lock" not assigned

Use the following steps to assign the user the locking right for the desired "Electronic cylindrical lock":

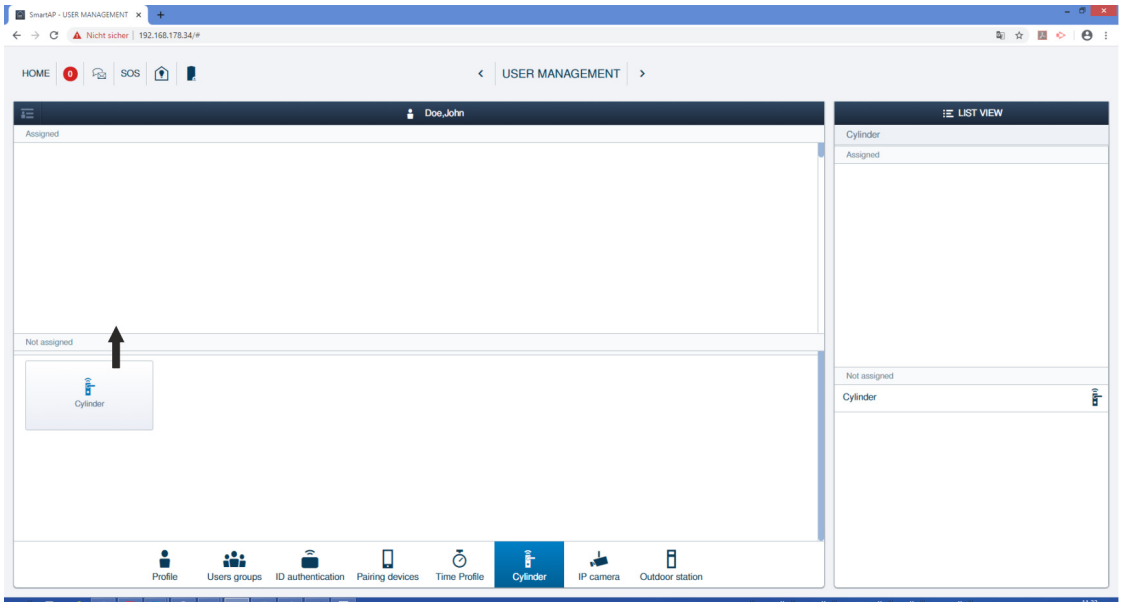


Fig. 147: Assigning locking right for "Electronic cylindrical lock"

1. Pull the "Electronic cylindrical lock" into the "Assigned" area via drag and drop.

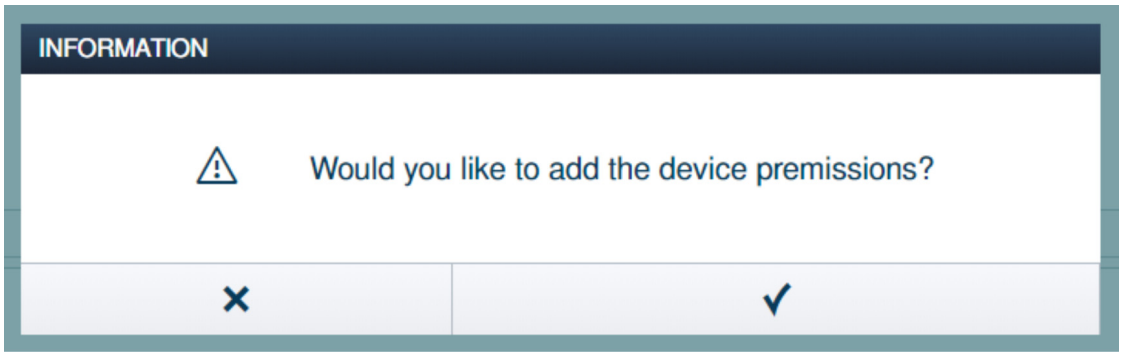


Fig. 148: "Device authorization" window

2. Confirm the question in the "Device authorization" window.

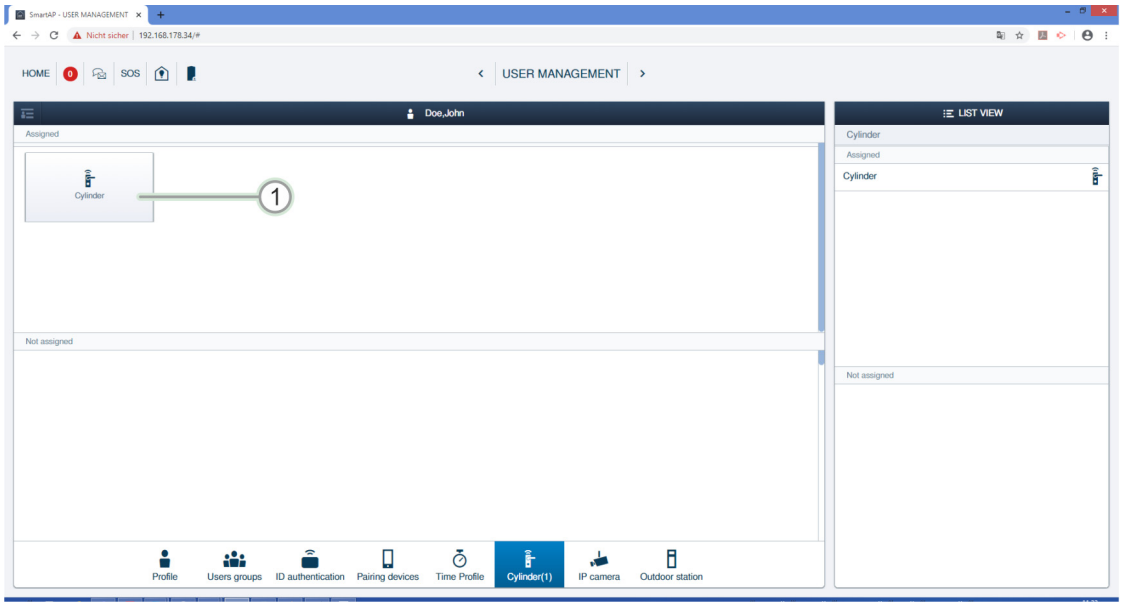


Fig. 149: "Electronic cylindrical lock" assigned

The "Electronic cylindrical lock" is displayed in the "Assigned" field [1].

– With his transponder key the user has the locking right to this "Electronic cylindrical lock".

Notice

If several transponder keys have been assigned to the user, the user automatically has the locking right with all transponder keys for the "Electronic cylindrical lock" that are displayed as assigned in field "Assigned".

Notice

If the user is to receive the locking right to several "Electronic cylindrical lock", repeat steps 1 and 2 in this chapter until all desired "Electronic cylindrical lock" are listed in field "Assigned".

5.6 Deleting data from the "User management menu

The deletion of the "Electronic cylindrical lock", transponder keys and locking rights is carried out via menu item "User management" [1] in the main menu of the "Smart Access Point Pro".

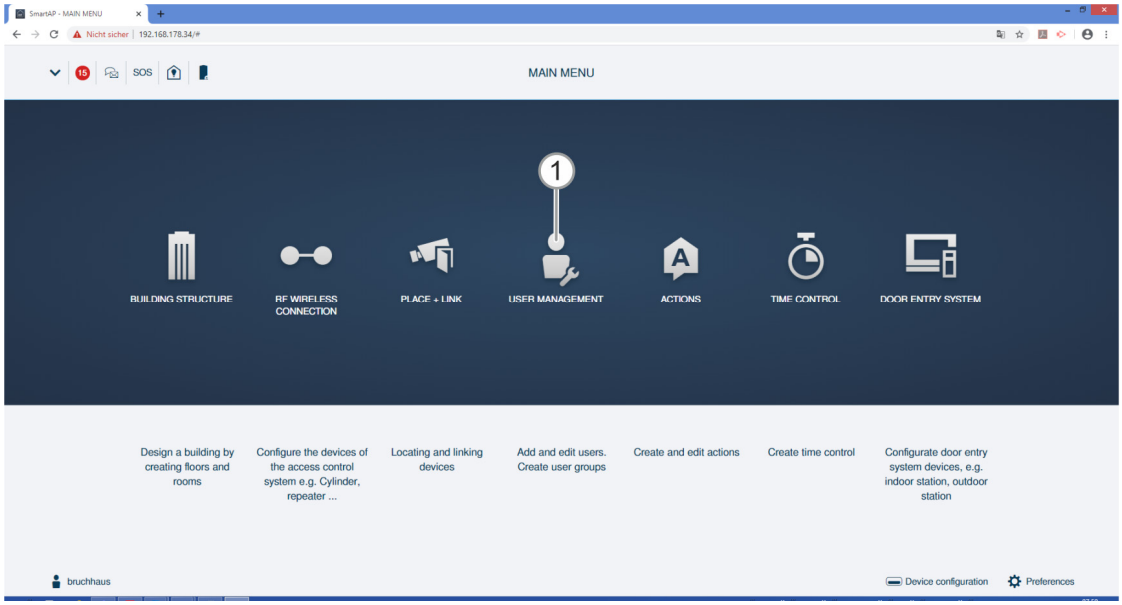


Fig. 150: Menu item "User management"

5.6.1 Deleting locking right

Use the following steps to delete a locking right:

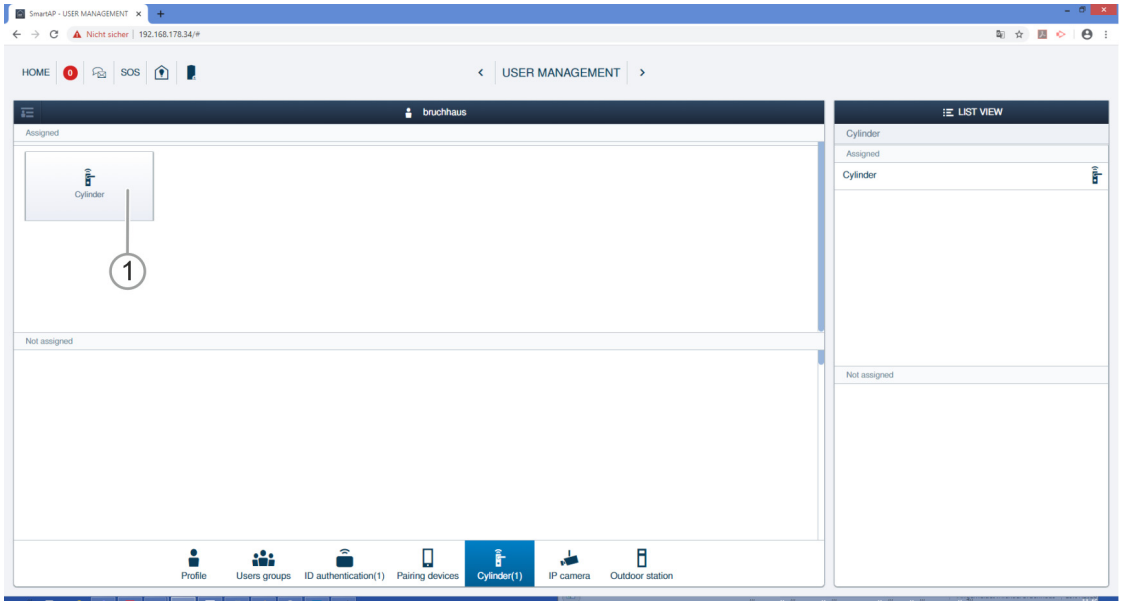


Fig. 151: "Electronic cylindrical lock" assigned

1. Click on the desired "Electronic cylindrical lock" [1].

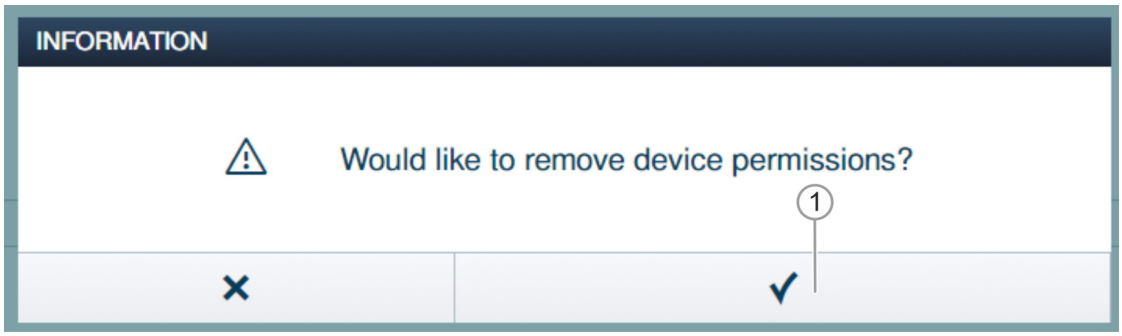


Fig. 152: Confirming the withdrawal of locking rights

2. Confirm the question with button [1].
   – The locking right for this "Electronic cylindrical lock" has been withdrawn.

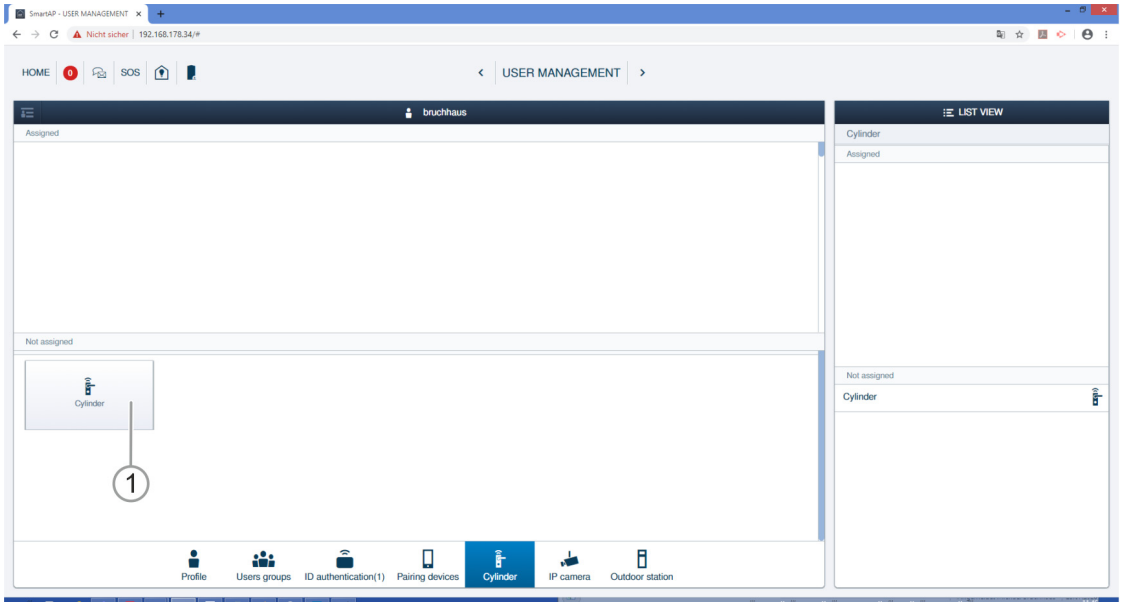


Fig. 153: "Electronic cylindrical lock" not assigned

The "Electronic cylindrical lock" is displayed in the "Not assigned" area [1].

5.6.2 Deleting authentication

To delete an authentication (= a transponder key), perform the following steps:

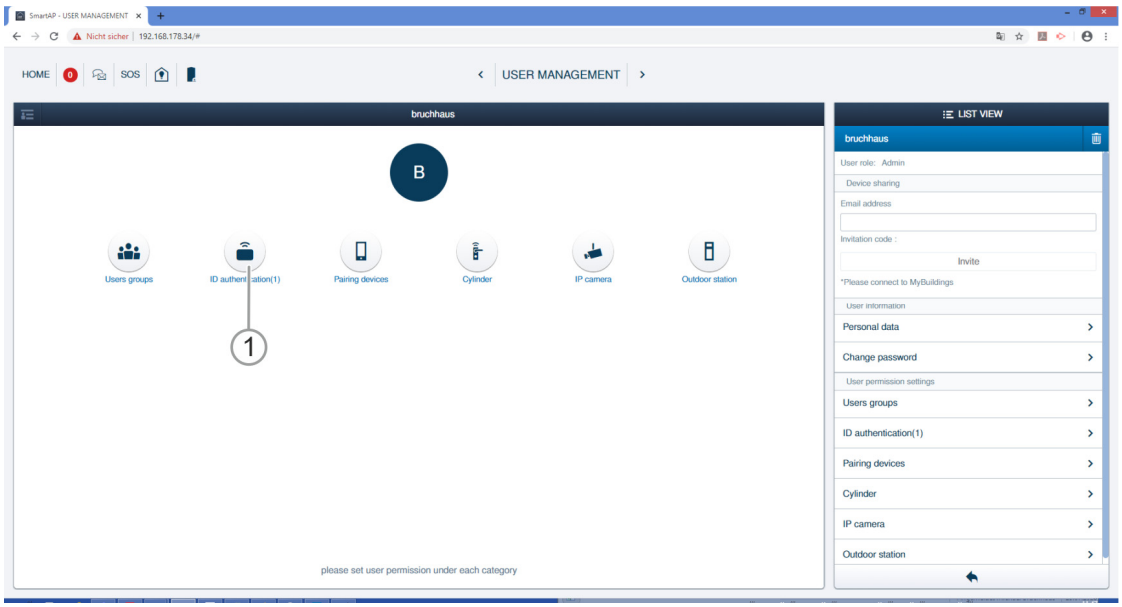


Fig. 154: ID authentication

1. Click on the "ID authentication" button [1].
   – All authentications of the user are displayed.

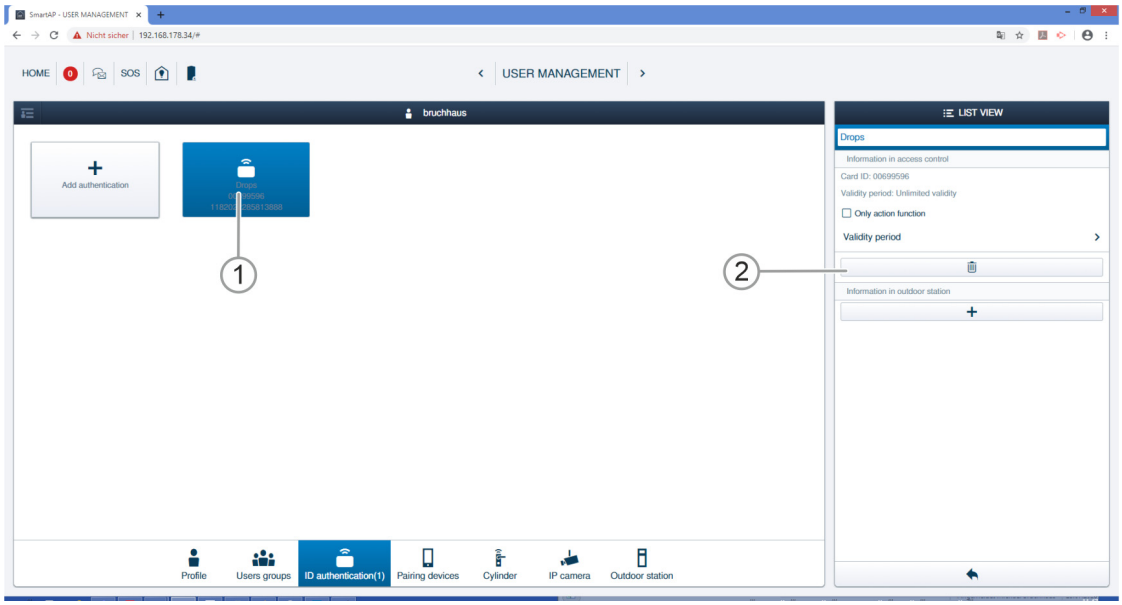


Fig. 155: Deleting authentication

2. Click on the desired authentication [1].
3. Click on the "Delete" button [2].

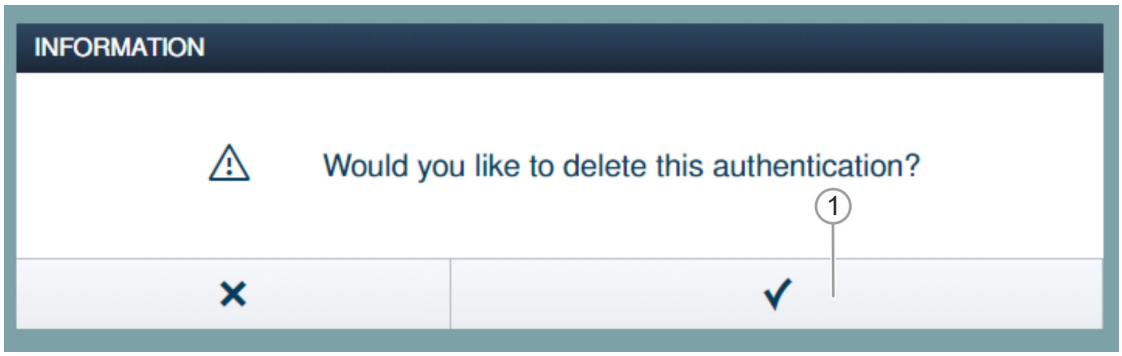


Fig. 156: Confirming the deletion of the authentication

4. Confirm the question with button [1].
   – The authentication is deleted.

5.6.3 Delete users

To delete a user, perform the following steps:

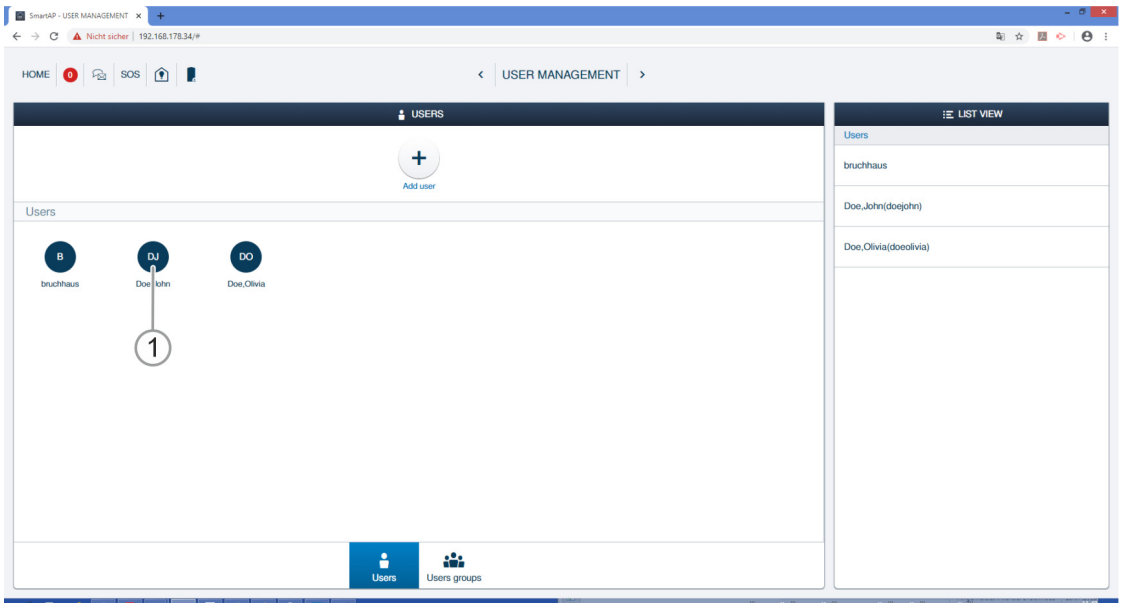


Fig. 157: Marking the user

1. Click on the username [1].

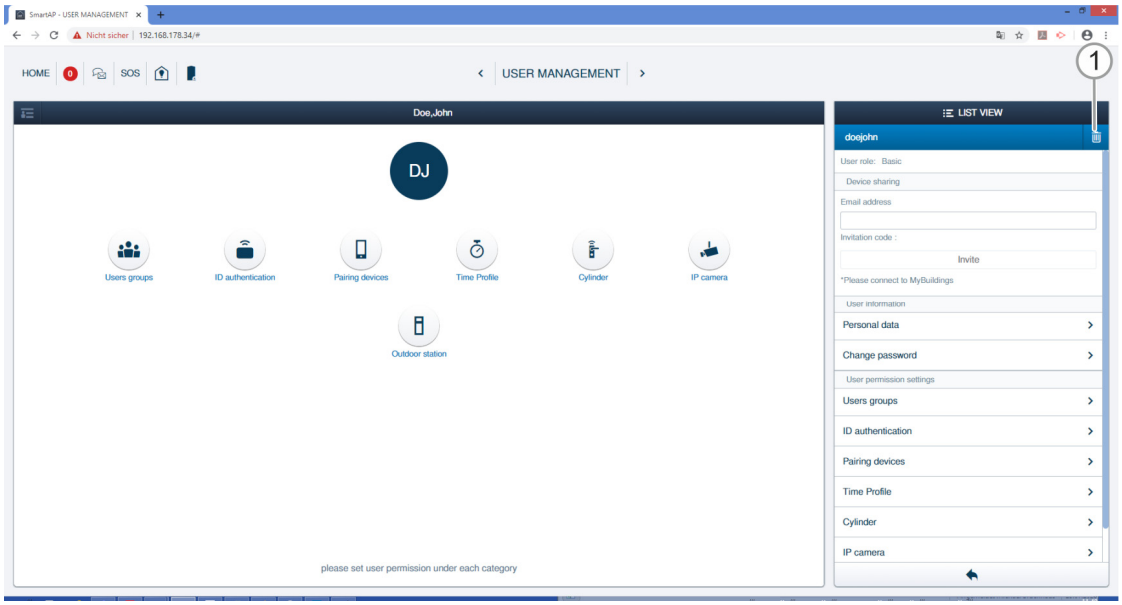


Fig. 158: Deleting the user

2. Click on the "Delete" button [1].

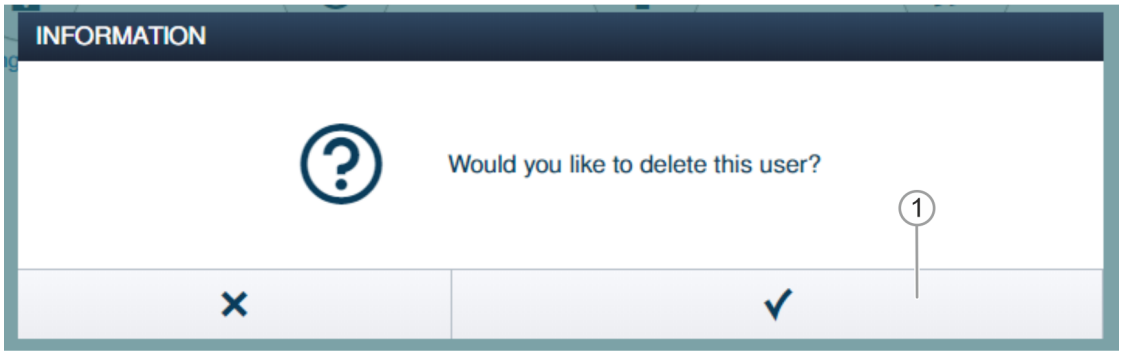


Fig. 159: Confirming the deletion of the user

3. Confirm the question with button [1].
   – The user is deleted.

5.7 Deleting data from the "Access control" menu

The uncoupling and removal of devices from the individual rooms and floors is carried out via menu item "Access control" in the main menu of the "Smart Access Point Pro".

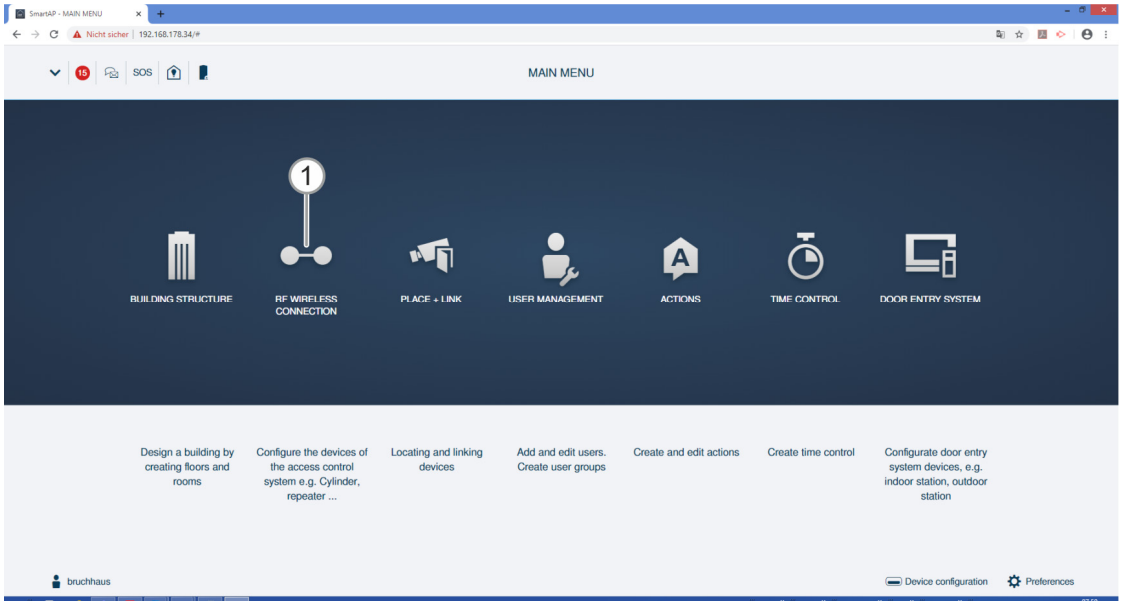


Fig. 160: Menu "Access control"

5.7.1 Uncoupling "Electronic cylindrical lock" from "Smart Access Point Pro"

Use the following steps to uncouple the "Electronic cylindrical lock" from the "Smart Access Point Pro":

Fig. 161: Marking the coupling

1. Search for the "Electronic cylindrical lock" [1] in the building structure and mark it.
2. Mark the "Smart Access Point Pro" [2].

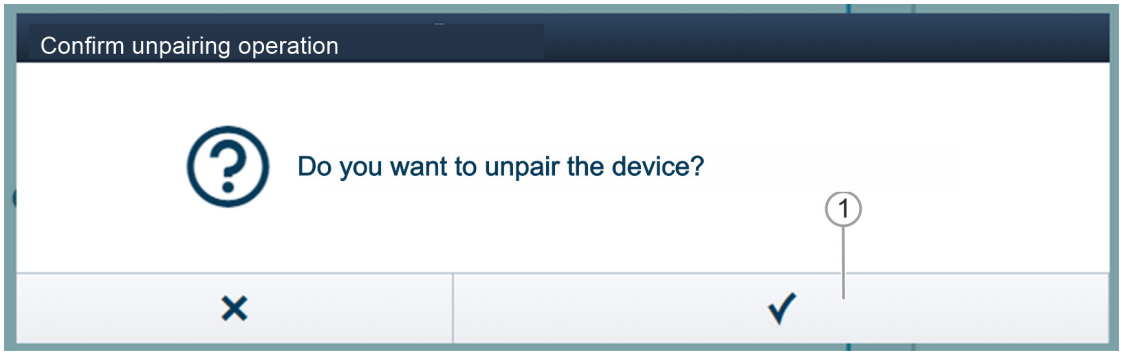


Fig. 162: Confirming the uncoupling process

3. Confirm the question with button [1].

Fig. 163: Uncoupling process 1

4. Follow the instructions and confirm with button [1].

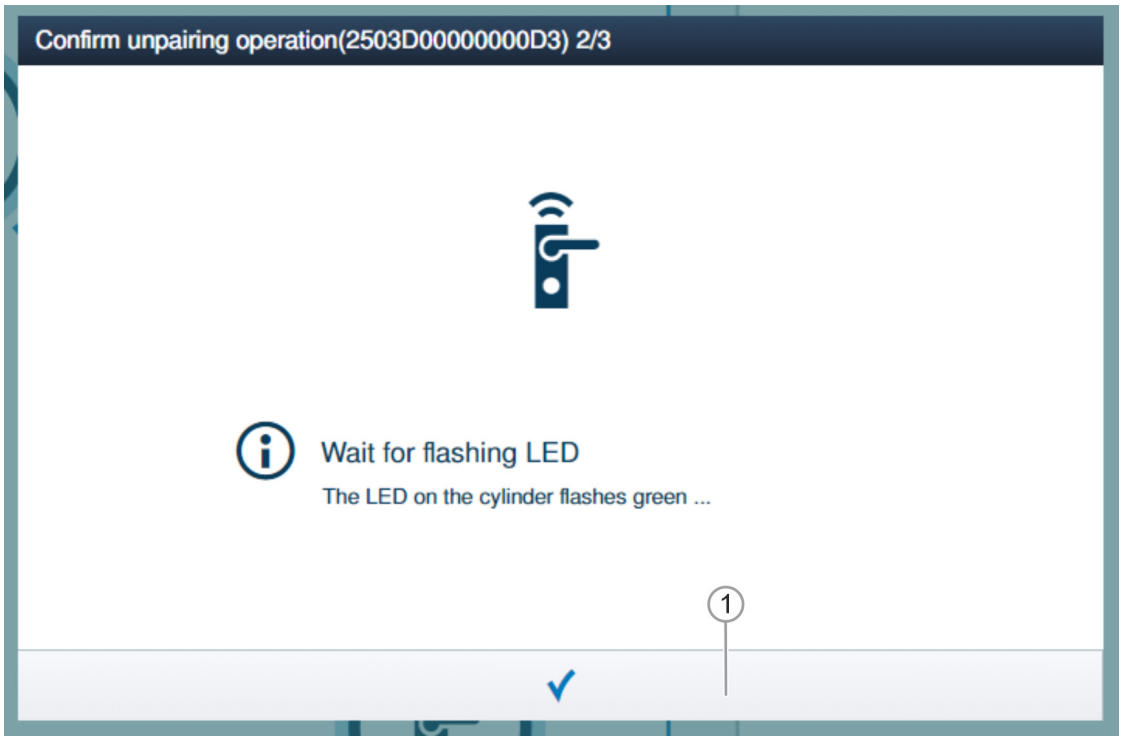


Fig. 164: Uncoupling process 2

5. Follow the instructions and confirm with button [1].

Fig. 165: Uncoupling process 3

6. Follow the instructions and confirm with button [1].

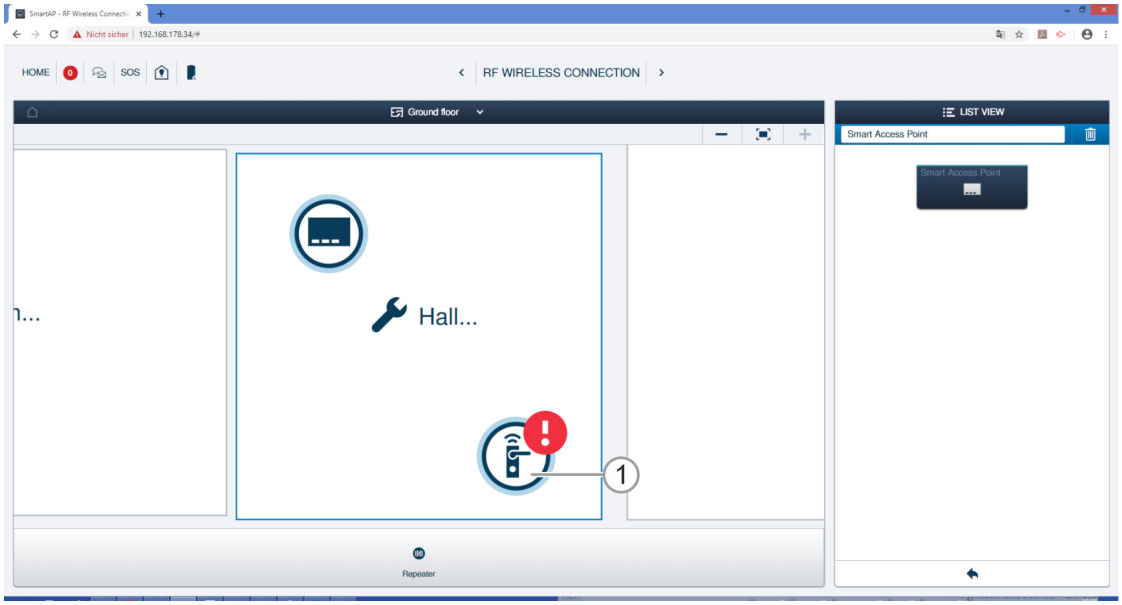


Fig. 166: The "Electronic cylindrical lock" is uncoupled

The "Electronic cylindrical lock" and the "Smart Access Point Pro" have been uncoupled. The icon "!" on the "Electronic cylindrical lock" [1] shows that the two devices are no longer connected.

5.7.2 Removing the "Electronic cylindrical lock" from the room

Use the following steps to remove the "Electronic cylindrical lock":

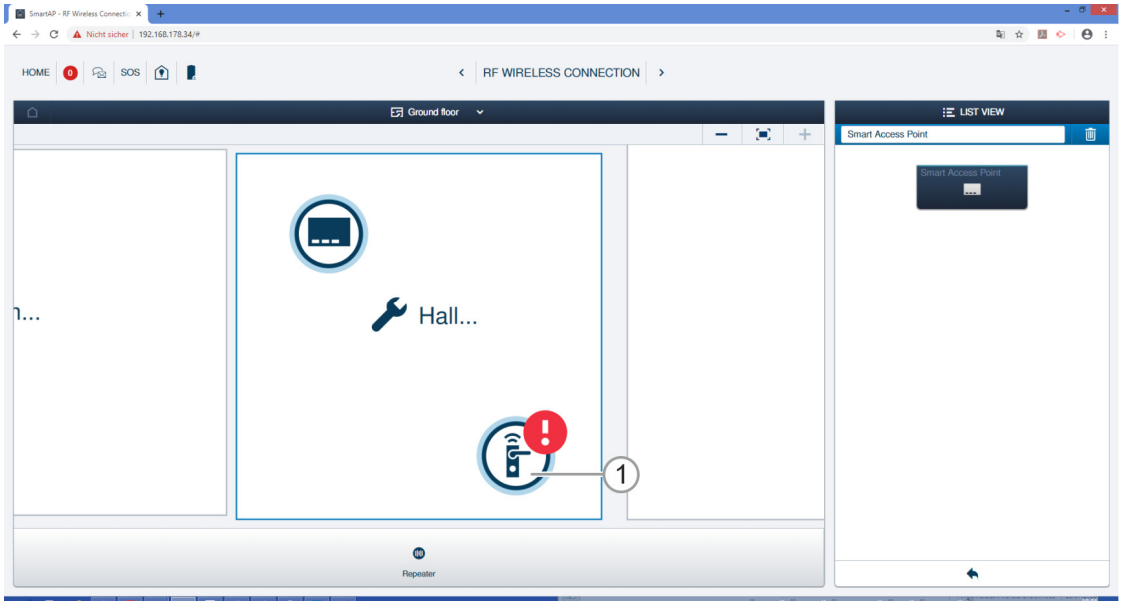


Fig. 167: Removing "Electronic cylindrical lock" from the building structure

1. Search for "Electronic cylindrical lock" [1] in the building structure and mark it.
2. Click on the "Delete" button [2].
   – The "Electronic cylindrical lock" will be removed from the room.

5.7.3 Removing the "Smart Access Point Pro" from the room

Use the following steps to remove a "Smart Access Point Pro":

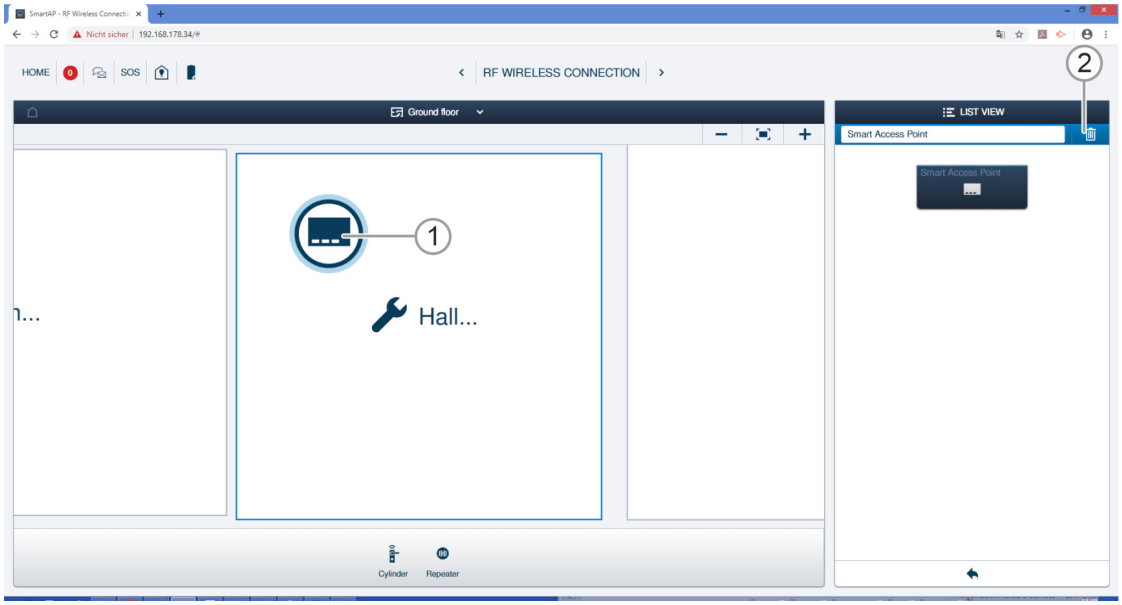


Fig. 168: Marking the "Smart Access Point Pro"

1. Search for the "Smart Access Point Pro" [1] in the building structure and mark it.
2. Click on the "Delete" button [2].
   – The "Smart Access Point Pro" has been deleted from the room.

5.7.4 Uncoupling the "RF Repeater" Fehler! Textmarke nicht definiert.

Use the following steps to uncouple the "RF Repeater" from the "Smart Access Point Pro":

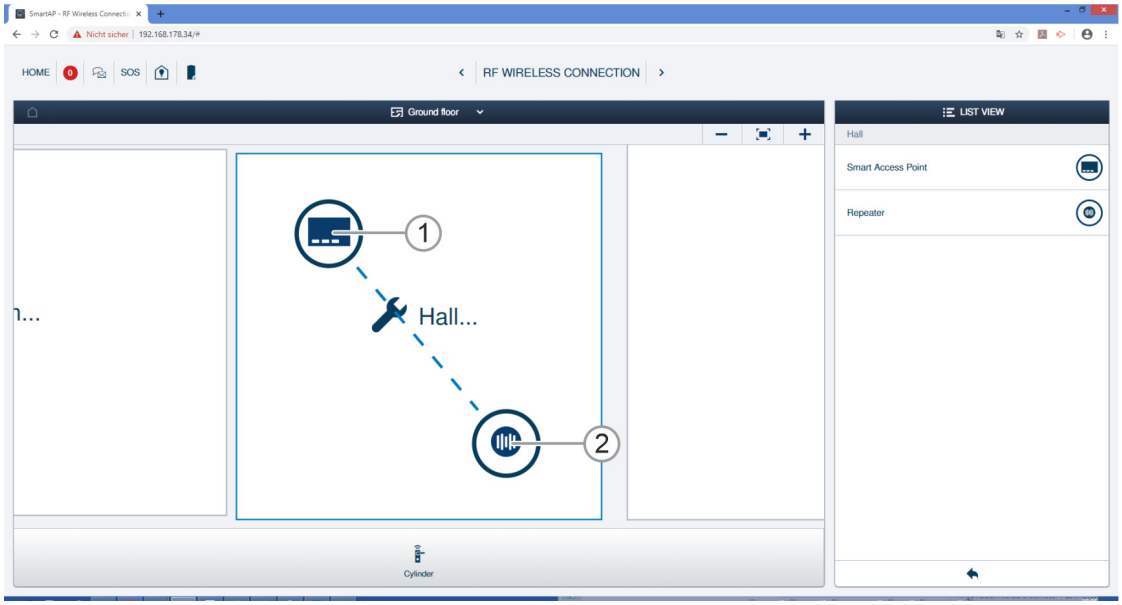


Fig. 169: Marking the coupling

3. Search for the "RF Repeater" [1] in the building structure and mark it.
4. Mark the "Smart Access Point Pro" [2].

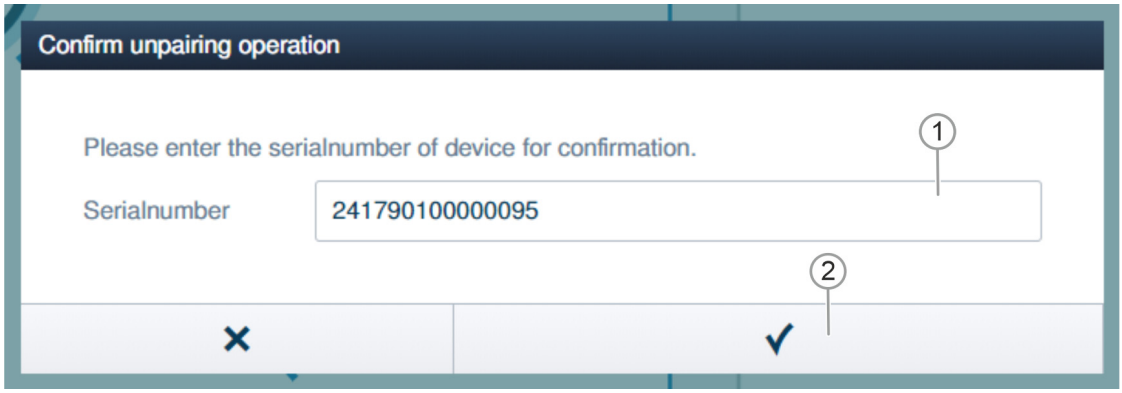


Fig. 170: Confirming the uncoupling process

5. Confirm the uncoupling process with the entry of the "RF Repeater" serial number [1].
6. Click on button [2].

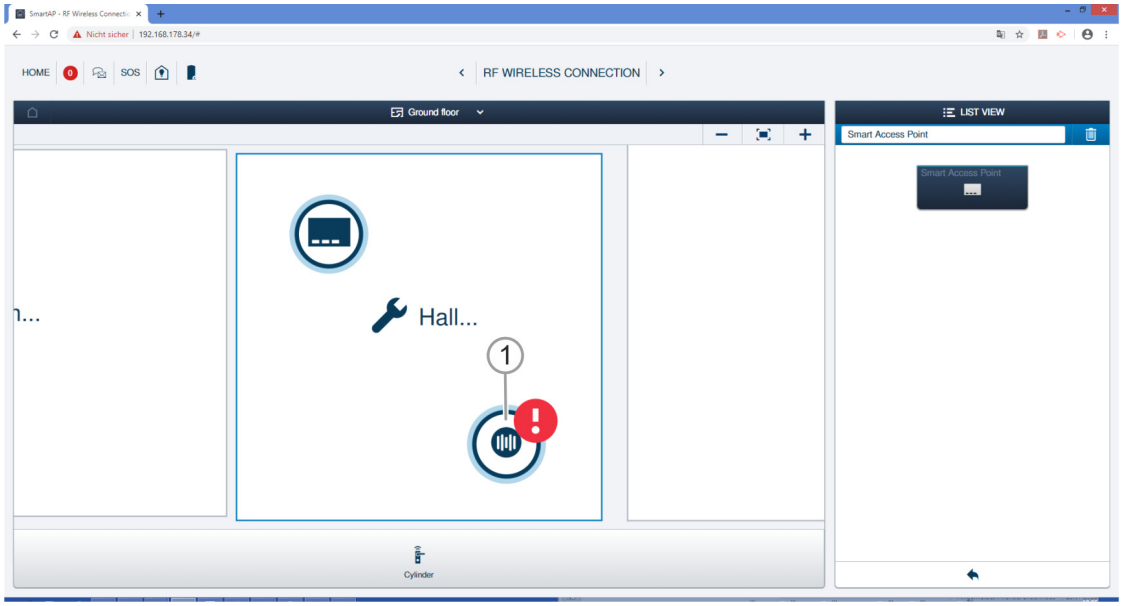


Fig. 171: The "RF Repeater" is uncoupled

The "RF Repeater" [1] and the "Smart Access Point Pro" have been uncoupled. The icon "!" on the "RF Repeater" [1] shows that the two devices are no longer connected.

5.7.5 Removing the "RF Repeater" from the room

Use the following steps to remove a "RF Repeater":

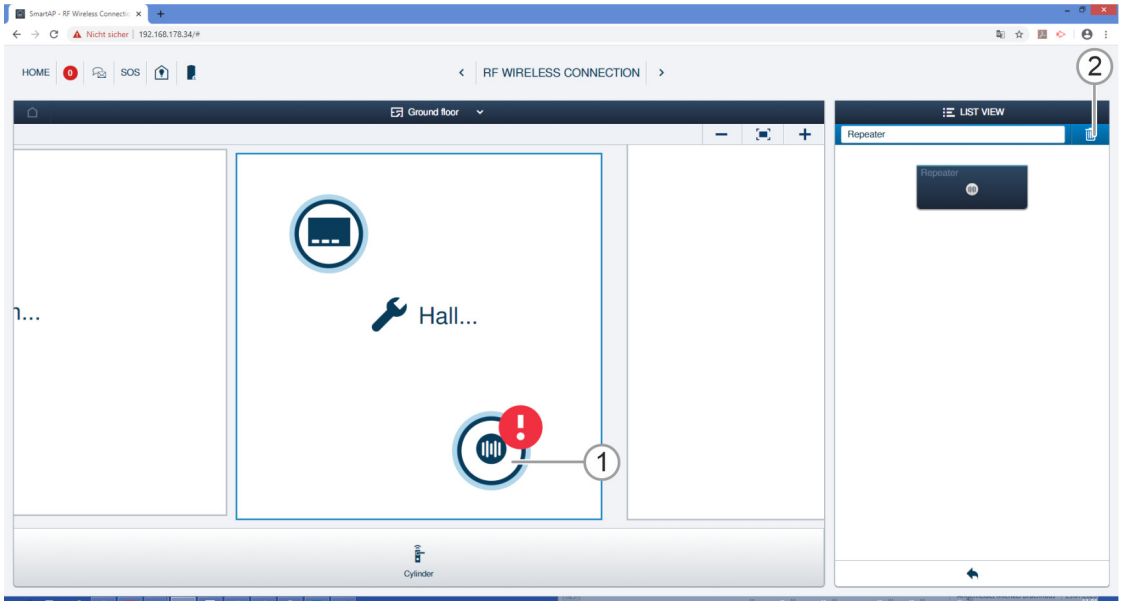


Fig. 172: Marking the "RF Repeater"

1. Search for the "RF Repeater" [1] in the building structure and mark it.
2. Click on the "Delete" button [2].
   – The "RF Repeater" has been deleted from the room.

5.8 Deleting data from the "Device configuration" menu

Devices are deleted from the system via menu item "Device configuration" [1] in the main menu of the "Smart Access Point Pro".

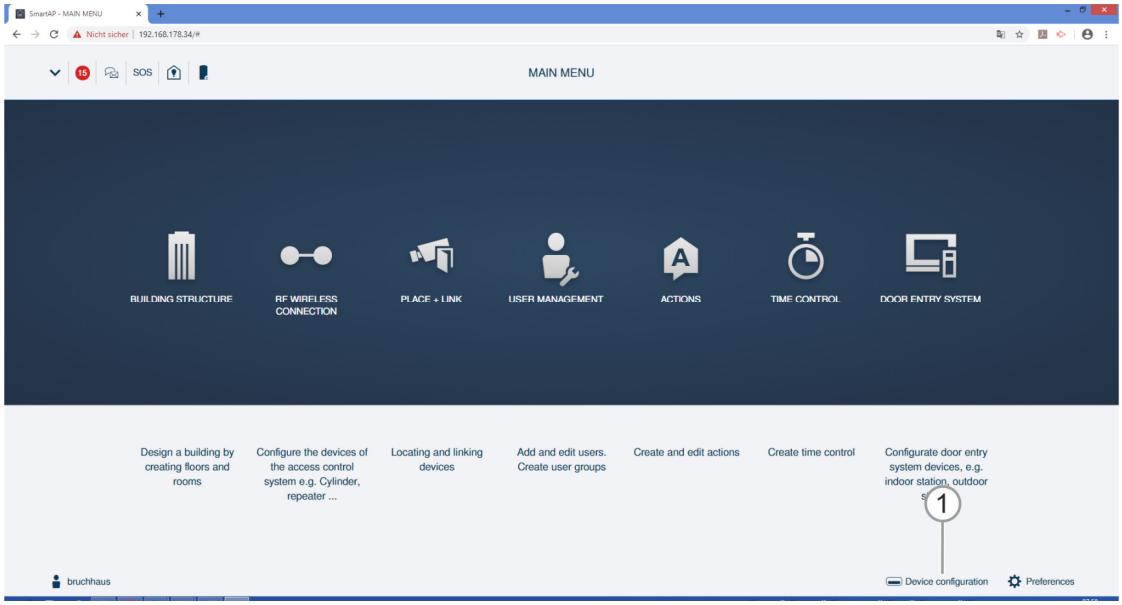


Fig. 173: Menu "Device configuration"

5.8.1 Deleting the "Electronic cylindrical lock" from the system

Use the following steps to delete the "Electronic cylindrical lock":

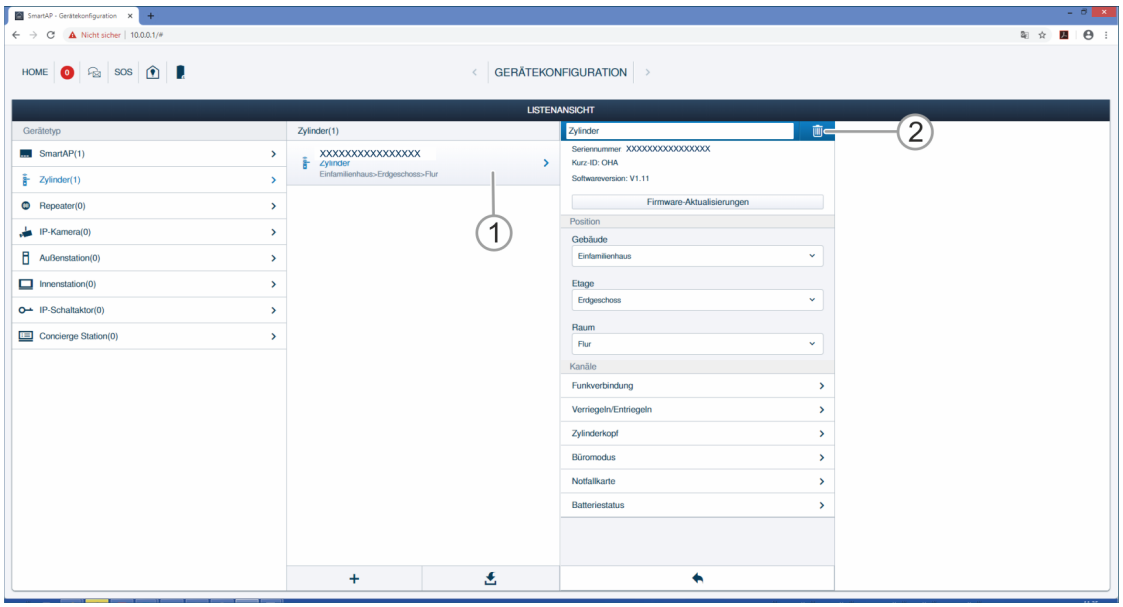


Fig. 174: Deleting the "Electronic cylindrical lock"

1. Mark the "Electronic cylindrical lock" [1].
2. Click on the "Delete" button [2].

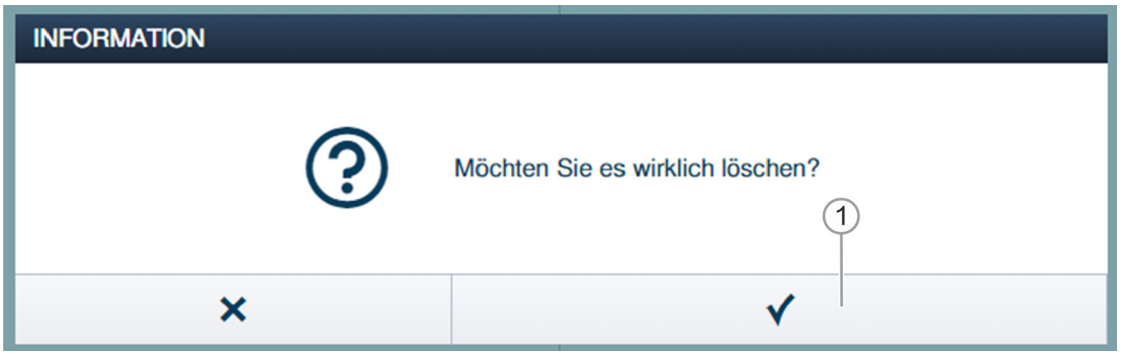


Fig. 175: Confirming the deletion of the "Electronic cylindrical lock"

3. Confirm the question with button [1].
   – The "Electronic cylindrical lock "is deleted.

5.8.2 Deleting the "RF Repeater" from the system

Use the following steps to delete a "RF Repeater":

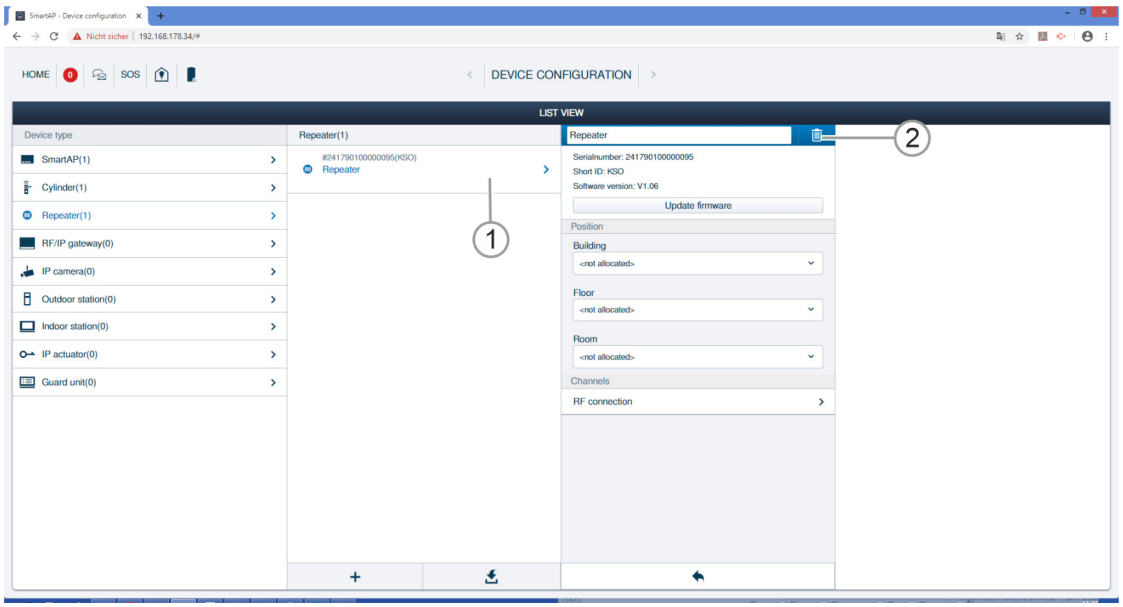


Fig. 176: Deleting the "RF Repeater" from the system

1. Mark the "RF Repeater" [1].
2. Click on the "Delete" button [2].

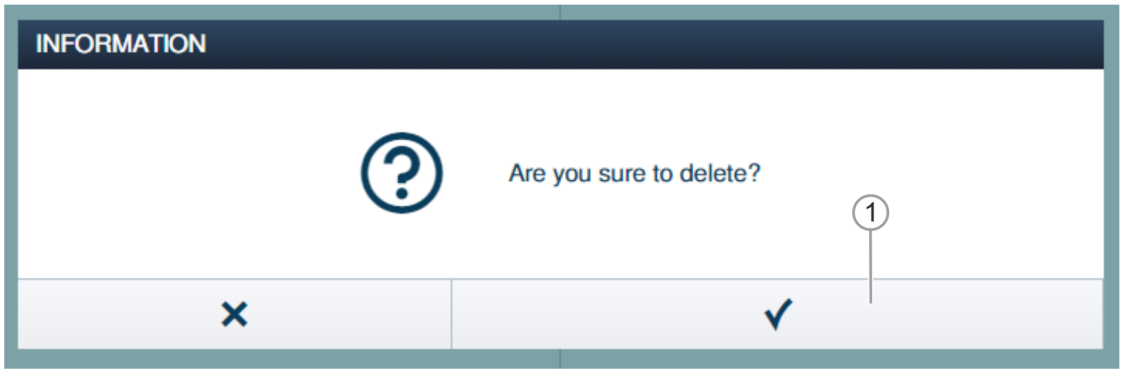


Fig. 177: Confirming the deletion of the "RF Repeater"

3. Confirm the question with button [1].
   – The "RF Repeater "is deleted.

5.8.1 Deleting the "RF/IP Gateway" from the system

Use the following steps to delete a "RF/IP Gateway":

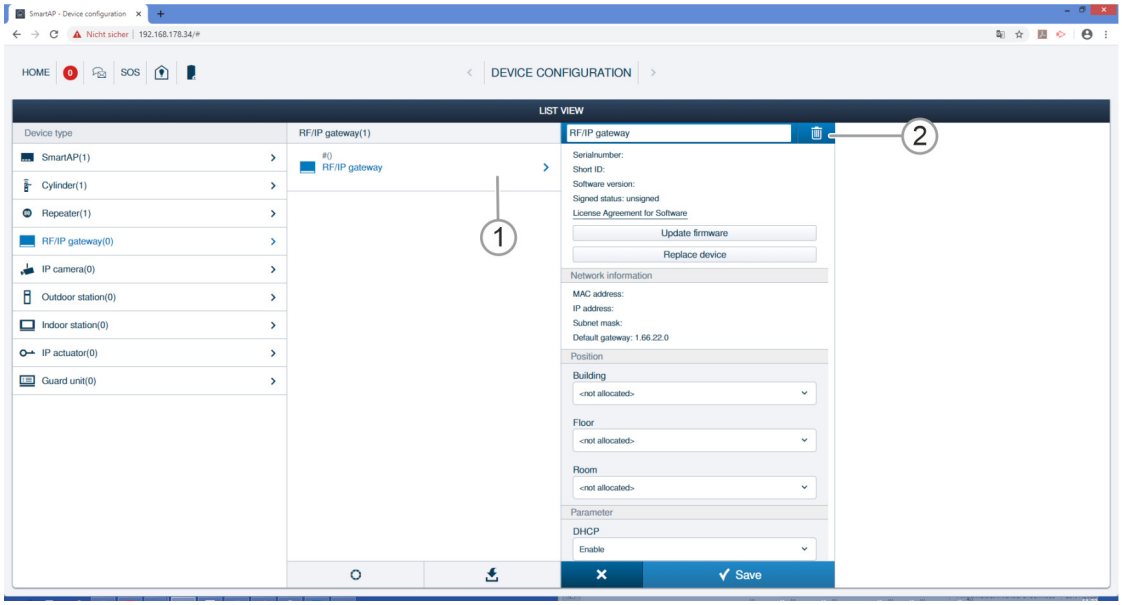


Fig. 178: Deleting the "RF/IP Gateway" from the system

1. Mark the "RF/IP Gateway" [1].
2. Click on the "Delete" button [2].

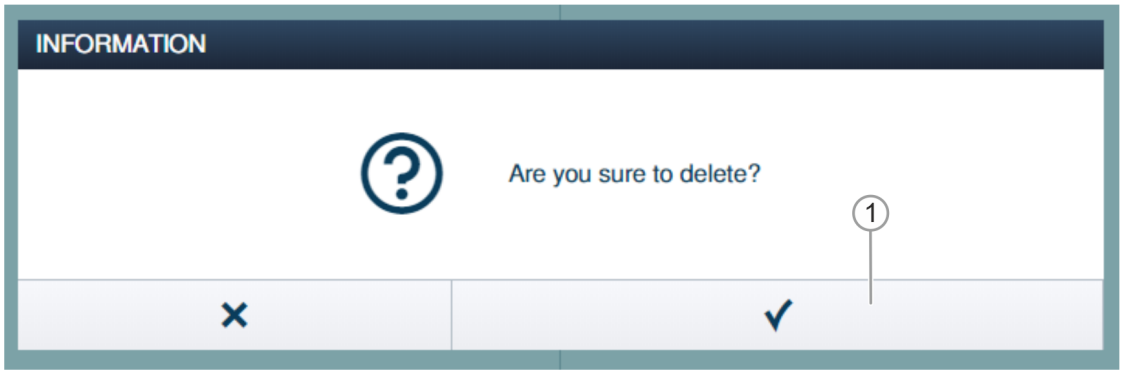


Fig. 179: Confirming the deletion of the "RF/IP Gateway"

3. Confirm the question with button [1].
   – The "RF/IP Gateway "is deleted.

5.9 Deleting data from the "Building structure" menu

The buildings, floors and rooms are deleted via menu item "Building structure" [1] in the main menu of the "Smart Access Point Pro".

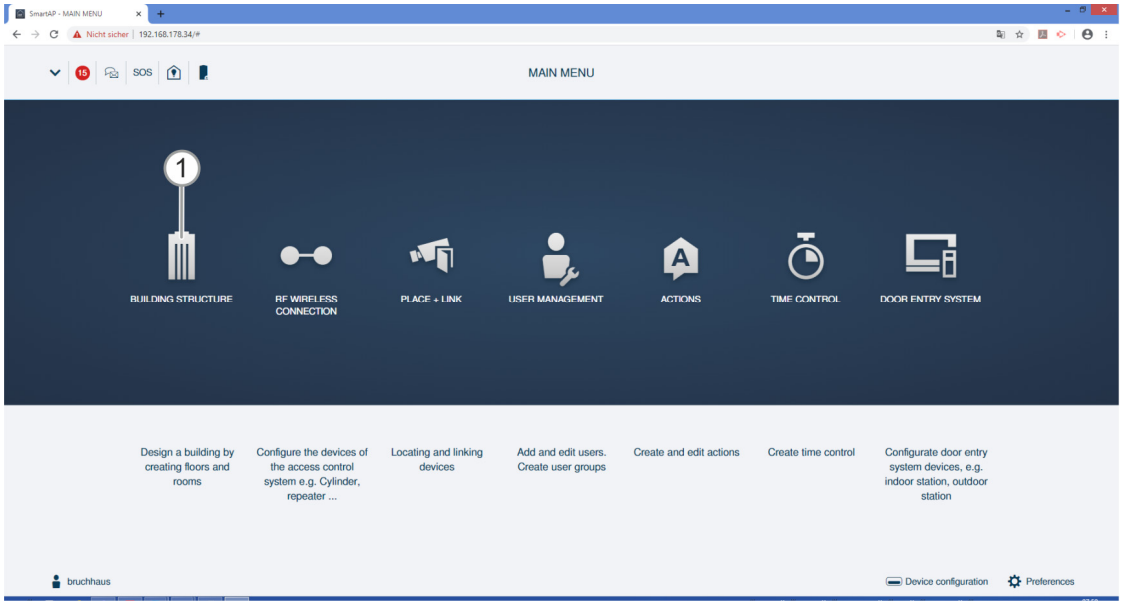


Fig. 180: "Building structure" menu

5.9.1 Deleting rooms

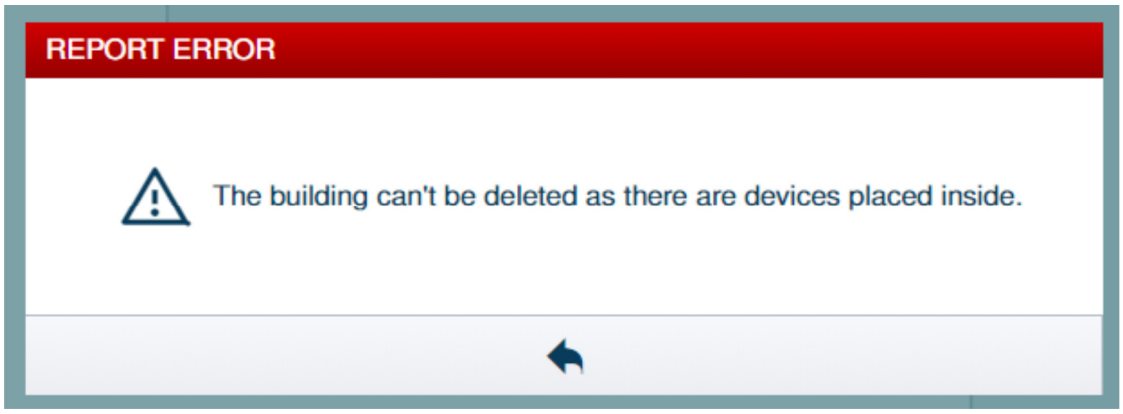


Fig. 181: Warning message

Notice

A room can only be deleted if it contains no devices.

– Delete all devices of the room before deleting the room, see chapter 5.8 “Deleting data from the "Device configuration" menu“ on page 161

Use the following steps to delete rooms:

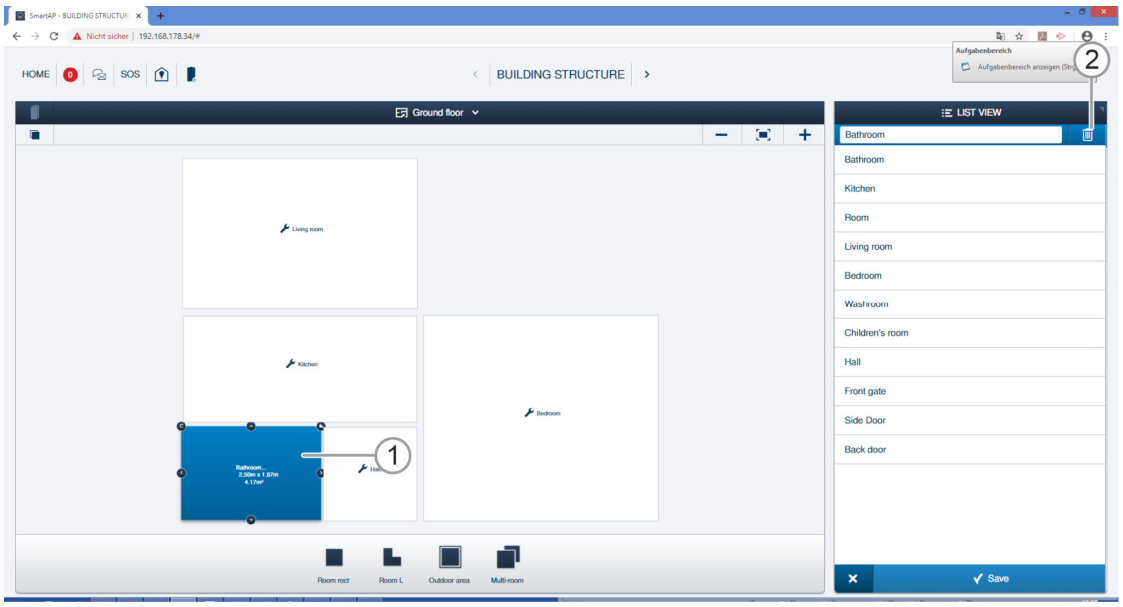


Fig. 182: Delete room

1. Search for the room [1] in the building structure and mark it.
2. Click on the "Delete" button [2].
   – The room is deleted.
3. Repeat the step until all desired rooms have been deleted.

5.9.2 Delete floors

Notice

A floor can only be deleted if it contains no rooms.

– Delete all rooms on the floor before deleting the floor, see chapter 5.9.1 “Deleting rooms“ on page 166

Use the following steps to delete floors:

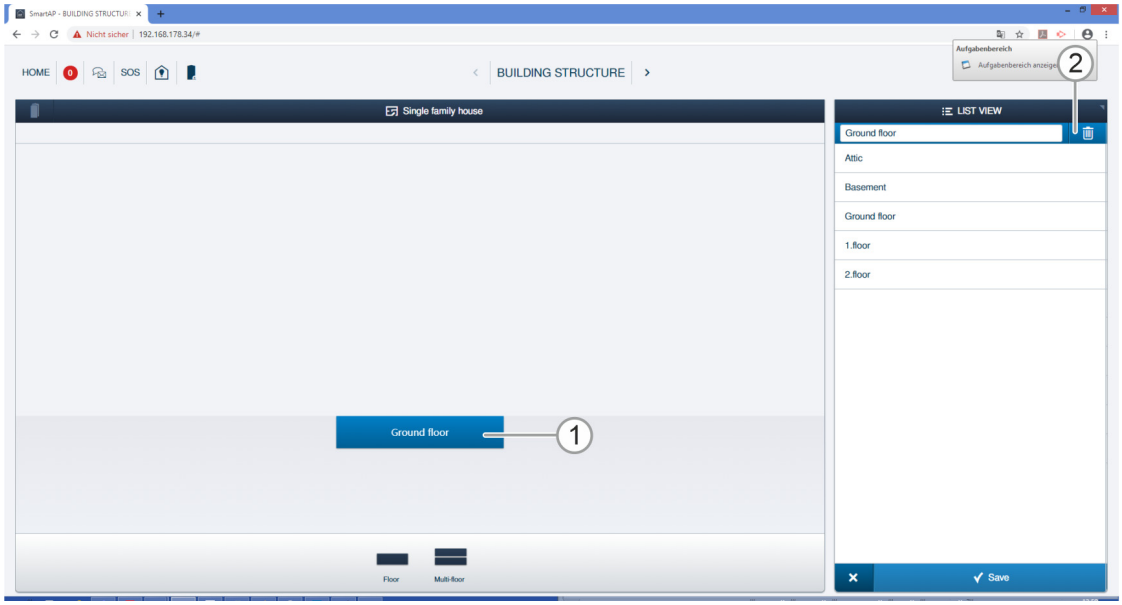


Fig. 183: Delete floor

1. Search for the floor [1] in the building structure and mark it.
2. Click on the "Delete" button [2].
   – The floor is deleted.
3. Repeat the step until all desired floors have been deleted.

5.9.3 Delete buildings

Notice

A building can only be deleted if it contains no floors.

– Delete all floors of the building before deleting the building, see chapter 5.9.2 “Delete floors“ on page 167

Use the following steps to delete buildings:

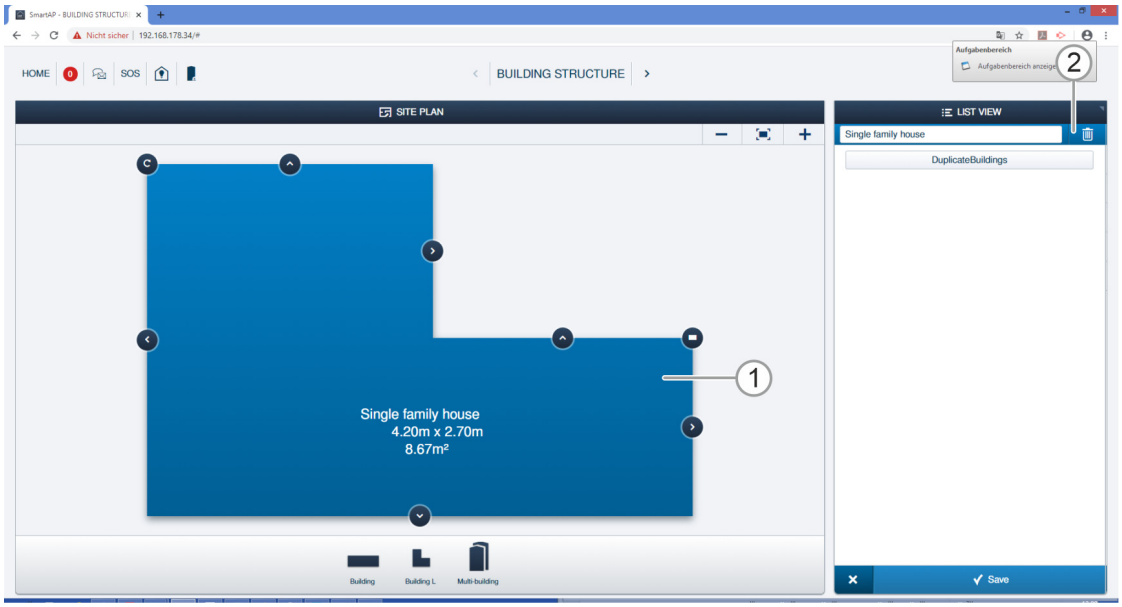


Fig. 184: Delete building

1. Search for the building [1] in the building structure and mark it.
2. Click on the "Delete" button [2].
   – The building is deleted.
3. Repeat the step until all desired buildings have been deleted.

6 Notes

7 Index

Busch-Jaeger Elektro GmbH
A member of the ABB Group

Freisenbergstraße 2
58513 Lüdenscheid

www.BUSCH-JAEGER.com
info.bje@de.abb.com

Central sales service:
Tel.: +49 2351 956-1600
Fax: +49 2351 956-1700

2CKA001473B5074