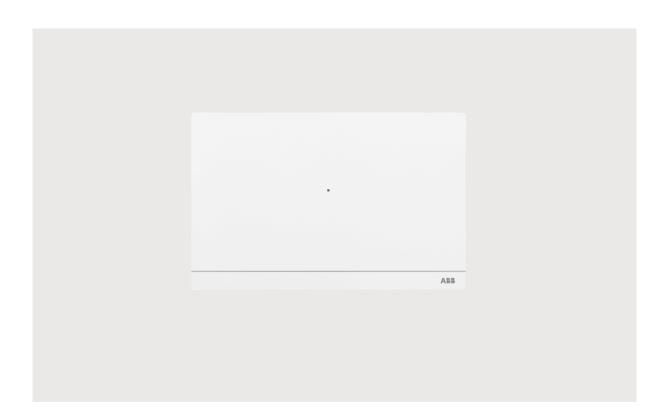


2TMD041800D0088 | 28.06.2023

# Product manual ABB-Welcome IP ABB-AccessControl

# D04011 Smart Access Point Pro



1	Notes	s on the ins	struction manual	7
2	Safet	у		7
3	Inten	ded use		7
4	Envir	onment		8
	4.1		vices	
5	Produ		otion	
	5.1	Device t	уре	9
	5.2	Termina	I description	10
6	Tech	nical data.		12
7	Mour	nting/Instal	lation	13
	7.1	Requirer	ment for the electrician	13
	7.2	Mountine	g	14
			•	
8	Com	missioning		16
	8.1	System	requirements	16
	8.2	Accessir	ng the web-based user interface of "Smart Access Point"	19
	8.3	Initial se	tup	
	8.4	Login sc	reen	
	8.5	•	ration screen	
	8.6	•	screen	
	8.7			
	•	8.7.1	Accessing quick settings	
		8.7.2	Accessing the "Preference" screen	
		8.7.3	Viewing the version	
		8.7.4	Disclaimer information	44
		8.7.5	Network setting	45
		8.7.6	Language setting	50
		8.7.7	Time settings	
		8.7.8	MyBuildings settings	
		8.7.9	WiFi Access Point mode settings	
		8.7.10 8.7.11	Third part authority settings	
		8.7.12	Abnormal devices Onvif IP-Camera settings	
		8.7.13	Alarm notification settings	
		8.7.14	Configuring "Smart Access Point"	
9	Opera	ating Door	Entry System devices	72
	9.1		try System topology	
	9.2		devices	
	U.L	9.2.1	Adding devices via scan	
		9.2.1	Adding devices manually	
	9.3		g the trusted devices	
		9.3.1	Managing the trusted devices for outdoor station	

	9.3.2	Managing the trusted devices for IP actuator	. 87
	9.3.3	Managing the trusted devices for "Smart Access Point"	. 92
	9.3.4	Emergency unlock	. 96
9.4	Assigning	permissions	.98
	9.4.1	Assigning the ID authentications to a user	. 99
	9.4.2	Assigning the outdoor stations to a user	104
	9.4.3	Assigning the unlock passwords to a user	
9.5	Managing	the backup	
9.6		permissions	
0.0	9.6.1	Removing ID authentications from a user	
	9.6.2	Removing outdoor stations from a user	
	9.6.3	Removing the unlock passwords from a user	
	9.6.4	Removing the QR codes from a user	
9.7		-	
9.7	•	ig the indoor station	
	9.7.1	Changing the language	
	9.7.2	Renaming the device	
	9.7.3	Viewing the serial number	
	9.7.4	Managing the physical address	
	9.7.5	Managing the logic address	
	9.7.6	Managing the screensaver	
	9.7.7	Managing the floorplan	124
	9.7.8	Duplicating the settings	125
	9.7.9	Updating the firmware	126
9.8	Configurir	g the outdoor station	127
	9.8.1	Changing the language	128
	9.8.2	Viewing the serial number	129
	9.8.3	Managing the physical address	130
	9.8.4	Surveillance call	132
	9.8.5	Unlock setting	133
	9.8.6	Time synchronization	134
	9.8.7	Managing Lift control	135
	9.8.8	Managing the trusted devices	136
	9.8.9	Initiating a call via the physical address	137
	9.8.10	Initiating a call via the logic address	138
	9.8.11	Initiating a call via the name list	146
	9.8.12	Managing the welcome message	153
	9.8.13	Managing the developer information	154
	9.8.14	Managing the bulletin	155
	9.8.15	Managing the unlock QR code	156
	9.8.16	Updating the firmware	158
9.9	Configurir	g the guard unit	
	9.9.1	Setting the device number	
	9.9.2	Viewing the serial number	
	9.9.3	Updating the firmware	
9.10		ig the IP actuator	
	9.10.1	Viewing the serial number	
	9.10.1	Managing the physical address	
	9.10.2	Unlock setting	
	9.10.3	Managing the trusted devices.	
	9.10. <del>4</del> 9.10.5	Releasing the IP actuator related to the outdoor station	

	9.11	Removing the devices			
		9.11.1	Removing the devices one by one	172	
		9.11.2	Removing the devices in batch		
10	Opera	ting the Ac	ccessControl devices	174	
	10.1	AccessControl topology			
	10.2	Creating	a building		
		10.2.1	Creating a building via "Smart Access Point"		
		10.2.2	Creating a building via Welcome App		
	10.3	Adding a	nd locating the devices		
		10.3.1	Locating "Smart Access Point"		
		10.3.2	Adding and locating "Electronic locking cylinders"		
		10.3.3	Adding and locating "RF Repeaters"		
		10.3.4	Adding and locating "RF/IP Gateways"		
	10.4		ng the devices		
		10.4.1	Connecting "RF Repeaters"		
		10.4.2	Connecting "Electronic locking cylinders"		
	10.5	10.4.3	AccessControl device is offline		
	10.5		g permissions		
		10.5.1 10.5.2	Assigning permissions to a user		
		10.5.2	Assigning the permission to users Setting the offline day		
		10.5.4	Managing the emergency cards		
	10.6		ng the devices		
		10.6.1	Configuring "Electronic locking cylinders"		
		10.6.2	Configuring "RF Repeaters"		
		10.6.3	Configuring "RF/IP Gateways"		
		10.6.4	Office mode		
	10.7	Controllin	ng the devices via "Smart Access Point"	226	
		10.7.1	Controlling the devices via floorplan		
		10.7.2	Controlling the devices via matrix		
	10.8	Controllin	ng the devices via Welcome App	237	
		10.8.1	Pairing "Smart Access Point" with Welcome App		
		10.8.2	Controlling "Electronic locking cylinders" via Welcome App		
	10.9	Managing	g the backup	245	
	10.10	Removing	g permissions	246	
		10.10.1	Removing permissions for a user		
		10.10.2	Removing the permissions for the users in a group		
	10.11	Disconne	ecting the devices	250	
		10.11.1	Disconnecting "Electronic locking cylinders"		
		10.11.2	Disconnecting "RF Repeaters"		
	10.12	Removing	g the devices	259	
		10.12.1	Removing "Electronic locking cylinders"		
		10.12.2	Removing "RF Repeaters"		
		10.12.3	Removing "RF/IP Gateways"		
	10.13	Replacino	g the damaged "RF Repeater"		
	10.14	Managing	g the link between the devices		
		10.14.1	Adding the link		

		10.14.2	Managing the link	
		10.14.3	Removing the link	2/1
11	Mana	ging action	S	273
	11.1	Adding ar	action	274
	11.2	Managing	the action	278
	11.3	Removing	, the action	279
40	<u> </u>	.,		
12	•			
	12.1		r	
	12.2		nce and service and network performance	
	12.3		ent guideline	
	12.4		]	
	12.5	Backup/re	estore	
	12.6	Data purg	ing	
	12.7	Malware p	prevention solution	
	12.8	Default pa	asswords and user accounts	
	12.9	Password	l rule	
	12.10	Logging		
13	Annor	adiv		207
15	13.1		ng an account on the MyBuildings portal	
	13.1	-		
	-	•	the password for the primary admin	
	13.3		agement	
		13.3.1 13.3.2	User roles Adding users	
		13.3.3	Adding user groups	
		13.3.4	Assigning the users to a user group	
		13.3.5	Configuring a user	
		13.3.6	Configuring a user group	
	13.4		the firmware	
		13.4.1 13.4.2	Updating the firmware for "Smart Access Point" Updating the firmware for Door Entry System devices	
		13.4.2	Updating the firmware for AccessControl devices	
	13.5		the backup	
		13.5.1	Creating the backup	
		13.5.2	Restoring the backup	319
		13.5.3	Removing the backup	
		13.5.4	Exporting the backup	
	13.6	13.5.5 Restoring	Importing the backup to factory default	
	15.0	13.6.1	Restoring the AccessControl devices	
		13.6.2	Accessing "Smart Access Point" remotely	
		13.6.3	Restoring the "Remote control" function	
		13.6.4	Restoring all settings to the factory defaults	
	13.7		n	
		13.7.1	Notification	
		13.7.2	Alarm record	

		13.7.3	Logs	
			Exporting the notifications	
	13.8		je center	
		13.8.1	Creating a message	
			Replying to a message	
14	Notice	е		

## 1 Notes on the instruction manual

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

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

## 2 Safety



#### Warning Electric voltage!

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

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

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

## 3 Intended use

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

## 4 Environment



#### Consider the protection of the environment!

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

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

#### 4.1 ABB devices

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

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

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

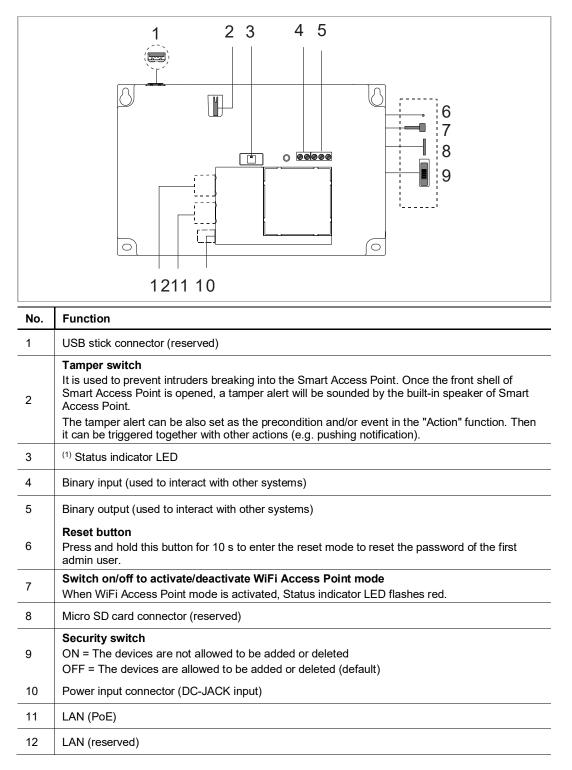
(EU-REACH ordinance and law for the implementation of the ordinance (EG) No.1907/2006)

## 5 Product description

## 5.1 Device type

Article number	Product ID	Product name	Color	Size (DxHxW) Unit: mm
D04011	2TMA400260W0002	Smart Access Point Pro	White	204 x 132 x 32

#### 5.2 Terminal description



## <sup>(1)</sup> Status indicator LED

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

## 6 Technical data

Designation	Value
Rating voltage	24 V
Operating voltage range	20-27 V ==
Rating current	24 V ==, 375 mA
PoE standard	IEEE802.3 af
Wireless transmission band	802.11b/g/n: 24122462MHz (for United States) 24122472MHz (for European countries) 802.11a/n: 51505250MHz 52505350MHz 54705725MHz (not used in Russia) 57255850MHz (for United States)
Wireless transmission power	Max. 20 dBm@12 Mbps OFDM 2.4 G Max. 20 dBm@12 Mbps OFDM 5.8 G
Wireless transmission standard	IEEE 802.11 a/b/g/n
Operating temperature	-10 °C+45 °C
Storage temperature	-25 °C+70 °C
IP level	IP 30
IK level Relay output	IK 05 30 V =, 1 A
Binary input	5 V =, 1mA

#### Bluetooth data

Bluetooth standard	4.2
Frequency range	2.4022.480 GHz
TX power	Maximum 8 dBm
RX sensitivity	Minimum -92 dBm

## 7 Mounting/Installation



#### Warning Electric voltage!

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

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

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

#### 7.1 Requirement for the electrician



#### Warning

Electric voltage!

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

Incorrect installation endangers your life and that of the user of the electrical system.

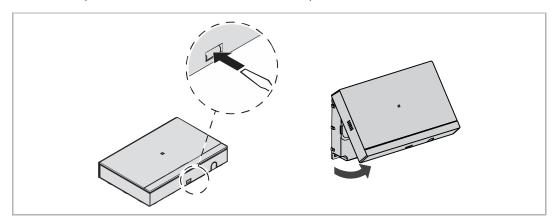
Incorrect installation can cause serious damage to property, e.g. due to fire.
 The minimum necessary expert knowledge and requirements for the installation are as follows:

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

#### 7.2 Mounting

#### 1. Dismantle

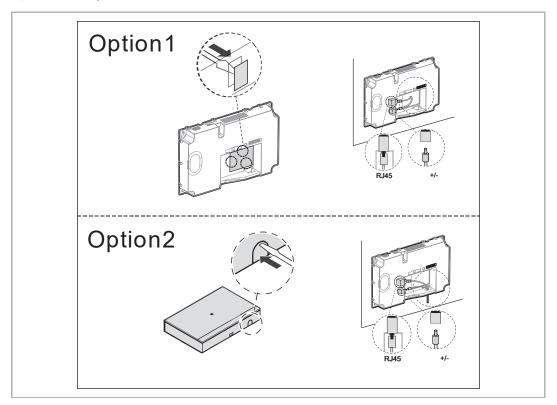
Pull the clamp on the bottom of the device and then open the front cover.



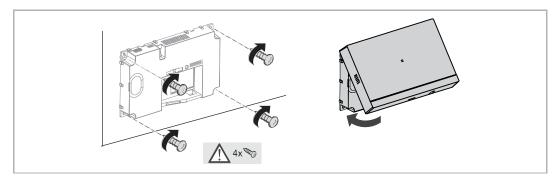
#### 2. Wiring

Option 1: Wiring from the back

Option 2: Wiring from the bottom



## 3. Mounting



## 8 Commissioning

#### 8.1 System requirements

#### **User interface**

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

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

The recommended browsers are:

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

#### Welcome App

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

#### Home network

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

#### **Building type**

"Smart Access Point" supports two building types for different applications.



Topology mode can only be selected in the initial setup.

#### 1. Residential

This mode is used for a single-family application.

Note

In this mode, "Smart Access Point" can be used to manage the devices in the house.

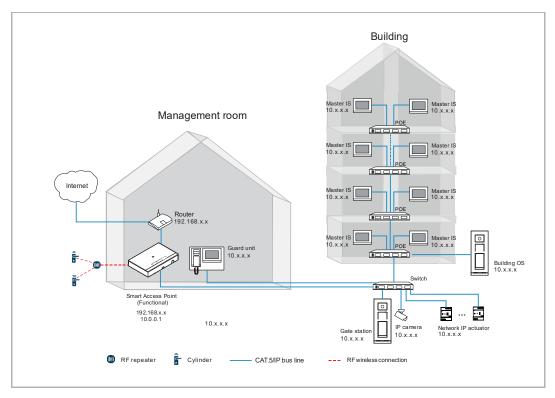
In this mode, "Smart Access Point" can only communicate with the other TCP/IP devices in a network segment which normally is the home network with static IP address or the dynamic IP address from DHCP server.

#### 2. Functional

This mode is used for multi-apartment or commercial applications.

In this mode, "Smart Access Point" can communicate with the other TCP/IP devices in 2 network segments. One is the home network in the management room. The other is the building network. IP address of "Smart Access Point" is fixed to 10.0.0.1.

All the devices on the building network can generate the IP address automatically from their physical address (e.g. building number, floor number and room number).



#### **MyBuildings account**

It is recommended to register a MyBuildings account before the initial setup.

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

#### **Remote control service**

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

1. Remote Access and Notifications

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

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

#### 2. Remote Lock Release

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

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

#### 3. Video Storage and Streaming

Remote storage services for VideoControl devices (addition package for the "Remote Access and Notifications" package):

- Storage and streaming services for event-based recording in the cloud.
- Different cloud storage packages available.
- 4. How to register an account on the MyBuildings portal

see chapter 13.1 "Registering an account on the MyBuildings portal" on page 287.

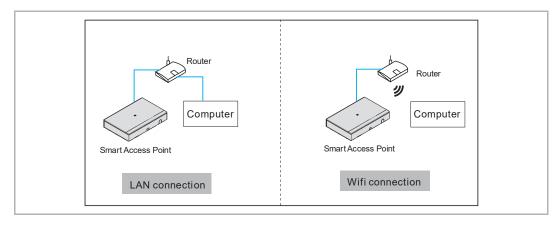
#### 8.2 Accessing the web-based user interface of "Smart Access Point"

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

1. Through Windows UPnP service

#### Precondition

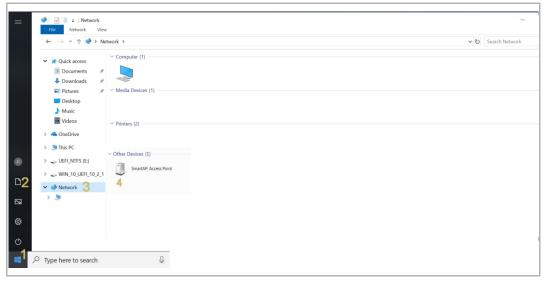
- There is a DHCP server on the network, e.g. integrated DHCP is used in the router.
- "Smart Access Point" is connected to the router by a LAN cable.
- The computer is connected to the router by LAN connection or WiFi connection.
- "Smart Access Point" is powered on and ready for operation.



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

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

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



#### Note

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

 $\cap$ 

#### [3] Switch to Security Login

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

Privacy error     X     +	
← → C ▲ Not secure   192.168.1.101/index html	
	Your connection is not private
	Attackers might be trying to steal your information from <b>192.168.1.101</b> (for example, passwords, messages, or credit cards). Learn more
	NET::ERR_CERT_AUTHORITY_INVALID
	Help improve Chrome security by sending URLs of some pages you visit. limited system
	information. and some page content to Google. Privacy policy
	Hide advanced 5 Back to safety
	This server could not prove that it is <b>192.168.1.101</b> ; its security certificate is not trusted by
	your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.
	Proceed to 192,168.1.101 (unsafe) 6

2. Through entering the IP address

#### Precondition

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

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

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

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

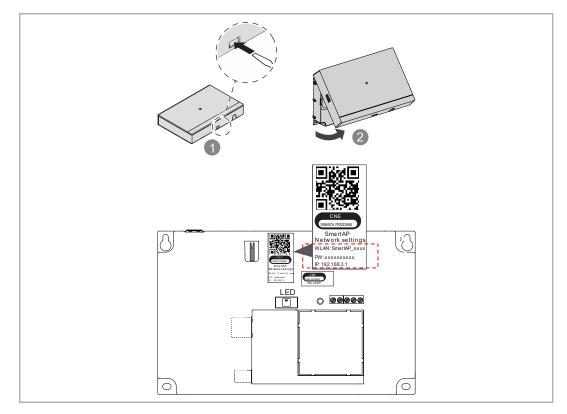
Privacy error × +	
← → C ▲ Not sequre   192.168.1.101/index.html	
	Your connection is not private
	Attackers might be trying to steal your information from <b>192.168.1.101</b> (for example, passwords, messages, or credit cards). <u>Learn more</u>
	NET:ERR_CERT_AUTHORITY_INVALID
	Help improve Chrome security by sending <u>URLs of some pages you visit</u> , <u>limited system</u> information, and some page content to Google. <u>Privacy policy</u>
	Hide advanced 1 Back to safety
	This server could not prove that it is <b>192.168.1.101</b> ; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.
	Proceed to 192.168.1.101 (unsafe) 2

3. Through WiFi Access Point hotpot

#### Precondition

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

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



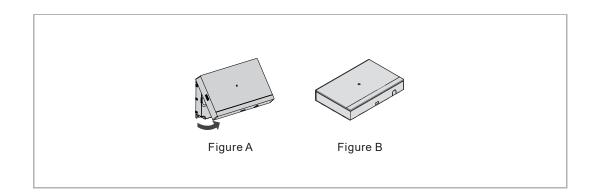
- Ensure the alarm (e.g. tamper alarm) is not activated



#### Note

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

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



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

Status indicator LED	



#### Note

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

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

- [1] Click "Internet access" icon.
- [2] Click the WLAN name (SSID) of "Smart Access Point".
- [3] Enter the password.
- [4] Click "Next".
- [5] Click "Yes" to connect your computer to the WiFi hotspot of "Smart Access Point".

		Common SmartAP_0734 No Internet, secured Properties Disconnect
SmartAP_0734 2 Secured 2 Enter the network security key ••••••••••••••••••••••••••••••••••••	SmartAP_0734 Secured           Do you want to allow your PC to be discoverable by other PCs and devices on this network?           We recommend allowing this on your home and work networks, but not public ones.	
Network & Internet settings         Change settings, such as making a connection metered.         Image: State of the settings of the setting of the settings of the settings of the setti	Yes 5 No Network & Internet settings Change settings, such as making a connection metered.	Network & Internet settings Change settings, such as making a connection metered. Wi-Fi Airplane mode hotspot

- [6] Enter "192.168.3.1" on the website to access "Smart Access Point".
- [7] Switch to Security Login
  - Http-connection is insecure. It is recommended to use an https-connection.
  - Click "Advanced", followed by "Proceed to ...." to access the web-based user interface of "Smart Access Point". (Google chrome as an example)

Image: Optimized privacy error         ×         +           ←         →         C         ▲         https://192.168.3.1	
	Your connection is not private
	Attackers might be trying to steal your information from <b>192.168.3.1</b> (for example, passwords, messages, or credit cards). Learn more
	NET::ERR_CERT_AUTHORITY_INVALID
	Help improve Chrome security by sending <u>URLs of some pages you visit. limited system</u> information. and some page content to Google. <u>Privacy policy</u>
	Hide advanced 1 Back to safety
	This server could not prove that it is <b>192.168.3.1</b> ; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.
	Proceed to 192.168.3.1 (unsafe) 2

#### 8.3 Initial setup

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

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

1. Select language

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

Please choose y	our language
简体中文	
Český	
Dansk	
Deutsch	
English	✓
Español	
St	art

#### 2. Accept end user license

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

End user licens	e agreement			
ABB End User License Agre	ement ("EULA")			
IMPORTANT: PLEASE REA CONTINUING WITH THIS P	D THE TERMS AND CONDITION	IS OF THIS LICENSE AGRI	EEMENT CAREFULLY BI	EFORE
GENWAY XIAMEN ELECTR SOFTWARE PRODUCT me copies made, bug fixes for, u "online" or electronic docume SOFTWARE PRODUCT. By entering into this EULA on b entire agreement concerning	ement ("EULA") is a legal agreem ICAL EQUIPMENT CO., LTD or it ans the machine readable (object podates to, or upgrades thereof, a entation"Use" or "Using" means Using the SOFTWARE PRODUC healf of an entity, you represent th the program between you and the parties. If you do not agree to the t	s affiliates (the "Company") ( code) version of the computed associated software comp to download, install, copy, a 77, you agree to be bound by 14 you have authority to bind be Company, and it supersed	or the "SOFTWARE PRO ter programs including firm ponents, media, printed m ctivate, access or otherwis y the terms of this EULA. y that entity. This EULA re es any prior proposal, rep	DUCT". ware, any aterials, and se use the If you are ppresents the resentation, or
✓ I have read the "E	nd User Licence Agreeme	ent" and accepted it.		

3. Accept Open Source Software license

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

Licensing terms	ABB-Welcome		
Following Licenses are used in			
HGM52-AC & HGM52-IPC	0x		
Component: Linux OS			
License: GNU GENERAL PUE	BLIC LICENSE V2		
Copyright year: 1992 - 2010 Copyright holder: Linus Torvak	ds et al.		
Source Code Download location	on: git://git.freescale.com/imx/fsl-arm	i-yocto-bsp.git	
Component: QT			
License: GNU Lesser General	Public License V2.1 or later		
✓ I accept the licensir	ng terms		
	<	>	
✓ I accept the licensir			
	<	>	

4. Accept data privacy

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

Data privacy				
We take the protection of your per refer to below link.	ersonal data very seriously and foll	ow the legally valid regulations re	garding data protection, detail	
https://eu.mybuildings.abb.com/e	en/page/privacy-policy			
<b>G</b>				
✓ I accept the data priv	acy			
	<	>		

5. Choose building type

see chapter 8.1 "System requirements" on page 16.



#### Attention!

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

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

Please choos	e your building t	type
<ul> <li>Residential (for sir</li> <li>Functional (for mul apartment/comment/</li> </ul>		
<	>	

#### 6. Define your location

Select the time zone from the drop-down list.

Please de	fine your location
Time zone	(UTC-12:00) International D 🗸
Date and time	2019-08-20 11:24:58
<	>

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

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

## Attention!

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

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

Wi-Fi a	access po	int mode s	settings	
SSID	s	martAP_0734		
Password	-		×	At least 10 characters Uppercase to lowercase let At least one special charact
Repeat pass	sword			At least one number
Country cod	ie A	fghanistan	~	
	<			

#### 8. Select a connection type

There are 3 options to connect to home network:

Please	e select co	nnection type
LAN		
WiFi		
	<	Skip

#### **Option 1: LAN**

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

#### **Option 2: WiFi**

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

#### **Option 3: Skip the selection**

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

#### **Establish LAN connection**

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

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

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

Please esta	ablish LAN connection
Obtain IP addre	ess automatically
IP address	192.168.1.100
Subnet mask	255.255.255.0
Default gateway	
<	>

#### Connect to a WiFi Network

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

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

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

Please connect to	a WIFI netwo
21	.at
TP-LINK_9416	
21_ISS_5G	.al
cisco	.at
21_2.4G	
EACT 7000	- I-
< Refresh	Connect

9. Create the first admin user

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



#### Note

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

If you want to reset the password for the first admin, see chapter 13.2 "Resetting the password for the primary admin" on page 288.

Please create	e your user account
User name	jacky
Password	
Repeat password	
<	>

#### 10. Select reset option

You can select reset option according to the use scenario.

Options for R	eset	
Without myBuildings a	account *	✓
With myBuildings acco	ount (recommended) **	
* Reset of the password is can be performed by anyor ** Reset of the password is once valid security code, w account by email.	ne via the reset button. s done with a security verif	cation by a
<	>	

#### Reset option = Without MyBuildings account

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

#### Reset option = With MyBuildings account

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



#### Attention!

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

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

#### 11. MyBuildings setting

#### Reset option = Without MyBuildings account

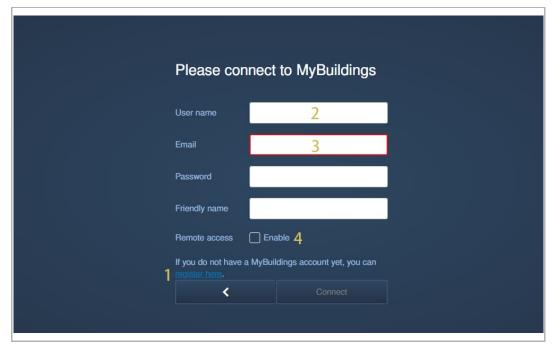
If the reset option is set to "Without MyBuildings account", you will access this screen.

	lease conno	ect to My	/Buildi	ngs		
Us						
	er name		3			
Pa	ssword					
Frie	endly name					
Re	emote access	Enable 4				
	you do not have a M <u>gister here</u> .	lyBuildings acc	ount yet, yo	ou can		
	<		Skip	1		

- [1] Click "Skip" to turn to next step if you don't want to connect to MyBuildings currently.
- [2] Click "Register here" to access the MyBuildings portal to register an account. see chapter 13.1 "Registering an account on the MyBuildings portal" on page 287.
- [3] Enter the username, password and friendly name, followed by "Connect" to connect to MyBuildings portal.
- [4] If you want to access "Smart Access Point" from the MyBuildings portal, you need to tick the "Enable" checkbox to enable the remote access function.

#### Reset option = With MyBuildings account

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



- [1] Click "Register here" to access the MyBuildings portal to register an account. see chapter 13.1 "Registering an account on the MyBuildings portal" on page 287.
- [2] Enter the username, password and friendly name, followed by "Connect" to connect to MyBuildings portal.
- [3] Enter the Email used to activate the MyBuildings account. This mail will receive a security code when you want to reset the first admin user. see chapter 13.2 "Resetting the password for the primary admin" on page 288.
- [4] If you want to access "Smart Access Point" from the MyBuildings portal, you need to tick the "Enable" checkbox to enable the remote access function.

#### 12. Set the device name

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

Please ente	er the device name	
Device name	Jacky's Pro	
<	>	

#### 13. Confirm the settings

è

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

Click "Finish" to complete the initial setup.

Thank you!		
Language	English	1
Time zone	(UTC-12:00) Internation	
System access point	SmartAP_D590	
Connection type	WiFi	
User name	jacky	
Building type	Functional	
MvBuildings	disable	
<	Finish	

#### 8.4 Login screen

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

#### The number of users <6

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

	Jacky's Pro	
PLEASE LOGIN		
🛔 jacky		
amon 🔒		
🛔 faye		
	CONTROL	
	E CONTROL	

#### The number of users $\geq 6$

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

Jacky's Pro
PLEASE LOGIN
User name
Password

#### 8.5 Configuration screen

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

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

	PI FA	se login				
	🛔 jacky					
		CONFIGURAT	ION		DL	
❤ 🧿 🗟 sc	os 🕐 🖡		MAIN MENU			
_			•			_
M			• •	A	ō	G
	CONNECTION	PLACE - LINK	USER MANAGEMENT	ACTIONS	<b>Ö</b> Time control	DOOR ENTRY SYSTEM
BUILDING STRUCTURE Design a building by creating floors and rooms		PLADE & LINK PLADE & LINK	USER MANAGEMENT Add and edit users. Create user groups	ACTORS	THE CONTROL	DOOR ENTRY SYSTEM Configurate door entry system devices, e.g. indoor station, outdoor station

#### 8.6 Control screen

The control screen is used to control the AccessControl devices.

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

	PLEASE LOGIN	CONTROL	
Foorplan           ∎		MENU	Vert history

#### 8.7 Settings

### 8.7.1 Accessing quick settings

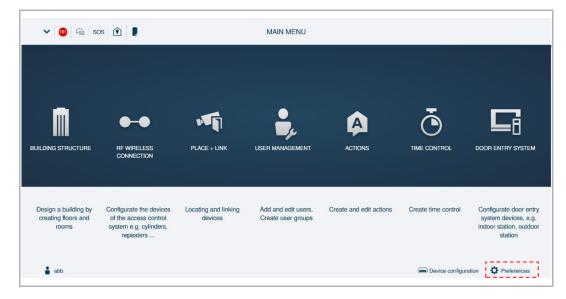
On the configuration screen, click " $\vee$ " to carry out some common operations:

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

^	MENU	F		MAIN MENU			
Network							
✓ Network	LAN client >						
SmartAP	Jacky's Pro >						
	A ivanslagecn >	▶●			A	Ā	
General settings				-4-			
Settings	>	WIRELESS NNECTION					
Logout jacky							
		urate the devices access control n.e.g. cylinders, opeaters	Locating and linking devices	Add and edit users. Create user groups	Create and edit actions	Create time control	Configurate door entry system devices, e.g. indoor station, outdoor station
						Device configure	ation 🔅 Preferences

#### 8.7.2 Accessing the "Preference" screen

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



# 8.7.3 Viewing the version

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

HOME 📵 🗟 SOS 🕅	PREFERENCES >
	C PREFERENCES
Preferences	System information
System information	Version information
Network settings	Version V2.41 Date 20200228163012
Localization	> System information
Project backups	Devices 5     Operating time 1309m (0d 21h)
Firmware updates	>
MyBuildings Account	> Data Privacy End user license agreement
Service	Licensing Terms ABB-Welcome     @Copyright 2019 ABB.All rights reserved
Wi-Fi access point mode settings	
Third party authority	<b>&gt;</b>
Abnormal devices	<b>3</b>
Onvif IPC list	> •

#### 8.7.4 **Disclaimer information**

Ē

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

	PREFERENCES >
Preferences	System information
System information	Version information
Network settings	Version         V2.41           Date         2020028163012
Localization	> System information
Project backups	Devices 5     Operating time 1309m (0d 21h)
Firmware updates	> Cybradung inne 100am (00.2 m)
MyBuildings Account	> Data Privacy End user license agreement
Service	Licensing Terms ABB Welcome     @Copyright 2019 ABB All rights reserved
Wi-Fi access point mode settings	>
Third party authority	5 ·
Abnormal devices	2
Onvif IPC list	, <b>*</b>

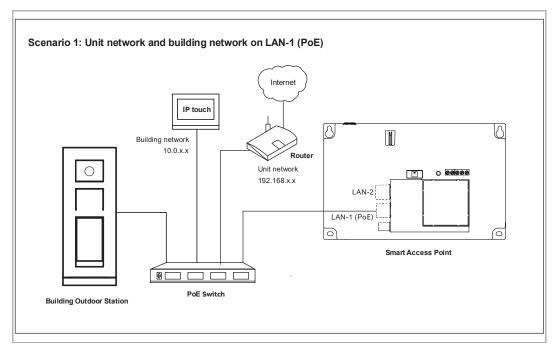
#### 8.7.5 Network setting

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

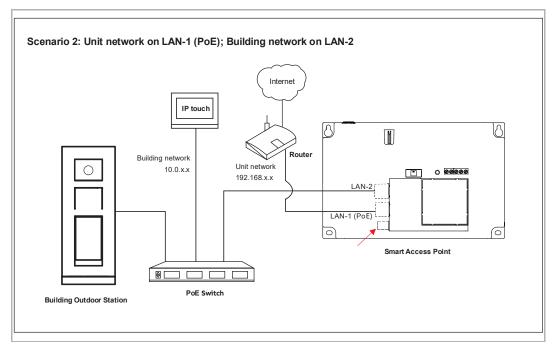
- [1] "Unit network and building network on LAN-1 (POE)" is used by default.
- [2] Click the right diagram to view the zoom view.

	🔅 PREFEF	RENCES	
Preferences	Network settings		Scenario 1: Unit exteronic and building natwork on LAIN-1 (Poll)
System information	> Network mode		
Network settings	> Unit network and building network on LAN-1 (POE	=) ~	0 Bringer (* 1997)
Localization	Unit network and building network on LAN-1 (PO	E)	Contraction for a second system of the second
Project backups	Unit network on LAN-1 (POE); Building network o	on LAN-2	A state in team of the second se
Firmware updates	Unit network on LAN-2; Building network on LAN	I-1 (POE) (Recommended setting)	
MyBuildings Account	Unit network on WLAN; Building network on LAN	I-1 (POE)	
Service	Subnet mask	255.255.255.0	
Wi-Fi access point mode settings	Default gateway		
	DNS server	114.114.114	
Third party authority	Building network		
Abnormal devices	>	•	
	🔅 PREFEF	254052	
Preferences			amont on LW-2 Building paravet on LW-1 (Put) (Recommended setting)
System information	Scenario 3: Unit network on LAN-2; Building network o	n LAN-1 (PoE) (Recommended setting)	-
Network settings	Intern	for	
Localization	IP touch		
Project backups	Building network 10.0.x.x Unit metwork 192.168.x.x	Router	
Firmware updates		LAN2-	
MyBuildings Account			
Service		Smart Access Point Smart Access Point can be powered by Power Supply or PoE LAN1.	Switch via
Wi-Fi access point mode settings	PoE Switch Building Outdoor Station	Smart Access Point access the internet via LAN2 (Router).     Smart Access Point access the building network via LAN1. DEI	3 devices
Third party authority	Connecting status	can be updated the firmware remotely via Smart Access Point.	
Abnormal devices	Obtain IP address automatically     X	<b>√</b> Save	

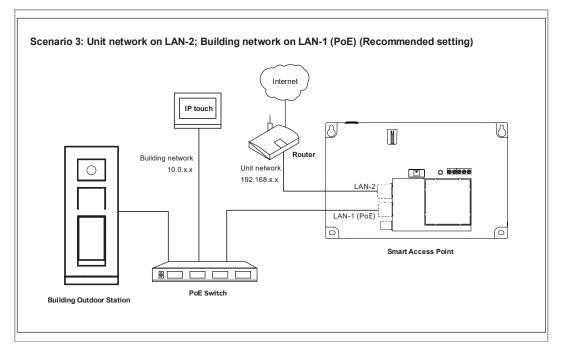
- 1. Unit network and building network on LAN-1 (POE)
- Smart Access Point can be powered by Power Supply or PoE Switch via LAN-1 (PoE).
- Smart Access Point access the internet via LAN-1 (PoE).
- Smart Access Point access the building network via LAN-1 (PoE). DES devices can be updated the firmware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



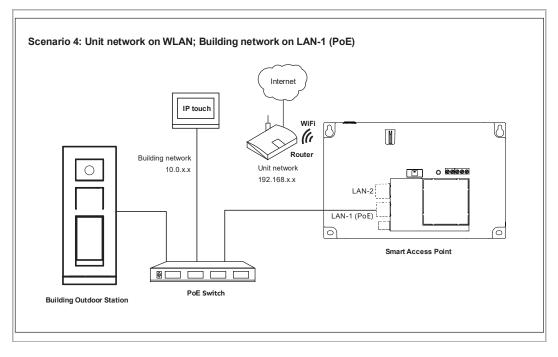
- 2. Unit network on LAN-1 (POE); Building network on LAN-2
- Smart Access Point can be powered by Power Supply.
- Smart Access Point access the internet via LAN-1 (PoE).
- Smart Access Point access the building network via LAN-2. DES devices can be updated the firmware remotely via Smart Access Point.



- 3. Unit network on LAN-2; Building network on LAN-1 (POE) (Recommended setting)
- Smart Access Point can be powered by Power Supply or PoE Switch via LAN-1 (PoE).
- Smart Access Point access the internet via LAN-2.
- Smart Access Point access the building network via LAN-1 (PoE). DES devices can be updated the firmware remotely via Smart Access Point.



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



see chapter 8.3 "Initial setup" on page 26

# 8.7.6 Language setting

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

Preferences		Localization		
System information	>	System settings		
Network settings	>	Device name	Jacky's Pro	
Localization	>	Language		
Project backups	>	Language	English ~	
Firmware updates	>	Time zone		
MyBuildings	>	Time zone	(UTC+08:00) Beijing,Chongqing,H ✓	
Service	>	Date/time		
WI-FI access point mode settings	>	Mode	NTP time service	
Third party authority	>	Server	pool.ntp.org	
Abnormal devices	>			
Onvif IPC list	>		•	

# 8.7.7 Time settings

# Time zone setting

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

Preferences		Localization		
System information	>	System settings		
Network settings	>	Device name	Jacky's Pro	
Localization	>	Language		
Project backups	>	Language	English ~	
Firmware updates	>	Time zone		
MyBuildings	>	Time zone	(UTC+08:00) Beijing,Chongqing,H ~	
Service	>	Date/time		
WI-FI access point mode settings	>	Mode	NTP time service ~	
Third party authority	>	Server	pool.ntp.org	
Abnormal devices	>			
Onvif IPC list	>		•	

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

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

		*	PREFERENCES
Preferences		Localization	
System information	>	System settings	
Network settings	>	Device name	Jacky's Pro
Localization	>	Language	
Project backups	>	Language	English ×
Firmware updates	>	Time zone	
MyBuildings	>	Time zone	(UTC+08:00) Beijing,Chongqing,H… ✓
Service	>	Date/time	! ! !
WI-FI access point mode settings	>	Mode Smart Access Point time	Local system time   2019-09-30 11:43:47
Third party authority	>	PC time	2019-09-30 11:43:47
Abnormal devices	>	L	Synchronize with PC time
Onvif IPC list	>	×	✓ Save
		¢	PREFERENCES
Preferences		Localization	
System information	>	System settings	
Network settings	>	Device name	Jacky's Pro
Localization	>	Language	
Project backups	>	Language	English ~
Firmware updates	>	Time zone	
MyBuildings	>	Time zone	(UTC+08:00) Beijing,Chongqing,H ✓
Service	>	Date/time	
WI-FI access point mode settings	>	Mode Server	NTP time service ~
		Gerver	poortriptorg
Third party authority	>	·	'
Third party authority Abnormal devices	>		

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



Note

This function is only used for Door Entry System devices.

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

	a de casa esta de casa
	PREFERENCES
Preferences	Misc settings
Network settings	Time synchronisation for door entry system devices
Localization	> O Automatically Manually
Project backups	Synchronize period(hour)
Firmware updates	> Apply
MyBuildings Account	> Door communication devices
Service	Alarm when device goes offline
Wi-Fi access point mode settings	<ul> <li>✓ Enable sound notification</li> <li>✓ Enable popup notification</li> </ul>
Third party authority	Access control devices
Abnormal devices	> Alarm when cylinder goes offline
Onvif IPC list	> Apply
Misc settings	>
	_

#### 8.7.8 MyBuildings settings

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

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

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

			🔅 PREFE	ERENCES	
Preferences		MyBuildings		MyBuildings	
System information	>	Connection	>		Buildings account information to register this device with
Network settings	>	License	>	about MyBuildings, re	o not have account yet, you can register here. For more information efer to the help.
Localization	>			At present, the remote	e function is temporarily in the trial operation phase.
Project backups	>				Pair: 🖌 Connect: 🖌
Firmware updates	>			User name	
MyBuildings	>			Password	
Service	>			Friendly name	
WI-FI access point mode settings	>			UUID Remote access	638a0b1c-5b39-4952-876c-083941d29d67
Third party authority	>			nemole access	Logout
Abnormal devices	>				
Onvif IPC list	>	*			•

#### **Refresh the license**

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

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

		🔅 PRE	FE	RENCES	
Preferences		MyBuildings		MyBuildings	
System information	>	Connection >	,	Remote Access and Notifications	
Network settings	>	License >	,	Effective date Expiration date	2019-09-30 13:13:04 2019-10-20 06:00:00
Localization	>				
Project backups	>				
Firmware updates	>				
MyBuildings	>				
Service	>				
WI-FI access point mode settings	>				
Third party authority	>				
Abnormal devices	>				
Onvif IPC list	>	*			0

#### 8.7.9 WiFi Access Point mode settings

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

Preferences		WI-FI access point mode settings	WI-FI access point mode settings					
System information	>	WI-FI access point mode setti	ings					
Network settings	>	SSID	SmartAP_D590					
Localization	>	Password						
Project backups	>	IP address	192.168.3.1					
Firmware updates	>	Band	2.4G	~				
MyBuildings	>	Country code	China	~				
Service	>							
WI-FI access point mode settings	>							
Third party authority	>							
Abnormal devices	>							
Onvif IPC list	>	×	✔ Save					

#### 8.7.10 Third part authority settings

Third party device can obtain the data of Door Entry System (e.g. unlock information) from "Smart Access Point" by setting the designated IP address and port of the third-party device.

On the "Preferences", "Third party authority" screen, click "add" and enter the IP address and the port number, then click "Applied" to apply the setting.

Preferences		Third party authority
System information	>	,Add
Network settings	>	
Localization	>	IP address Port
Project backups	>	
Firmware updates	>	
MyBuildings	>	
Service	>	
WI-FI access point mode settings	>	
Third party authority	>	
Abnormal devices	>	
Onvif IPC list	>	
Preferences		Third party authority
System information	>	
Network settings	>	Add IP address
Localization	>	IP address
Project backups	>	Port
Firmware updates	>	Cancel Applied
	,	
MyBuildings		
Service	>	
WI-FI access point mode settings	>	
Third party authority	>	
Abnormal devices	>	
Onvif IPC list	>	<b>*</b>

#### 8.7.11 Abnormal devices

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

				🔅 PREFE	RENCES		
Preferences		Abnormal	devices				
letwork settings	>						
ocalization	>	Room No.	Device No.	Device type	Serial No.	MAC	Reason
Project backups	,	00	01	Outdoor station	101807A7F02F948	807A7F02F948	Device signed failed
		00	02	Outdoor station	101807A7F02F945	807A7F02F945	Device signed failed
irmware updates	>	02	01	Indoor station	102807A7F02F605	807A7F02F605	Device signed failed
lyBuildings	>	01	01	Indoor station	102807A7F0280D8	807A7F0280D8	Device signed failed
Service	>						
VI-FI access point mode settings	>						
hird party authority	>						
Abnormal devices	>						
Dnvif IPC list	>						
isc settings	>				•		

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

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

#### 8.7.12 Onvif IP-Camera settings

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

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

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

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

			* PREFERENCES		
Preferences		Onvif IPC list			
Network settings	>	Search device			
Localization	>	IP address	Name	Status	Action
Project backups	>	IF address	Name	Sidius	Acion
Firmware updates	>				
MyBuildings	>				
Service	>				
VI-FI access point mode settings	>				
hird party authority	>				
bnormal devices	>				
Onvif IPC list	>				
Aisc settings	>		•		

			PREFERENCES		
Preferences		Onvif IPC list			
Network settings	>	Search dev	ice		
Localization	>	IP address	Name	Status	Action
Project backups	>	10.0.0.3	HIKVISION%20DS-2CD2142FWD-I	Unpaired	Enter credentials
Firmware updates	>	10.0.0.0		Chparod	
MyBuildings	>				
Service	>				
VI-FI access point mode settings	>				
hird party authority	>				
Abnormal devices	>				
Onvif IPC list	>				
/lisc settings	>		•		

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

			9				
Preferences		Onvif IPC list					
Network settings	>	Search	device				
Localization	>	INFORMATION					
Project backups	>	Enterior					Action
Firmware updates	>		mera crede	entials			
MyBuildings	>		admin				
Service	>	Password					
WI-FI access point mode settings	>	×			Pair		
Third party authority	>						
Abnormal devices	>						
Onvif IPC list	>						
Misc settings	>			٠			
Preferences		Onvif IPC list			1		
Network settings	>	Search	levice				
Localization	>				10000		
Project backups	>	IP address		Name	Status		tion
Firmware updates	>	10.0.0.3	HIKVISIC	111762UUS-2GU2142FWU-I	Paireo	Update c	reventials
MyBuildings	>						
Service	>						
WI-FI access point mode settings	>						
Third party authority	>						
Abnormal devices	>						
Onvif IPC list	>						

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

#### 8.7.13 Alarm notification settings

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

	C PREFERENCES					
Preferences	Misc settings					
Network settings	Time synchronisation for door entry system devices					
Localization	> • • Automatically OManually					
Project backups	Synchronize period(hour)					
Firmware updates	Apply					
MyBuildings Account	> Door communication devices					
Service	Alarm when device goes offline     Vertication					
Wi-Fi access point mode settings	Crable source non-manual      Crable popup notification					
Third party authority	Access control devices					
Abnormal devices	> I Alarm when cylinder goes offline					
Onvif IPC list	> Apply					
Misc settings	•					



#### Note

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

# 8.7.14 Configuring "Smart Access Point"

#### Access the setting screen

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

	LIST	VIEW	
Device type	SmartAP(1)	Smart Access Point	Tamper alarm
SmartAP(1)	#105807A7F030734(RGA) Smart Access Point	Floor	Tamper alarm
Cylinder(0)		<not allocated=""></not>	1×
Repeater(0) >		Room (not allocated)	
RF/IP gateway(0)		Channels	
IP camera(0)		Doorbell ring	
Outdoor station(0)		Alarm alert	
Indoor station(0)		Binary input	
O- IP actuator(0)		Binary output >	
Guard unit(0)		Tamper alarm	
		Security Switch	Parameter
		Mute >	Tamper alarm
		Day/night switchover	Disable
		*	♠ )

# Doorbell ring

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

Smart Access Point		Doorbell ring		
the mode volument a viso		Doorbeit ning		
RF module version: V1.05		Door	bell ring	
Update firmware			<b>9</b> /1	1
Position			î	
Building				
<not allocated=""></not>	~			
Floor				
<not allocated=""></not>	~			
Room				
<not allocated=""></not>	~			
Channels				
Doorbell ring	>			
Alarm alert	>	Parameter		
Binary input	>	Ringtone 4	2	~
Binary output	>	Repeat times		
Tamper alarm	>	-	4	+ 3
Security Switch	>	Repeat interval tir		
Mute	>	- 1	10	+ 4
w 100 cm (000 c)		Volume		
Day/night switchover	>	-	4	+ 5
÷			+	

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

#### Alarm alert

Duration time (minutes)

Time duration of the alarm alert.

2

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

		Alarm alert	
Smart Access Point			
RF module version: V1.05		Alarm alert	
Update firmware		遂	1
Position			
Building			
<not allocated=""></not>	~		
Floor			
<not allocated=""></not>	~		
Room			
<not allocated=""></not>	~		
Channels			
Doorbell ring	>		
Alarm alert	>		
Binary input	>		
Binary output	>		
Tamper alarm	>		
Security Switch	>		
Mute	>	Parameter Duration time (minutes)	2
Day/night switchover	>	- 5	<b>4</b>
4		•	
. Description			
-			
Icon			

#### **Binary input**

Position

2

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

		Smart Access Point		Binary input	
		RF module version: V1.05 Update firmware		Binary înput	1
		Position		Ľ	
		Building			
		<not allocated=""></not>	~	Position	
				Building	
		Floor		<not allocated=""> 2</not>	~
		<not allocated=""></not>	~	Floor	
		Room		<not allocated=""></not>	~
		<not allocated=""></not>	~		
		Channels		Room	
		Doorbell ring	>	<not allocated=""></not>	~
		Alarm alert	>		
		Binary input	>		
		Binary output	>		
		Tamper alarm	>		
		Security Switch	>		
		Mute	>		
		Day/night switchover	>		
		*		•	
lo.	Description				
	lcon				
		us of the channel.			

Assign the sensor connected to the binary input to the building structure (building, floor, room).

# Binary output

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

	Binary output	
	4	1
~		
	<not allocated=""></not>	~
	Floor	
	<not allocated=""></not>	~
~		
>	<not allocated=""></not>	*
>		
>		
>		
>		
>		
>	Parameter Duration time (seconds)	
>	- 1	+ 3
	•	
	<ul> <li></li> <li>&gt;</li> <li>&gt;<!--</td--><td></td></li></ul>	

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

#### Tamper alarm

Enable/disable the function

Click the drop-down list to enable/disable the function.

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

						_
		Smart Access Point		Tamper alarm		
		RF module version: V1.05			mper alarm	
		Update firmware		1.1.4	<i>I</i> ∕∕ <sub>∕</sub>	1
		Position				
		Building				
		<not allocated=""></not>	~			
		Floor				
		<not allocated=""></not>	*			
		Room				
		<not allocated=""></not>	~			
		Channels				
		Doorbell ring	>			
		Alarm alert	>			
		Binary input	>			
		Binary output	>			
		Tamper alarm	>			
		Security Switch	>	Description		
		Mute	>	Parameter Tamper alarm		
		Day/night switchover	>	Disable	2	~
		÷.			*	
	<b>-</b>					
No.	Description					
4	lcon					
1	Display the statu	us of the channel.				

2

# Security switch

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

		Smart Access Point		Security Switch	
		RF module version: V1.05			-
		Update firmware		Security Switch	
		Position		Ø 1	
		Building			
		<not allocated=""></not>	~		
		Floor			
		<not allocated=""></not>	~		
		Room			
		<not allocated=""></not>	~		
		Channels			
		Doorbell ring	>		
		Alarm alert	>		
		Binary input	>		
		Binary output	>		
		Tamper alarm	>		
		Security Switch	>		
		Mute	>		
		Day/night switchover	>		
		*		*	
No.	Description				
	lcon				
1		<b>. </b>			
	Display the statu	is of the channel.			

#### Mute

lcon

1

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

Smart Access Point	M	ute	
RF module version: V1.05		Mute	
Update firmware		. Mule	1
Position		· · · · ·	
Building			
<not allocated=""></not>	~		
Floor			
<not allocated=""></not>	~		
Room			
<not allocated=""></not>	~		
Channels			
Doorbell ring	>		
Alarm alert	>		
Binary input	>		
Binary output	>		
Tamper alarm	>		
Security Switch	>		
Mute	>		
Day/night switchover	>		
4		*	
Description			
•			

Display the status of the channel. It can be triggered manually by pushing the icon.

#### Day/night switchover

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

Smart Access Point		Day/night switchover	
RF module version: V1.05		Destriction	
Update firmware		Day/night switchover	1
Position			S
Building			
<not allocated=""></not>	~		
Floor			
<not allocated=""></not>	~		
Room			
<not allocated=""></not>	~		
Channels			
Doorbell ring	>		
Alarm alert	>		
Binary input	>		
Binary output	>		
Tamper alarm	>		
Security Switch	>		
Mute	>		
Day/night switchover	>		
*		*	

No. Description

1

Display the status when it is day or when it is night. The day and night switch is triggered by the internal astro function.

# 9 Operating Door Entry System devices

# 9.1 Door Entry System topology

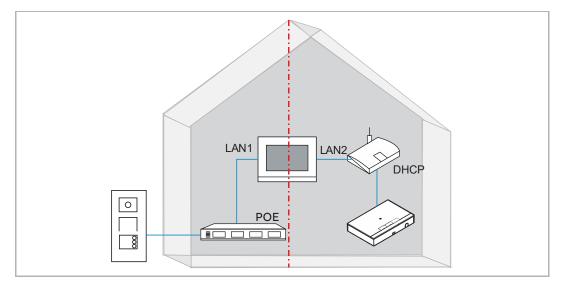
#### Topology1: Single-family house

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

An IP Touch 7/10 is installed.

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

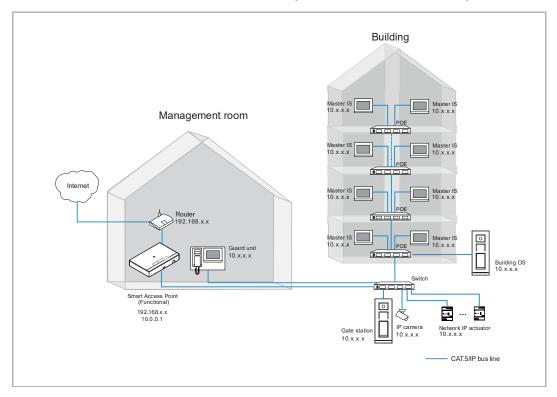
"Smart Access Point" should be set to "Commercial Mode" on the initial Setup.



# Topology 2: High rise building

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

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

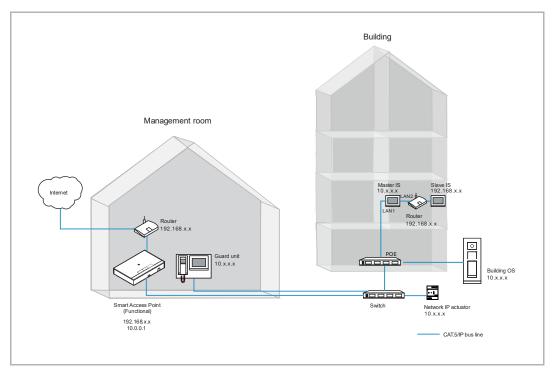


# Demo case for operating Door Entry System devices

The following demo case refers to topology 2.

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

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



#### 9.2 Adding devices



#### Note

All the Door Entry System devices need a signature on "Smart Access Point" before use.

#### Note

"Smart Access Point" will assign a signature to the devices automatically when adding them.



Ο

#### Note

Note

If the device has already been signed by current "Smart Access Point", it will not be signed again.

If the device has already been signed by other "Smart Access Point", it will not be signed and "Sign failed" will be displayed on the "Abnormal devices" screen. see chapter 8.7.11 "Abnormal devices" on page 58.

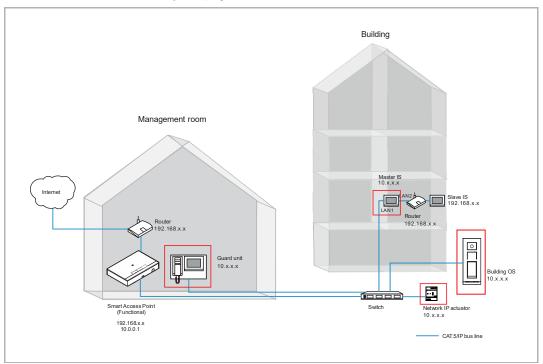
# 9.2.1 Adding devices via scan



#### Note

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

"Slave indoor station "cannot be added via scan. see chapter 9.2.2 "Adding devices manually" on page 80



#### Precondition

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

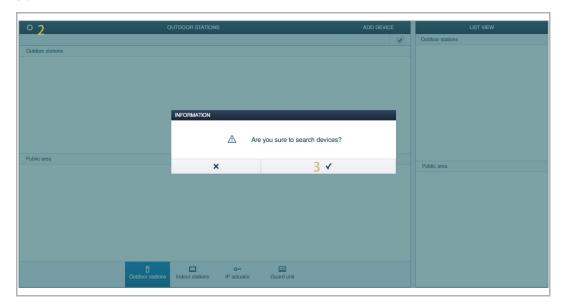
#### Adding the devices via scan

Please follow the steps below:

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

BUILDING STRUCTURE	GE-OC ARE WARELEESS SCHWARELEESS	PLACE - LINK	USER MANAGEMENT	ACTIONS	THE CONTROL	DOOR ENTRY SYSTEM
Design a building by creating floors and rooms	Configure the devices of the AccessControl system e.g. Cylinder, repeater	Locating and linking devices	Add and edit users. Create user groups	Create and edit actions	Create time control	Configurate door entry system devices, e.g. indoor station, outdoor station
🛔 jacky					Device	configuration

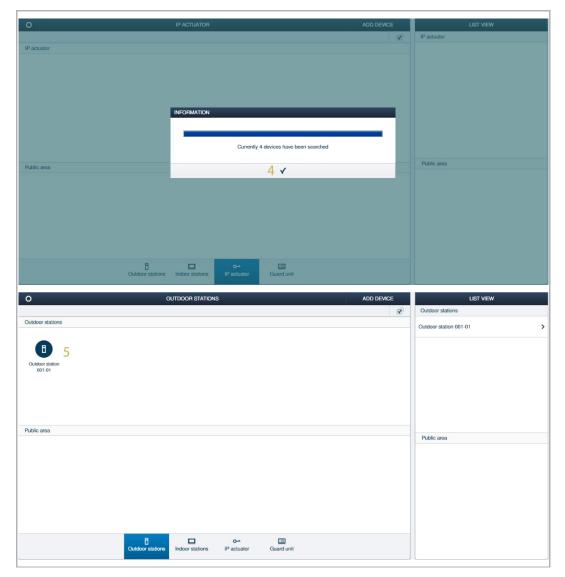
- [2] On the "Door Entry System" screen, click " O ".
- [3] Click "  $\checkmark$  " to continue.



		ADD DEVICE	LIST VIEW	
		<b>T</b>	Outdoor stations	
Outdoor stations			Outdoor station 001-01	>
Public area	INFORMATION Currently 1 devices have been searched Hide the window		Public area	
E Outdoor station	s Indoor stations IP actuator Guard unit			
0	OUTDOOR STATIONS	ADD DEVICE	LIST VIEW	
		<b>A</b>	Outdoor stations	
Outdoor stations			Outdoor station 001-01	
			Chubbel station of 1-01	>
Outdoor station 001-01				
Outdoor station 001-01			Public area	,

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

- [4] Search result is displayed on the screen; click "  $\checkmark$  " to continue.
- [5] The devices are displayed on the screen if successful.



# 9.2.2 Adding devices manually



Note

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

#### Precondition

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

# Adding the devices manually

Please follow the steps below:

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

BUILDING STRUCTURE	C-C-C- AR WARLENSE ECONARCENSM	PLACE - LINK	USER MANAGEMENT	ASTERNO ASTERNO	THE CONTROL	DOOR ENTRY SYSTEM
Design a building by creating floors and rooms	Configure the devices of the AccessControl system e.g. Cylinder, repeater	Locating and linking devices	Add and edit users. Create user groups	Create and edit actions	Create time control	Configurate door entry system devices, e.g. indoor station, outdoor station
🛔 jacky					Device	configuration 🌣 Preferences

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



#### Note

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

- [3] Select a device type from the drop-down list (e.g. "Indoor station").
- [4] Enter block number.
- [5] Enter floor number
- [6] Enter room number.
- [7] Enter device number.
- [8] Enter serial number.
- [9] Click "Save" to save.

0	NDOOR STATIONS	2 ADD DEVICE	LIST VIEW
Induce station 201- 0101-01	ADD DEVICE Device type Indoor station 3 Device addr. 1 4 1 5 1 6 2 7 Serial No. 102807A7F030593 {	· · ·	Indoor stations Indoor station 001-0101-01
	Cancel	9 Save	
Cutdoor stations	Indoor stations IP actuator Ge	ard unit	

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

(	С	)	

#### Note

If the device has already been signed by other "Smart Access Point", it will not be signed and "Sign failed" will be displayed on the "Abnormal devices" screen. see chapter 8.7.11 "Abnormal devices" on page 58.

0	INDOOR STATIONS	ADD DEVICE	LIST VIEW
		<b>™</b>	Indoor stations
	<b>D</b> <sup>10</sup>		Indoor station 001-0101-01
Indoor station 001- 0101-01	Indeer station 001- 0101-02		Indoor station 001-0101-02

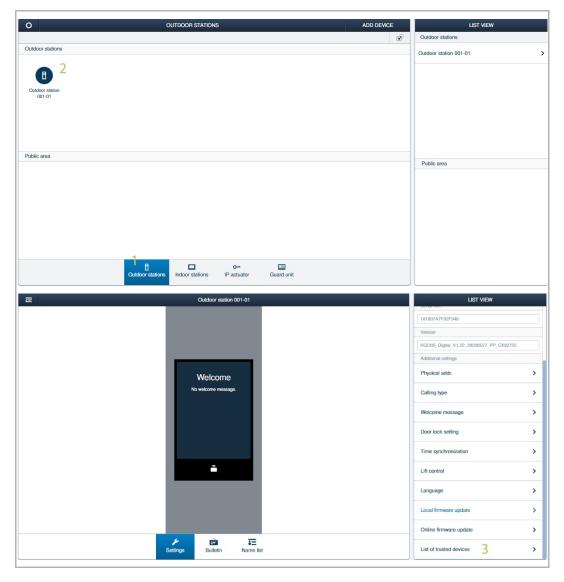
# 9.3 Managing the trusted devices

#### 9.3.1 Managing the trusted devices for outdoor station

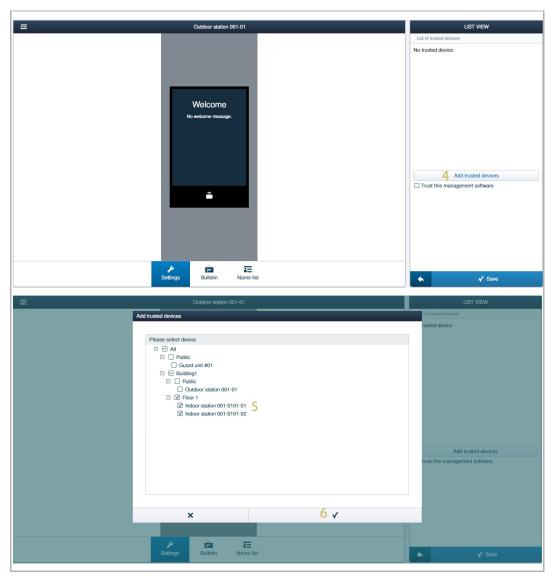
If you want to release the lock on the outdoor station, you need to check:

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

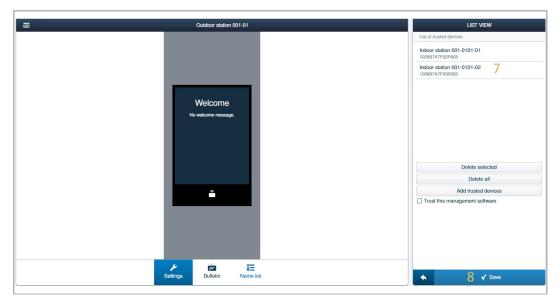
- [1] On the "Door Entry System" screen, click "Outdoor stations".
- [2] Click the designated outdoor station.
- [3] Scroll down the list and click "List of trusted devices".



- [4] Click "Add trusted devices".
- [5] Tick the check boxes to select the devices to be trusted.
- [6] Click "  $\checkmark$  " to confirm.



- [7] The result is displayed on the screen.
- [8] Click "Save" to save.

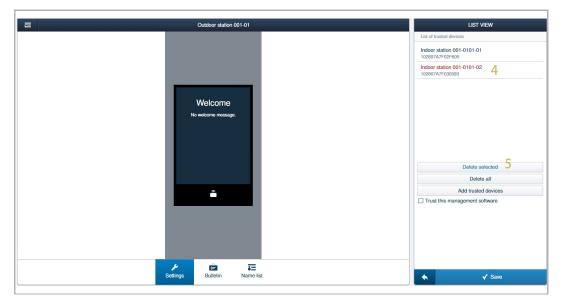


2. Removing the trusted devices

- [1] On the "Door Entry System" screen, click "Outdoor stations".
- [2] Click the designated outdoor station.
- [3] Scroll down the list and click "List of trusted devices".

O OUTDOOR STATIONS ADD DEVICE	LIST VIEW
of ∂	Outdoor stations
Outdoor stations	Outdoor station 001-01
Outdoor station OUT-01	
Public area	
	Public area
Outdoor stations IP actuator Guard unit	
Outdoor station 001-01	LIST VIEW
	101807A7F02F948
	Version
	HG005_Digital_V1.22_20200527_PP_CX92755
	Additional settings
Welcome	Physical addr.
No welcome message.	Calling type
	Welcome message >
	Door lock setting
	Time synchronization
â	Lift control
	Language >
	Local firmware update
	Online firmware update
ν Settings Bulletin Name list	List of trusted devices 3 >

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

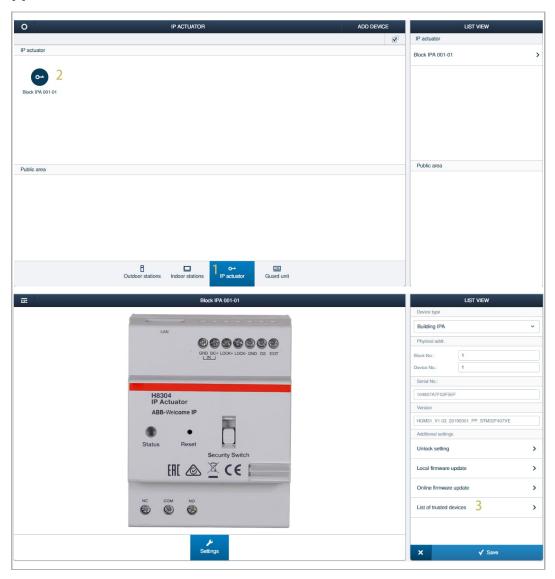


#### 9.3.2 Managing the trusted devices for IP actuator

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

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

- [1] On the "Door Entry System" screen, click "IP actuator".
- [2] Click the designated IP actuator.
- [3] Click "List of trusted devices".



- [4] Click "Add trusted devices".
- [5] Tick the check boxes to select the devices to be trusted.
- [6] Click "  $\checkmark$  " to confirm.

=	Block IPA 001-01	LIST VIEW
	BIDA 174 UUI-UT	LIST VIEW List of trusted devices
	LAN We want want want want want want want want	No trusted device  A Add trusted devices Trust this management software  X V Save
	Sounds	× V Save
	Block IDA 001-01	LIST VIEW
<b>—</b>	Block IPA 001-01	LIST VIEW
ē.	Block IPA 001-01 Add trusted devices	of trusted devices
	Add trusted device Please select device All Guad unit 401 Building1 Duble For 1 More station 001-0101-01 More station 001-0101-02	I d trusted devices  Add trusted devices
3	Add trusted devices           Please select device           □         All           □         Q hubic           ⑦         Guard unit 801           □         Public           □         Public	I d trusted devices Add trusted devices
	Add trusted device Please select device All Guad unit 401 Building1 Duble For 1 More station 001-0101-01 More station 001-0101-02	I d trusted devices  Add trusted devices

- [7] The result is displayed on the screen.
- [8] Click "Save" to save.

E Block IPA 001-01	LIST VIEW
	List of trusted devices
LAN	Guard unit #01 103807A7F02F93C
	Indoor station 001-0101-01 102807A7F02F605 7
CHO DC+ LOCK- OND DS EVIT	Indoor station 001-0101-02 102807A7F030593
H8304 IP Actuator ABB-Welcome IP Status Reset Security Switch ERE IN ICE	Delete selected Delete all Add trusted devices Trust this management software
NC COM NO	
Je Settings	× 8 🗸 Savo

2. Removing the trusted devices

- [1] On the "Door Entry System" screen, click "IP actuator".
- [2] Click the designated IP actuator.
- [3] Click "List of trusted devices".

O IP ACTUATOR ADD DEVICE	LIST VIEW
Ŕ	IP actuator
IP actuator	Block IPA 001-01
<b>2</b>	
Block IPA 001-01	
Public area	Public area
1 Mini urus	
B I Outdoor stations Indoor stations Indoor stations Guard unit	
GT Block IPA 001-01	LIST VIEW
	Device type
LAN	Building IPA ~
	Physical addr.
GND DC+LOCK+LOCK-GND DS EXIT	Block No.: 1 Davice No.: 1
	Serial No.:
H8304	104807A7F02F5EF
H8304 IP Actuator ABE-Weicome IP	Version
	HGM51_V1.03_20190301_PP_STM32F407VE
	Additional settings
Status Reset Security Switch	Unlock setting
ERE 💩 🗏 CE	Local firmware update
	Online firmware update
NC COM NO	List of trusted devices 3 >
4	

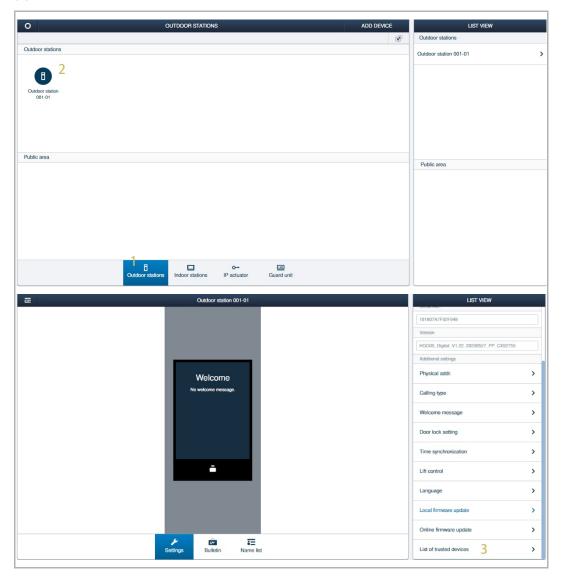
- [4] Click the designated device to select one by one (the selected devices are highlighted in red).
- [5] Click "Delete selected".

	LIST MEDI
LAN LAN CONCENCE LOCK- LOCK- OND DS EXT	List VIEW           Litt of trusted devices           Indoor station 001-0110-02           102807/A7505/5930C           Guard unit #01           103807/A7505/5930C           Indoor station 001-0101-01           102807/A7505/5605
H8304 IP Actuator ABB-Welcome IP Status Peset Security Switch ERE COM KO COM KO	Delete selected 5 Delete all Add trusted devices Trust this management software
Settings	× √ Save

# 9.3.3 Managing the trusted devices for "Smart Access Point"

1. Trusting the designated outdoor stations

- [1] On the "Door Entry System" screen, click "Outdoor stations".
- [2] Click the designated outdoor station.
- [3] Scroll down the list and click "List of trusted devices".



- [4] Click "Trust this management software".
- [5] The result is displayed on the list.
- [6] Click "  $\checkmark$  " to save.

a a constant	Outdoor station 001-01	LIST VIEW
<b>□</b>	Outdoor station 001-01 Welcome No welcome message	LIST VIEW List of trusted devices Index ration 001-0101-01 103807AFF067605 Index or station 001-0101-02 103807AFF06790C MGMT-SW 105807AFF08793C MGMT-SW 105807AFF087734 5 Delete selected Delete all Add trusted devices ☑ Trust this management software 4
	Settings Bulletin Name list	

2. Trusting the designated IP Actuators

- [1] On the "Door Entry System" screen, click "IP actuator".
- [2] Click the designated IP actuator.
- [3] Click "List of trusted devices".

O IP ACTUATOR ADD DEVICE	LIST VIEW
Ŕ	IP actuator
IP actuator	Block IPA 001-01
<b>2</b>	
Block IPA 001-01	
Public area	Public area
1 Mini uruu	
B I Outdoor stations Indoor stations Indoor stations Guard unit	
GT Block IPA 001-01	LIST VIEW
	Device type
LAN	Building IPA ~
	Physical addr.
GND DC+LOCK+LOCK-GND DS EXIT	Block No.: 1 Davice No.: 1
	Serial No.:
H8304	104807A7F02F5EF
H8304 IP Actuator ABE-Weicome IP	Version
	HGM51_V1.03_20190301_PP_STM32F407VE
	Additional settings
Status Reset Security Switch	Unlock setting
ERE 💩 🗏 CE	Local firmware update
	Online firmware update
NC COM NO	List of trusted devices 3 >
4	

- [4] Click "Trust this management software".
- [5] The result is displayed on the list.
- [6] Click "  $\checkmark$  " to save.

Block IPA 001-01	LIST VIEW
	List of trusted devices
LAN	Indoor station 001-0101-02 102807A7F030593
	Guard unit #01 103807A7F02F93C
UND DO+LOOK+LOOK-OND DS ENT	Indoor station 001-0101-01 102807A7F02F605
	MGMT-SW 105807A7F030734 5
H8304 IP Actuator	
ABB-Welcome IP	
Status Reset	Delete selected
Security Switch	Delete all
ERE 💩 🖉 CE	Add trusted devices
	✓ Trust this management software 4
NC COM NO	
4	
Sottings	× 6 ✓ Save

# 9.3.4 Emergency unlock

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

see chapter 9.3.3 "Managing the trusted devices for "Smart Access Point"" on page 92.

#### Release all public doors

- [1] On the configuration screen, click "SOS".
- [2] Enter the password for current admin user.
- [3] Click "Unlock all public doors".
- [4] The result status is displayed on the screen.

✓ <b>0</b> 🗟 sos 🕅	<b>)</b> Ф		MAIN MENU		
BUILDING STRUCTURE		IERGENCY UNLOCK(NORMA User name Password	L STATE This operation will unlock all public doorst jacky 		DOOR ENTRY SYSTEM
Design a building by creating floors and rooms	Configure the devices of the access control system e.g. Cylinder, repeater	Locating and linking devices	Add and edit users. Create and edit actions Create user groups	Create time control	Configurate door entry system devices, e.g. indoor station, outdoor station
jacky				Device	configuration 🌣 Preferences
BUILDING STRUCTURE		ERGENCY UNLOCK	Now the system is in emergency state, all the public doors are open.		DOOR ENTRY SYSTEM
Design a building by creating floors and rooms	Configure the devices of the access control system e.g. Cylinder,	Locating and linking devices	X Add and edit users. Create and edit actions Create user groups	Create time control	Configurate door entry system devices, e.g. indoor station, outdoor

# Close all public doors

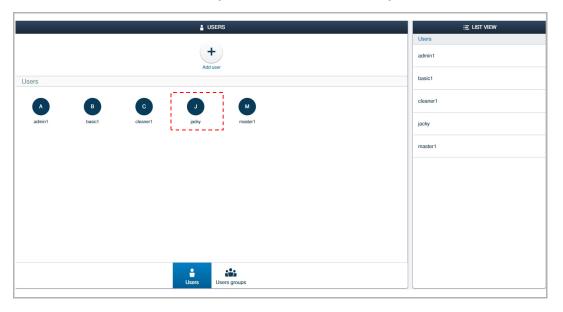
- [1] On the configuration screen, click "SOS".
- [2] Enter the password for the current admin user.
- [3] Click "Lock all public doors".
- [4] The result status is displayed on the screen.

✓ <b>0</b> R₂ sos ♠			MAIN MENU			
BUILDING STRUCTURE	EMERGI	ENCY UNLOCK(EMERGEN Attention User name Password	Now the system is in em doors are open. jacky 2	nergency state, all the public	The assessment	DOOR ENTRY SYSTEM
Design a building by creating floors and rooms	Configure the devices of Lo the access control system e.g. Cylinder, ropeator	ocating and linking devices	Add and edit users. Create user groups	Create and edit actions	Create time control	Configurate door entry system devices, e.g. indoor station, outdoor station
🛔 jacky	I \$		MAIN MENU		Device	configuration 🄅 Preferences
BUILDING STRUCTURE	EMERGE SOS	NCY UNLOCK Attention	Emergency unlock mode l	has been exited. 4	a contra	DOOR ENTRY SYSTEM
Design a building by creating floors and rooms	Configure the devices of Lo the access control system e.g. Cylinder, repeater	ocating and linking devices	X Add and edit users. Create user groups	Create and edit actions	Create time control	Configurate door entry system devices, e.g. indoor station, outdoor station
🍵 jacky						

# 9.4 Assigning permissions

# Access the designated user screen

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



# 9.4.1 Assigning the ID authentications to a user

You can assign the permission to a user by assigning both the ID authentications and the "Outdoor station" to the user.

1. Assigning the ID authentications to a user

Please follow the steps below:

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

Ξ			jacky			:≡ LIST VIEW	
						jacky	Û
						User role: Admin	
						Device sharing	
	1					Email address	
:*:	( <b>a</b>		6		Ε	Invitation code :	
Users groups(1)	ID authentication	Pairing devices	Cylinder	IP camera	Outdoor station	User information	
						Personal data	>
						Change password	>
							,
						User permission settings	
						Users groups(1)	>
						ID authentication	>
						Pairing devices	>
						Cylinder	>
						IP camera	>
						Outdoor station	>
		please set user permissi	on under each category			•	

- [2] Click "Add authentication".
- [3] Click "Add authentication for outdoor station".

i jacky	:E LIST VIEW
ADD NEW AUTHENTIFICATION METHOD Card type  Add authentication For access control Per outdoor station:	ID authentication
Profile Users groups Dauthoritication Pairing devices Cylinder IP camera Outdoor station	

- [4] Set card type to "Keycard/Tag".
- [5] Set validity period, there are 2 options:
  - Unlimited validity, it this type is selected, you can continue to the next step.
  - Limited validity, if this type is selected, you need to set the start date and end date by clicking " <sup>131</sup>
- [6] Set "Registered by" to "Outdoor station".
- [7] Select the designated outdoor station from the drop-down list for swiping the ID authentications.

(	С
_	

#### Note

For higher security, it is recommended to enable the "Safe mode" function on the designated IP touch 5 outdoor station when registering the ID authentications. For more information, see the product manual for IP touch 5 outdoor station.

- [8] Click "+" to select the floors to be controlled by the ID authentications (optional).
- [9] Click " $\sqrt{}$ " to continue.

TE .	🛓 jacky	i≣ LIST VIEW
ADD NEW (	CARD	
Add authentication	new card	
Card ty	pe Keycard/Tag 4	~
Validity	period Unlimited validity 5	•
Registe	outdoor station 6	•
Card re	ader Outdoor station 001-01 7	•
Avalab	Please click the button on the right to select the floor No.	+
		0
	× 9√	
Profile Users groups ID authentication F	Palifing devices Cylinder IP camera Outdoor station	
ADD NEW ( Select floor		
Plea	ase choose the floor number	
	5         15         25         35         45         55           6         16         26         36         46         56           7         17         27         37         47         57           8         18         28         38         48         58	
Sele	act all Inverse	
	× 8-2 v	

[10]Swipe the keycard or tag in front of the outdoor station.

[11]The outdoor station displays the card number and sounds a beep if successful.

Repeat steps 10-11 to register the ID authentications one by one.

	At Add new keycard/tag Please hold the keycard/tag against the card reader. Time out: 04:58 Please swipe 10 ×	
Advancements	Add new keycard/tag Please hold the keycard/tag against the card reader. Time out: 00:12 Current card number: 4052993446 11 1 success, 0 failures E	

# IC card specification

Operating frequency	13.56 MHz
Standard	ISO 14443A
Support card	Mifare one S50/S70, Mifare desfire EV1/EV2
Output format	Wiegand 26/34 bit

# ID card specification

Operating frequency	13.56 MHz
Standard	ISO 14443A
Support card	EM4100, EM4205, EM4305, EM4450, TK4100, T5567/T5577
Output format	Wiegand 26/34 bit



#### Note

Up to 200 ID authentications can be assigned to one user.

[12]The registered ID authentications are displayed on the screen. Click the designated ID authentication.

[13]Rename the ID authentication.

[14]Click " $\sqrt{}$ " to save.

īΞ	🛔 jacky	i≘ LIST VIEW
+ Add authentication	Elegaroration of the second of	Jacky - 1523685774 13 Information in access control Information in outdoor station Cord ID: 1523685774 Available foor No: Validity ported: Unlimited validity Immovement of the statement o
Profile	Users groups ID authentication(2) Pairing devices Cylinder IP camera Outdoor station(2)	× 14√ Save

# 9.4.2 Assigning the outdoor stations to a user

Please follow the steps below:

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

E			jacky			:E LIST VIEW	
						jacky	Û
						User role: Admin	
						Device sharing	
					1	Email address	
***			Ĩ		Β	Invitation code :	
Users groups	ID authentication(2)	Pairing devices	Cylinder	IP camera	Outdoor station	*Please connect to MyBuildings	
						User information	
						Personal data	>
						Change password	>
						User permission settings	
						Users groups	>
						ID authentication(2)	>
						Pairing devices	>
						Cylinder	>
						IP camera	>
						Outdoor station	>
		please set user permissi	on under each category			•	

[2] Click the designated outdoor station on the "Not assigned" section.

[3] Click "  $\checkmark$  " to confirm.

Repeat steps from 2-3 to assign the outdoor stations one by one.

12:	🛔 jacky			E LIST VIEW
Assigned				Jutdoor station
			A	
	INFORMATION			
	A Would you	like to add the device premissions	?	
Not assigned				
1	×	3 ✓		
8 2 8		5.		lot assigned
OS 001-01 OS 001-02				S 001-01
			0	S 001-02
	□ 3			
	entication(2) Pairing devices Cylin			
Frome Users groups ID autho	mucanon(z) ranng devices Cylin	ider in camera Outdoor station		

# 9.4.3 Assigning the unlock passwords to a user

Please follow the steps below:

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

Ξ	i	acky			; <u>≡</u> LIST VIEW	
					jacky	Ŵ
	J				User role: Admin	
					Device sharing	
1					Email address	
		Ē		8	Invitation code :	
Users groups(1) ID authentication	Pairing devices	Cylinder	IP camera	Outdoor station	User information	
					Personal data	>
					Change password	>
					User permission settings	
					Users groups(1)	>
					ID authentication	>
					Pairing devices	>
					Cylinder	>
					IP camera	>
					Outdoor station	>
	please set user permissio	on under each category			•	

- [2] Click "Add authentication".
- [3] Click "Add authentication for outdoor station".

🚈 🛔 jacky	:Ξ LIST VIEW
ADD NEW AUTHENTIFICATION METHOD Card type Add authentication For access control	ID authentication
Profile Users groups ID authontication Pairing devices Cylinder IIP camera Outdoor station	

- [4] Set card type to "Password".
- [5] Enter the name for the password.



**Note** This user name cannot be the same as the existing user name on "Smart Access Point".

[6] Enter the password.



**Note** This password cannot be the same as the existing password on "Smart Access Pont".

- [7] Set the lock type.
- [8] Set validity period, there are 2 options:
  - Unlimited validity, it this type is selected, you can continue to the next step.
  - Limited validity, if this type is selected, you need to set the start date and end date by clicking " <sup>31</sup>
- [9] Set unlock times.

[10]Click "+" to select the floors to be controlled by the ID authentications (optional).

TE	🛔 jacky		IE LIST VIEW
+	ADD AUTHENTICATION		
	Add authentic		
	Credential Type	Keycard/Tag ~	
	Validity period	Keycard/Tag	
	Register by	Password 4	
	Card No.	The card number can only be digit. If you enter more than one card, please use "," to separate	
	ADD AUTHENTICATION		
Add authentication	Credential Type	Password v	
	Name	Jacky 5	
	Password	112233 6	
	Lock Type	Default Lock 7 ~	
	Validity period	Limited validity 8 ~	
	Start	Aug 5, 2020 🛍 09:00 ~	
	End	Aug 5, 2020 🖬 17:00 🗸	
	Max Times	10 9	
	fumilable from No.	10 +	
	Available floor No.	11 ✓	
<u>i iii</u>	â 🛛	i 📥 🗄	
Profile Lisers groups ID a	Intentication Pairing devices	Cylinder IP.camera Outdoor station	

[11]The registered password is displayed on the screen. Click the password.

[12]Rename the password.

[13]View the unlock password.

Æ	🛔 jacky	i≣ LIST VIEW
+ Add authentication	L 11 JUNY 1	JACKY 12
Profile	Users groups ID authentication Pairing devices Cylinder IP camera Outdoor station	

# 9.5 Managing the backup

It is important to create a backup regularly.

For more information, see chapter 13.5 "Managing the backup" on page 317.

🔅 PREFERENCES						
Preferences	Project backups	Backup for Door Entry System - 20200806				
System information >	Create new project backup +	Description	1. Adding the devices - Done 2. Managing the trusted devices - Done 3. Assigning the parmission - Done			
Network settings >	Import project backup					
Localization >	Automatic backup Project backup is saved automatically when res >					
Project backups >	2020-08-04 13:07:29					
Firmware updates >						
MyBuildings Account >						
Service >						
Wi-Fi access point mode settings						
Third party authority >						
Abnormal devices >						
Onvif IPC list						
Misc settings >						
	*	×	✔ Save			

# 9.6 Removing permissions

# 9.6.1 Removing ID authentications from a user

Please follow the steps below:

- [1] On the designated user screen, click "ID authentication" to access the corresponding screen.
- [2] Click the designated ID authentication.
- [3] Click " 🔟 ".
- [4] Click "  $\checkmark$  " to confirm.

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

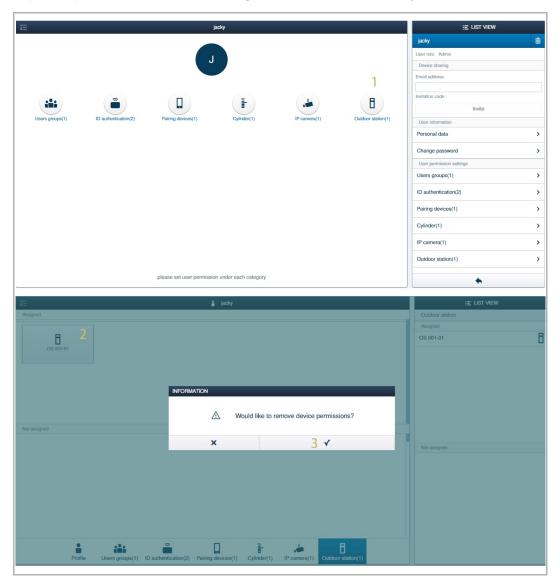
E	jacky			:≡ LIST VIEW	
				jacky	Û
				User role: Admin	
	J			Device sharing	
1				Email address	
::: ( â			8	Invitation code :	
Users groups(1) ID authentication(2) F	Pairing devices(1) Cylinder(1)	IP camera(1)	Outdoor station(1)		
				User information Personal data	>
				Personal data	
				Change password	>
				User permission settings	
				Users groups(1)	>
				ID authentication(2)	>
				Pairing devices(1)	>
				Cylinder(1)	>
				IP camera(1)	>
				Outdoor station(1)	>
	ease set user permission under each category				
	ease set user permission under each category			•	
12	🛔 jacky			i≣ LIST VIEW	
	iacky			:Ξ LIST VIEW	
SII + Add authentication Crylecoler 001	≗ jacky © 2			4052993446	
	<u>)</u>			4052993446 Information in access control + Information in outdoor station	
Add authentication Cylinder 001 00219222	<u>)</u>			405293446 Information in access control H Information in outdoor station Card ID: 405293446	
Add authentication Cylinder 001 00219222	<u>)</u>			4052993446 Information in access control Information in outdoor station Card Or.4052993446 Available floor No.: 10	
Add authentication Cylinder 001 00219222	<u>)</u>			4052993446 Information in access control Information in auditor station Carel DD : 4002993446 Available Book Price:	
Add authentication Cylinder 001 00219222	INFORMATION			4052993446 Information in access control Information in outdoor station Card Or.4052993446 Available floor No.: 10	
Add authentication Cylinder 001 00219222	INFORMATION	e to delete this authentic	ation?	4052993446 Information in access control Information in audioor station Card GD: 4050990446 Available floor No.: 10 Vaiding period: 2020-07-23 – 2020-07-24	
Add authentication Cylinder 001 00219222	0 NFORMATION		ation?	4052993446 Information in access control Information in audioor station Card GD: 4050990446 Available floor No.: 10 Vaiding period: 2020-07-23 – 2020-07-24	
Add authentication Cylinder 001 00219222	INFORMATION	e to delete this authentic: $4 \checkmark$	ation?	4052993446 Information in access control Information in audioor station Card GD: 4050990446 Available floor No.: 10 Vaiding period: 2020-07-23 – 2020-07-24	
Add authentication Cylinder 001 00219222	0 NFORMATION		ation?	4052993446 Information in access control Information in audioor station Card GD: 4050990446 Available floor No.: 10 Vaiding period: 2020-07-23 – 2020-07-24	
Add authentication Cylinder 001 00219222	0 NFORMATION		ation?	4052993446 Information in access control Information in outdoor station Card GD: 4050990446 Available floor No.: 10 Vaiddry period: 2220-07-23 – 2020-07-24	
Add authentication Cylinder 001 00219222	0 NFORMATION		ation?	4052993446 Information in access control Information in outdoor station Card GD: 4050990446 Available floor No.: 10 Vaiddry period: 2220-07-23 – 2020-07-24	
Add authentication Cylinder 001 00219222	0 NFORMATION		ation?	4052993446 Information in access control Information in outdoor station Card GD: 4050990446 Available floor No.: 10 Vaiddry period: 2220-07-23 – 2020-07-24	
Add authentication Cylinder 001 00219222	0 NFORMATION		ation?	4052993446 Information in access control Information in outdoor station Card GD: 4050990446 Available floor No.: 10 Vaiddry period: 2220-07-23 – 2020-07-24	
Add authentication Cylinder 001 00219222	0 NFORMATION		ation?	4052993446 Information in access control Information in outdoor station Card GD: 4050990446 Available floor No.: 10 Vaiddry period: 2220-07-23 – 2020-07-24	
Add authoritication Qrifrage 001 1103375355722886	0 NFORMATION	4 ∢	ation?	4052993446 Information in access control Information in outdoor station Card GD: 4050990446 Available floor No.: 10 Vaiddry period: 2220-07-23 – 2020-07-24	

# 9.6.2 Removing outdoor stations from a user

Please follow the steps below:

- [1] On the designated user screen, click "Outdoor station" to access the corresponding screen.
- [2] Click the designated outdoor station on the "Assigned" section
- [3] Click "  $\checkmark$  " to confirm.

Repeat steps from 2-3 to remove the designated outdoor stations one by one.



# 9.6.3 Removing the unlock passwords from a user

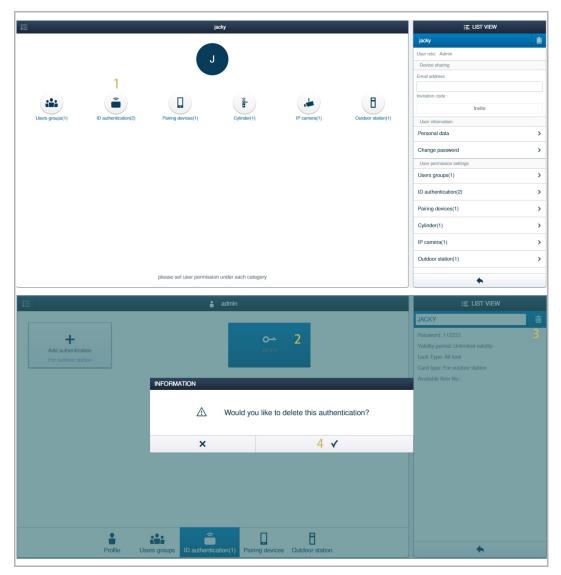
Please follow the steps below:

- [1] On the designated user screen, click "ID authentication" to access the corresponding screen.
- [2] Click the designated unlock password.

[3] Click " 🔟 ".

[4] Click "  $\checkmark$  " to confirm.

Repeat the steps from 2~4 to remove the unlock passwords one by one.



## 9.6.4 Removing the QR codes from a user

Welcome App can create QR codes for the user to to release the lock on the IP touch 5 outdoor station. For creating a QR code, see the product manual for Welcome App.

"Smart Access Point" can remove the QR code.

- [1] On the designated user screen, click the QR code.
- [2] View the validity period.
- [3] Click " 🔟 ".
- [4] Click "  $\checkmark$  " to remove the QR code.

Ξ	8111212		∷⊒ LIST VIEW
Add authentication For outdoor station	0 11		12 3 iii Or code: E32F8CBEC4B05BF2 Validity period: 2020-08-06 08:35 - 2020-08:21 08:35 Lock Type: Subsidiary Lock 2 Card type: For outdoor station
	INFORMATION  Would you like to delete	4	
	×	4 🗸	

# 9.7 Configuring the indoor station

#### Access the designated Indoor station screen

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

¥ 🚳 ि so	os 🕥 🕽		MAIN MENU			
	RF WIRELESS CONNECTION	PLACE + LINK	USER MANAGEMENT	ACTIONS		DOOR ENTRY SYSTEM
Design a building by creating floors and rooms	Configurate the devices of the access control system e.g. cylinders, repeaters	Locating and linking devices	Add and edit users. Create user groups	Create and edit actions	Create time control	Configurate door entry system devices, e.g. indoor station, outdoor station
abb					Device configura	ation 🔅 Preferences

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

0	INDOOR STATIONS	ADD DEVICE	LIST VIEW
		<b>N</b>	Indoor stations
8 8			Indoor station 001-0101-01
Indoor station 001- 0101-01 0102-01			Indoor station 001-0102-01
	[]		
Cutdoor stations	Indoor stations IP actuator Guard unit	Management software	

# 9.7.1 Changing the language

- [1] On the designated indoor station screen, click "Language".
- [2] Select the language from the drop-down list.
- [3] Click "  $\checkmark$  " to save.

æ	Indoor station 001-0101-01	LIST VIEW
		Jacky
		Serial No.:
		102807A7F02F605
		Version
		HGI16_Main_V9.99_20190711_PP_IMX6SOLO
		Additional settings
	No screensaver set for this indoor station yet	Physical addr.
	ind actionation and in an analysis action for	Logic addr.
		Duplicate settings >
		Local firmware update >
		Online firmware update >
		Resident(s)/Tenant(s)
		Screensaver >
		Floor plan >
	يم Settings	Language 1
		· · ·
=	Indoor station 001-0101-01	LIST VIEW
æ	Indoor station 001-0101-01	LIST VIEW
<b></b>	Indoor station 001-0101-01	
55 1	No screensaver set for this indoor station yet	Language

# 9.7.2 Renaming the device

Please follow the steps below:

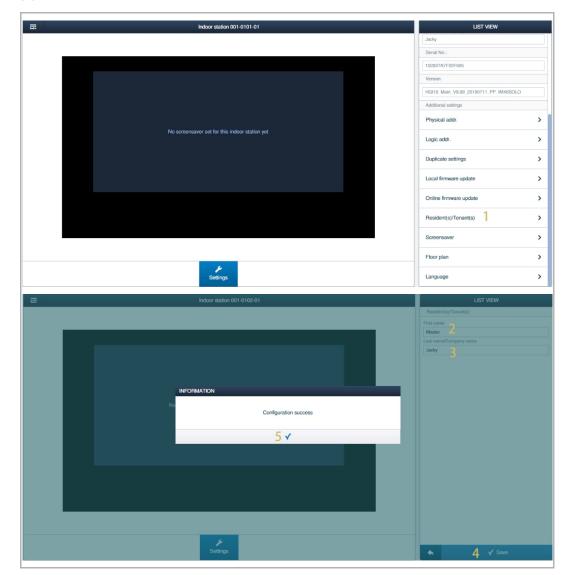
- [1] On the designated indoor station screen, click "Resident(s)/Tenant(s)".
- [2] Enter the first name.
- [3] Enter the last name or the company name.

(	С	)	

Note

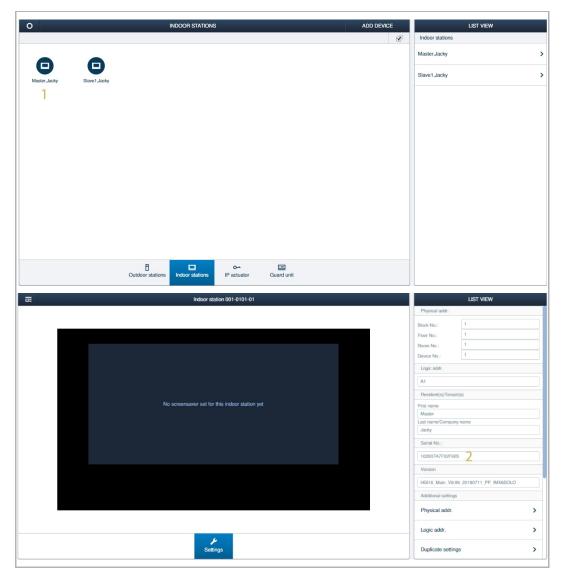
If the resident has multiple indoor stations in the apartment, it is recommended to use the appropriate name to show the association (e.g. "Master", "Slave 1" etc.).

- [4] Click "  $\checkmark$  " to save.
- [5] Click "  $\checkmark$  " to confirm.



# 9.7.3 Viewing the serial number

- [1] On the "Indoor stations" screen, click the designated indoor staiton.
- [2] The serial number is displayed on the screen. It is recommended to write down the serial number for futher use.



# 9.7.4 Managing the physical address



#### Note

If the master indoor station changes its physical address, the slave indoor stations need to obtain the signature again from "Smart Access Point". Please write down the serial number of the slave indoor stations before changing the physical address. see chapter 9.7.3 "Viewing the serial number" on page 116.

Please follow the steps below:

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

æ	Indoor station 001-0101-01	LIST VIEW	
		Jacky	
		Serial No.:	
		102807A7F02F605	
		Version	
		HGI16_Main_V9.99_20190711_PP_IMX6SOLO	
		Additional settings	
		Physical addr.	>
	No screensaver set for this indoor station yet	Logic addr.	>
		Duplicate settings	>
		Local firmware update	>
		Online firmware update	>
		Resident(s)/Tenant(s)	>
		Screensaver	>
		Floor plan	>
	Settings	Language	>

- [2] Change the physical address.
- [3] Click "  $\checkmark$  " to save.
- [4] Click "  $\checkmark$  " to confirm.

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

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

Indoor station 001-0101-01	LIST VIEW
Physics	al addr.
Block No.	a.: 1
Floor No.	
Room N	o.: 2 2
Device N	No.: 1
INFORMATION	
No.	
Configuration success	
4 🗸	
4	
Settings	3 √ Save

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

0	INDOOR STATIONS	ADD DEVICE	LIST VIEW
		(T)	Indoor stations
0 0			Slave1,Jacky
Slave1,Jacky Master,Jacky			Master,Jacky
	INFORMATION		
	△ Communication failed		
	7 🗸		
Cutdoor stations	Indoor stations IP actuator Guard unit		

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

Stave 1, Jacky	8 8	Indoor stations Slave 1, Jacky
	8	Slave1,Jacky
outer poury maker outry		Master, Jacky
Cutdoor stations IP actuator Guard unit		

[9] Click the slave indoor station.

[10]Click "Delete".

[11]Click "Confirm", followed by "  $\checkmark$  ".

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

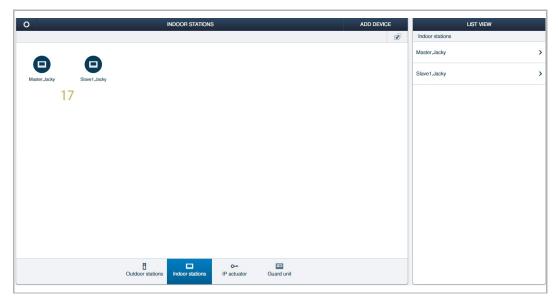
[13]Set "Device type" to "Indoor station".

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

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

[16]Click "Save", followed by "  $\checkmark$  ".

<b>.</b>		INDOO	R STATIONS			LIST VIEW	
		Select multiple devi	COS	Select all	Indoor stations		
					Buildingt		
0	•				Slave1, Jacky		
0					Master,Jacky		
Slave 1 Jacky	Master, Jacky						
		INFORMATION					
			If continue, the selected device will be deleted				
		×	11 Confirm				
					×	Next	Delete
					^		
0		INDOOR STATIONS	12	ADD DEVICE		LIST VIEW	
0		INDOOR STATIONS	12	ADD DEVICE	Indoor stations	LIST VIEW	
0		INDOOR STATIONS	12		Indoor stations Master,Jacky	LIST VIEW	, ,
0			12			LIST VIEW	>
O Master,Jacky		INDOOR STATIONS				LIST VIEW	>
•			12 Indoor station 13			LIST VIEW	>
•		ADD DEVICE Device type	Indoor station 13			LIST VIEW	>
•		ADD DEVICE	Indoor station 13			LIST VIEW	>
•		ADD DEVICE Device type	Indoor station 13			LIST VIEW	>
•		ADD DEVICE Device type	Indoor station 13			LIST VIEW	>
•		ADD DEVICE Device type	Indoor station 13			LIST VIEW	>
•		ADD DEVICE Device type	Indoor station 13 1 1 2 14 2			LIST VIEW	>
•		ADD DEVICE Device type	Indoor station 13			LIST VIEW	>
•		ADD DEVICE Device type Device addr. Serial No.	Indoor station 13 1 1 2 14 2 102807A7F030593 15			LIST VIEW	>
•		ADD DEVICE Device type Device addr.	Indoor station 13 1 1 2 14 2 102807A7F030593 15			LIST VIEW	>
•		ADD DEVICE Device type Device addr. Serial No.	Indoor station 13 1 1 2 14 2 102807A7F030593 15			LIST VIEW	>
•		ADD DEVICE Device type Device addr. Serial No.	Indoor station 13 1 1 2 14 2 102807A7F030593 15			LIST VIEW	>
•		ADD DEVICE Device type Device addr. Serial No.	Indoor station 13 1 1 2 14 2 102807A7F030593 15			LIST VIEW	>
•	8	ADD DEVICE Device type Device addr. Serial No. Care	Indoor station 13  1  2 14  2  102807A7F030593 15  cel 16 Save				>
•	e Outdoor stations	ADD DEVICE Device type Device addr.	Indoor station 13 1 1 2 14 2 102807A7F030593 15				>



[17]Rename the slave indoor station. see chapter 9.7.2 "Renaming the device" on page 115.

# 9.7.5 Managing the logic address

Please follow the steps below:

- [1] On the master indoor station screen, click "Logic addr.".
- [2] Enter the logic address. The address could not be the same to the exist one on "Smart Access Point".
- [3] Click " $\sqrt{}$ " to save.
- [4] Click " $\sqrt{}$ " to confirm.

E Indoor station 001-0101-01	LIST VIEW
	Jacky
	Serial No.:
	102807A7F02F605
	Version
	HGI16_Main_V9.99_20190711_PP_IMX6SOLO
	Additional settings
No screensaver set for this indoor station yet	Physical addr.
NO SERVITSION FOR THIS IRROOT SUBTION YOU	Logic addr. 1
	Duplicate settings
	Local firmware update
	Online firmware update >
	Resident(s)/Tenant(s)
	Screensaver >
6	Floor plan
مر Settings	Language >
금 Indoor station 001-0101-01	
GE Indoor station 001-0101-01	LIST VIEW
GE Indoor station 001-0101-01	
GE Indoor station 001-0101-01	Logic addr.
GE Indoor station 001-0101-01	Logic addr.
GE Indoor station 001-0101-01	Logic addr.
	Logic addr.
INFORMATION	Logic addr.
	Logic addr.
INFORMATION	Logic addr.
INFORMATION Na Configuration success	Logic addr.



# Note

The logic address set on the indoor station can be used on the outdoor station. see chapter 9.7.5 "Managing the logic address" on page 122.

# 9.7.6 Managing the screensaver

- [1] On the master indoor station screen, click "Screensaver".
- [2] Click "Upload screensaver image".
- [3] Click "Browse" to select the desiganted image (only .jpg is supported, maximum resolution of the image is 1024 x 600 pixels).
- [4] Click "  $\checkmark$  " to confirm.
- [5] Click "  $\checkmark$  " to upload.

æ	Indoor station 001-0101-01	LIST VIEW	
		Jacky	
		Serial No.:	
		102807A7F02F605	
		Version	
		HGI16_Main_V9.99_20190711_PP_IMX6SOLO	
		Additional settings	
	No screensaver set for this indoor station yet	Physical addr.	>
	i vu sureensaver sei nu iins inkuun saaluur yei	Logic addr.	>
		Duplicate settings	>
		Local firmware update	>
		Online firmware update	>
		Resident(s)/Tenant(s)	>
		Screensaver 1	>
		Floor plan	>
	F Settings	Language	>
=	Indoor station 001-0101-01	LIST VIEW	
æ	Indoor station 001-0101-01	LIST VIEW Scroensaver	
æ	Indoor station 001-0101-01		
	Indoor station 001-0101-01	Screensaver	5 .
	Indoor station 001-0101-01	Screensaver Upload screensaver image 2	s .
æ	Indoor station 001-0101-01	Screensaver Upload screensaver image 2	S .
æ	Indoor station 001-0101-01	Screensaver Upload screensaver image 2	S .
	INFORMATION	Screensaver Upload screensaver image 2	5.
		Screensaver Upload screensaver image 2	5.
-	INFORMATION	Screensaver Upload screensaver image 2	5.
-	Upload screensaver image	Screensaver Upload screensaver image 2	5.
æ	Upload screensaver image	Screensaver Upload screensaver image 2	S.
æ	Upload screensaver image	Screensaver Upload screensaver image 2	5.
	Upload screensaver image	Screensaver Upload screensaver image 2	5.
	Upload screensaver image	Screensaver Upload screensaver image 2	5.
	Upload screensaver image	Screensaver Upload screensaver image 2	5
	Upload screensaver image	Screensaver Upload screensaver image 2	5.

# 9.7.7 Managing the floorplan

- [1] On the master indoor station screen, click "Floor plan".
- [2] Click "Upload floorplan".
- [3] Click "Browse" to select the desiganted image (only .jpg is supported, maximum resolution of the image is 1024 x 600 pixels).
- [4] Click "  $\checkmark$  " to confirm.
- [5] Click "  $\checkmark$  " to upload.

료 Indoor station 001-0101-01	LIST VIEW
	Jacky
	Serial No.:
	102807A7F02F605
	Version
	HGI16_Main_V9.99_20190711_PP_IMX6SOLO
	Additional settings
No screensaver set for this indoor station yet	Physical addr.
ing descentation and the final magnet autom for	Logic addr.
	Duplicate settings
	Local firmware update
	Online firmware update
	Resident(s)/Tenant(s)
	Screensaver >
	Floor plan
Settings	Language >
E Indoor station 001-0101-01	LIST VIEW
Endoor station 001-0101-01	LIST VIEW Floor plan
문 Indoor station 001-0101-01	
EE Indoor station 001-0101-01	Floor plan
료 Indoor station 001-0101-01	Floor plan Upload floorplan
EE Indoor station 001-0101-01	Floor plan Upload floorplan
Indoor station 001-0101-01	Floor plan Upload floorplan
INFORMATION	Floor plan Upload floorplan
	Ploor plan Upload floorplan 2 () Use an image / logo with 1024 x 600 pixels .
INFORMATION Upload floorplan	Floor plan Upload floorplan
INFORMATION Upload floorplan	Ploor plan Upload floorplan 2 (1) Use an image / logo with 1024 x 600 plaets.
INFORMATION Upload floorplan	Ptoor plan Upload floorplan 2 ① Use an image / logo with 1024 x 600 plxets .
INFORMATION Upload floorplan	Ploor plan Upload floorplan 2 (1) Use an image / logo with 1024 x 600 plaets.
INFORMATION Upload floorplan	Ploor plan Upload floorplan 2 (1) Use an image / logo with 1024 x 600 plaets.
INFORMATION Upload floorplan	Ploor plan Upload floorplan 2 (1) Use an image / logo with 1024 x 600 plaets.
INFORMATION Upload floorplan	Ploor plan Upload floorplan 2 (1) Use an image / logo with 1024 x 600 plaets.
INFORMATION Upload floorplan	Ploor plan Upload floorplan 2 (1) Use an image / logo with 1024 x 600 plaets.
INFORMATION Upload floorplan	Ploor plan Upload floorplan 2 (1) Use an image / logo with 1024 x 600 plaets.

# 9.7.8 Duplicating the settings

- [1] On the master indoor station screen, click "Duplicate settings".
- [2] Click to select the designated indoor station to be dupliacted.
- [3] Tick the check boxes to select the settings to be duplicated.
- [4] Click " $\sqrt{}$ " to confirm.

=	Indoor station 001-0101-01	LIST VIEW	
		Jacky	
		Serial No.:	
		102807A7F02F605	
		Version	
		HGI16_Main_V9.99_20190711_PP_IMX6SOLO	
		Additional settings	
	No screensaver set for this indoor station yet	Physical addr.	>
		Logic addr.	>
		Duplicate settings	>
		Local firmware update	>
		Online firmware update	>
		Resident(s)/Tenant(s)	>
		Screensaver	>
		Floor plan	>
	Settings	Language	>
æ	Indoor station 001-0101-01	LIST VIEW	
æ	Indoor station 001-0101-01	Duplicate settings	
	Indoor station 001-0101-01		
Θ	G	Duplicate settings	
Θ	E total aday	Duplicate settings Settings choose Guard unit setttings	
Θ	G	Duplicate settings settings doose Guard unit settings General settings 3	
Θ	E total aday	Duplicate settings Settings doose Guard unit settings General settings Screensaver se	
Θ	E total aday	Duplicate settings       Settings choose       General settings       General settings       Screensaver settings       Alarm system	
Θ	E total aday	Duplicate settings       Settings choose       General settings       General settings       Screensaver settings       Alarm system	
Θ	E total aday	Duplicate settings       Settings choose       General settings       General settings       Screensaver settings       Alarm system	
Θ	E total aday	Duplicate settings       Settings choose       General settings       General settings       Screensaver settings       Alarm system	
Θ	E total aday	Duplicate settings       Settings choose       General settings       General settings       Screensaver settings       Alarm system	
Θ	E total aday	Duplicate settings       Settings choose       General settings       General settings       Screensaver settings       Alarm system	
Θ	E total aday	Duplicate settings       Settings choose       General settings       General settings       Screensaver settings       Alarm system	
Θ	E total aday	Duplicate settings       Settings choose       General settings       General settings       Screensaver settings       Alarm system	
Θ	E total aday	Duplicate settings       Settings choose       General settings       General settings       Screensaver settings       Alarm system	
Θ	E total aday	Duplicate settings       Settings choose       General settings       General settings       Screensaver settings       Alarm system	
Θ	E total aday	Duplicate settings       Settings choose       General settings       General settings       Screensaver settings       Alarm system	

# 9.7.9 Updating the firmware

see chapter 13.4 "Updating the firmware" on page 309.

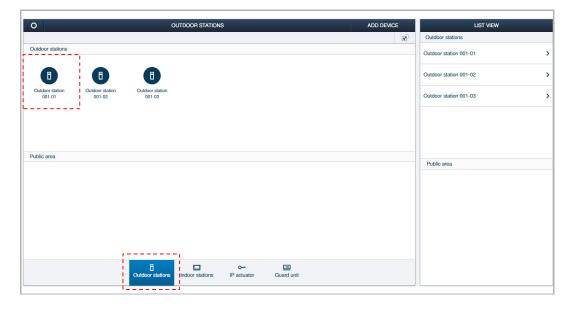
# 9.8 Configuring the outdoor station

#### Access the designated outdoor station screen

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

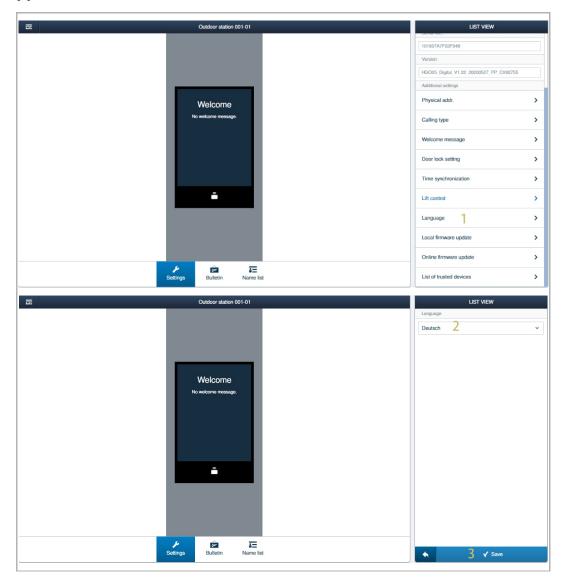
❤ <mark>16</mark> 9 F∞ SC	os 🕥 🕽		MAIN MENU			
	RF WIRELESS CONNECTION	PLACE + LINK	USER MANAGEMENT	ACTIONS		DOOR ENTRY SYSTEM
Design a building by creating floors and rooms	Configurate the devices of the access control system e.g. cylinders, repeaters	Locating and linking devices	Add and edit users. Create user groups	Create and edit actions	Create time control	Configurate door entry system devices, e.g. indoor station, outdoor station
abb					Device configura	ation 🌣 Preferences

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



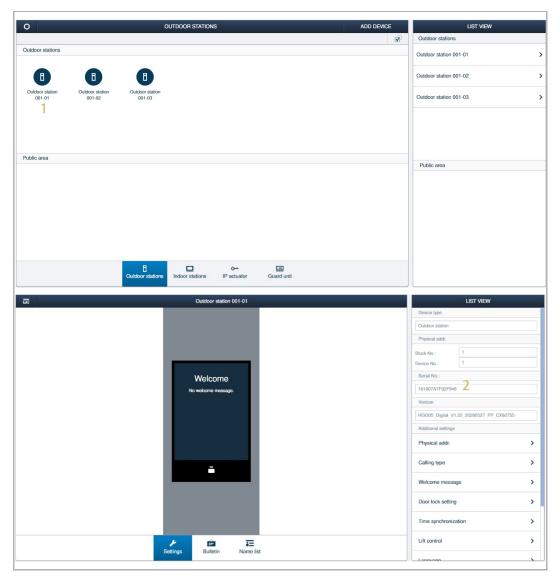
# 9.8.1 Changing the language

- [1] On the designated outdoor station screen, click "Language".
- [2] Select the language from the drop-down list.
- [3] Click "  $\checkmark$  " to save.



#### 9.8.2 Viewing the serial number

- [1] On the "Outdoor stations" screen, click the designated outdoor staiton.
- [2] The serial number is displayed on the screen. It is recommended to write down the serial number for futher use.



# 9.8.3 Managing the physical address

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

GE Outdoor station 001-02	LIST VIEW
	Device type
<i>st.</i>	Outdoor station
	Physical addr.
	Block No.: 1
	Device No.: 2
	Serial No.:
	101807A7F02D43D
	Version
	HGO05_Digital_V1.02_20190215_PP_CX92755
	Additional settings
	Physical addr.
M. Mueller	
	Door lock setting
	Time synchronization
	Lift control
	Local firmware update >
	Design label
Settings	Onlino firmutaro undato

There are 3 types devices for selection.

1. Outdoor station

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

규 Outdoor station 001-02	LIST VIEW
2.	Device type
#/n	Outdoor station ~
s s•	Physical addr.
	Block No.: 1
	Device No.: 2
M. Mueller	
1 August 1 Aug	
Settings	♠ ✓ Save

#### 2. Gate station

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

G Outdoor station 001-02	LIST VIEW
z.	Device type
**	Gate station ~
	Physical addr.
	Device No.: 2
M. Muetler	
مر Sortings	♦ ✓ Save

#### 3. Second-confirm station

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

G. Outdoor station 001-02	LIST VIEW
24	Device type
<i>P/</i>	Second-confirm station ~
	Physical addr.
	Block No.: 1
	Floor No.: 1 Room No.: 1
	Device No.: 1
M. Musiler	
р Sottings	♦ ✓ Save

# Note

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

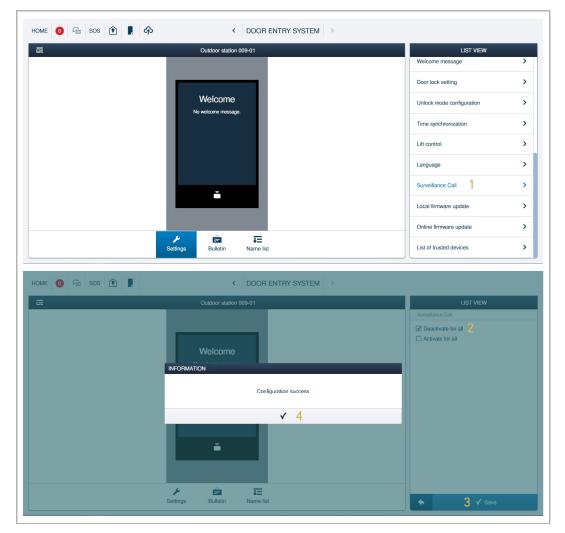
0

#### 9.8.4 Surveillance call

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

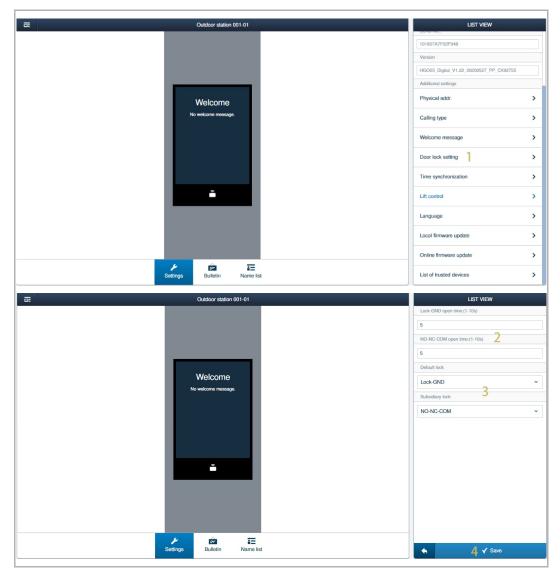
Please follow the steps below to deactivate the function:

- [1] On the designated outdoor station screen, click "Surveillance call".
- [2] Tick the check box "Deactivate for all".
- [3] Click "Save".
- [4] Click "√".



# 9.8.5 Unlock setting

- [1] On the designated outdoor station screen, click "Door lock setting".
- [2] Set the unlock time for the locks.
- [3] Set the lock type for the locks.
- [4] Click " $\sqrt{}$ " to save.

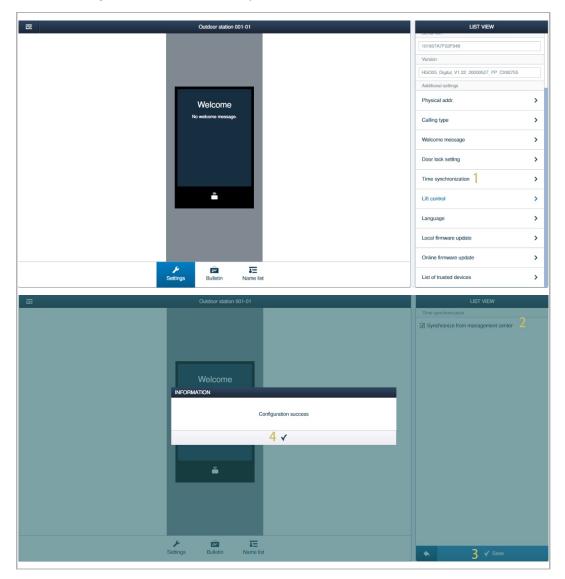


# 9.8.6 Time synchronization

Please follow the steps below:

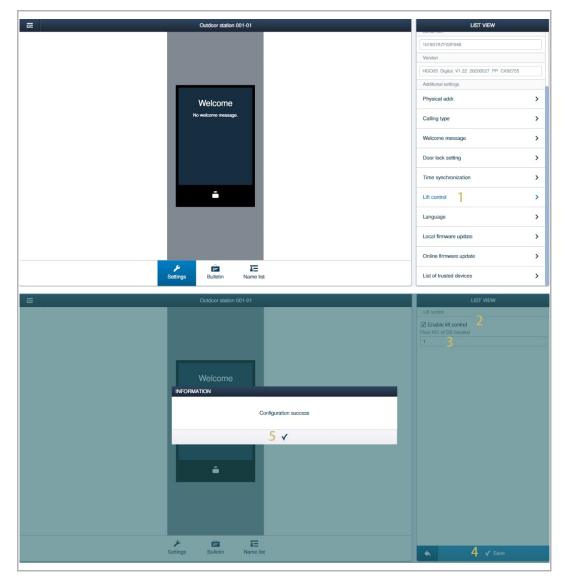
- [1] On the designated outdoor station screen, click "Time synchronization".
- [2] Tick the check box to enable the function.
- [3] Click " $\sqrt{}$ " to save.
- [4] Click " $\sqrt{}$ " to confirm.

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



# 9.8.7 Managing Lift control

- [1] On the designated outdoor station screen, click "Lift control".
- [2] Tick the check box to enable the function.
- [3] Enter the floor where the outdoor station is located.
- [4] Click " $\sqrt{}$ " to save.
- [5] Click " $\sqrt{}$ " to confirm.



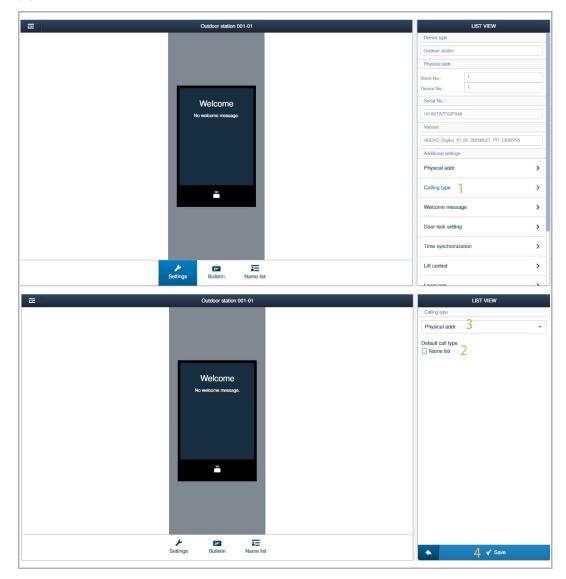
# 9.8.8 Managing the trusted devices

see chapter 9.3.1 "Managing the trusted devices for outdoor station" on page 82.

# 9.8.9 Initiating a call via the physical address

This chapter applies to the IP touch 5 outdoor station and IP keypad outdoor station. Please follow the steps below:

- [1] On the designated outdoor station screen, click "Call type".
- [2] Disable the "Name list" (only applied to IP touch 5 outdoor station).
- [3] Set "Call type" to "Physical addr."
- [4] Click " $\sqrt{}$ " to save.

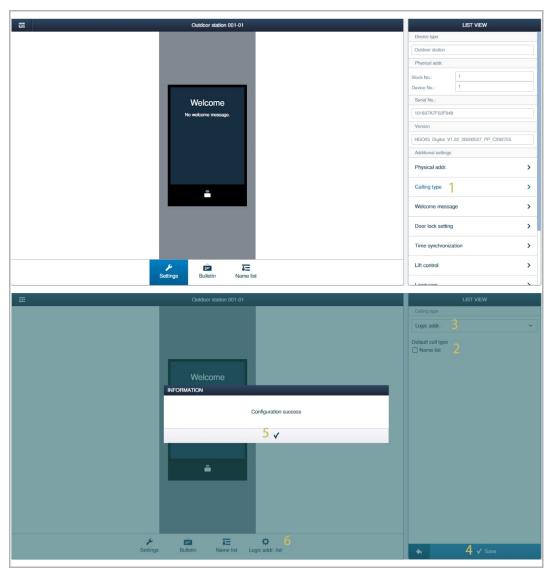


## 9.8.10 Initiating a call via the logic address

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

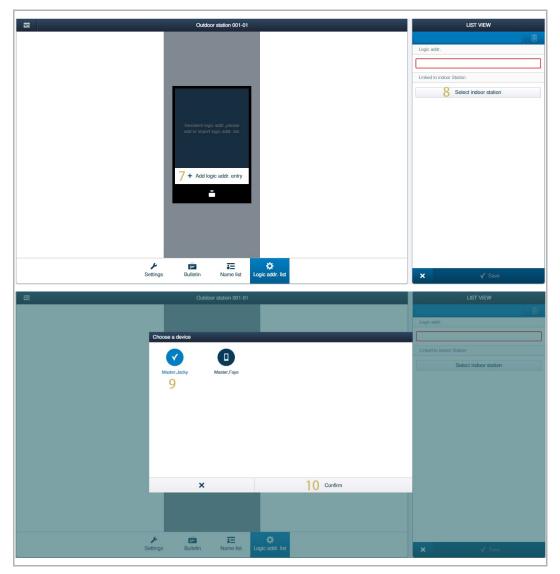
1. Adding the logic address

- [1] On the designated outdoor station screen, click "Call type".
- [2] Disable the "Name list" (only applies to the IP touch 5 outdoor station).
- [3] Set "Call type" to "Logic addr."
- [4] Click " $\sqrt{}$ " to save.
- [5] Click " $\sqrt{}$ " to confirm.
- [6] "Logic addr. list" is displayed on the screen. Click it to continue.



- [7] On the "Logic addr. list" screen, click "+".
- [8] Click "Select indoor station".
- [9] Click to select the designated indoor station.

[10]Click "Confirm".



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

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

[13]Click "  $\checkmark$  " to save, followed by "  $\checkmark$  " to confirm.

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

Cutdoor station 001-01	LIST VIEW
Hwister layis addr. plane add or import logic addr. int. Add logic addr. entry C	Logic addr. At 12 Linked to indeer Station Select indoor station Indoor station 001-0101-01 11
Settings Bulletin Name list Logic addr. list	× 13 √ Save

2. Importing the logic addresses

Please follow the steps below:

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



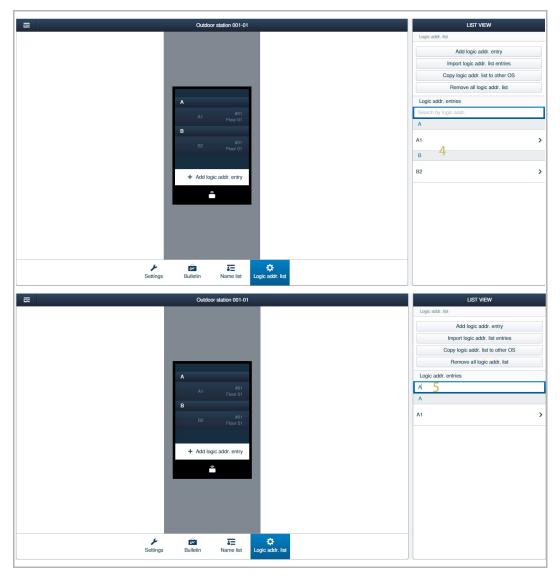
**Note** It is recommended to set the logic address for the indoor station before importing.

[2] Click to select the designated indoor stations.

[3] Click "Import", followed by "  $\checkmark$  ".

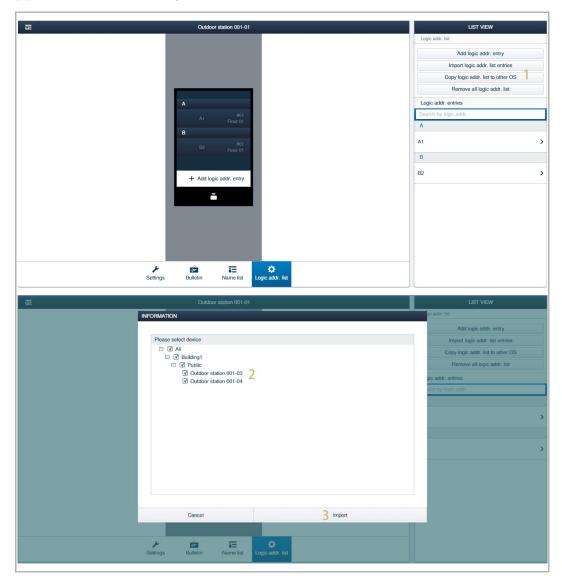
	Outdoor station 001-01		LIST VIEW
			Logic addr. list
			Add logic addr. entry
			Import logic addr. list entries
			Logic addr. entries
			Inexistent logic address.
	Inexistent logic addr.,please add or import logic addr. list.		
	+ Add logic addr. entry		
	<u>به</u> ۲	•	
		Logic addr. list	
	Outdoor station 001-01		LIST VIEW
æ	Outdoor station 001-01		lie addr. list
- <del></del>	INFORMATION		ic addr. list Add logic addr. entry
	INFORMATION Please select device		er addr. list Add logic addr. entry Import logic addr. list entries
- <del>-</del>	INFORMATION Please select device		er ador inst Add logic addr. entry Import logic addr. list entries pc addr entries
E	INFORMATION Please select device I All I Building1 I Floor 1 Master,Jacky		er addr. list Add logic addr. entry Import logic addr. list entries
E	INFORMATION Please select device I All I Building1 I Floor 1		er ador inst Add logic addr. entry Import logic addr. list entries pc addr entries
E	INFORMATION Please select device I All I Building1 I Floor 1 Master,Jacky		er ador inst Add logic addr. entry Import logic addr. list entries pc addr entries
E	INFORMATION Please select device I All I Building1 I Floor 1 Master,Jacky		er ador inst Add logic addr. entry Import logic addr. list entries pc addr entries
	INFORMATION Please select device I All I Building1 I Floor 1 Master,Jacky		er ador inst Add logic addr. entry Import logic addr. list entries pc addr entries
æ	INFORMATION Please select device I All I Building1 I Floor 1 Master,Jacky		er ador inst Add logic addr. entry Import logic addr. list entries pc addr entries
æ	INFORMATION Please select device I All I Building1 I Floor 1 Master,Jacky		er ador inst Add logic addr. entry Import logic addr. list entries pc addr entries
Ξ	INFORMATION Please select device I All I Building1 I Floor 1 Master,Jacky		er ador inst Add logic addr. entry Import logic addr. list entries pc addr entries
Œ	INFORMATION Please select device I All I Building1 I Floor 1 Master,Jacky		er ador inst Add logic addr. entry Import logic addr. list entries pc addr entries
α. 	INFORMATION Please select device I All I Building1 I Floor 1 Master,Jacky		er ador inst Add logic addr. entry Import logic addr. list entries pc addr entries
Œ	INFORMATION Please select device I I All I E building1 I Floor 1 I Master,Jacky I Master,Faye	2 mmt	er ador inst Add logic addr, entry Import logic addr, list entries pc addr entries
Œ	INFORMATION Please select device I All I Building1 I Floor 1 Master,Jacky	3 mport	er ador inst Add logic addr. entry Import logic addr. list entries pc addr entries
Œ	INFORMATION Please select device I I All I I Eliforn 1 I Master, Jacky 2 I Master, Fayo Cancel Cancel		er ador inst Add logic addr. entry Import logic addr. list entries pc addr entries
α 	Please select device  Please select device	3 mport	er ador inst Add logic addr, entry Import logic addr, list entries pc addr entries

- [4] The logic addresses are imported to the list.
- [5] Enter the key word to filter the search results.



3. Copying the logic address list to another outdoor station

- [1] On the "Logic addr. list" screen, click "Copy logic addr. list to other OS".
- [2] Click to select the designated outdoor stations.
- [3] Click "Import", followed by "  $\checkmark$  ".



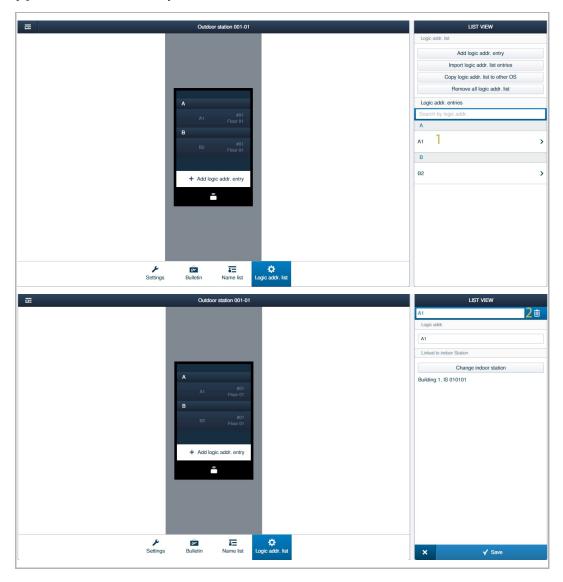
- LIST VIEW Outdoor stati on 001-03 2 Add logic addr. entry Import logic addr. list ent Copy logic addr. list to other OS Remove all logic addr. list Logic addr. entries A1 > в B2 > Cogic addr. list > Settings Bulletin
- [4] The logic address list is copied to the other outdoor station.

4. Removing the logic address

Please follow the steps below:

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

[2] Click "  $\fbox{1}$  ", followed by "  $\checkmark$  " to confirm.





Note

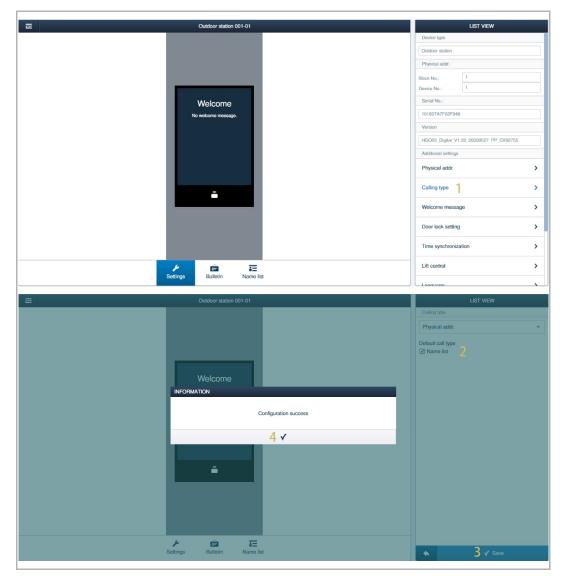
You can also click "Remove all logic addr. list" to clear all logic addresses.

#### 9.8.11 Initiating a call via the name list

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

1. Importing the name list

- [1] On the designated outdoor station screen, click "Call type".
- [2] Enable the "Name list".
- [3] Click " $\sqrt{}$ " to save.
- [4] Click " $\sqrt{}$ " to confirm.



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



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

[6] Click "Import name list entries".

Note

- [7] Click to select the designated indoor stations.
- [8] Click "Import", followed by "  $\checkmark$  " to confirm.
- [9] The names are imported to the list.

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

æ	Outdoor station 001-01		LIST VIEW
	Import name list		me list
			Import name list entries
	Please select device		me list entries
	C All C Building1 C Floor 1 C Master,Jacky C Master,Faye 7		lexistent names.
	Cancel	8 Import	
	Settings Bulletin Name list	5	
æ	Outdoor station 001-01		LIST VIEW
	M Master,Faye 601 Floor 01 Master,Jacky 601 Floor 01		Name list Import name list entries Copy name list o other OS Remove all entries J M M Master,Jacky
	+ Add item		
	ب ش		

[11]Click the designated name.

[12]Click "Upload logo image".

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

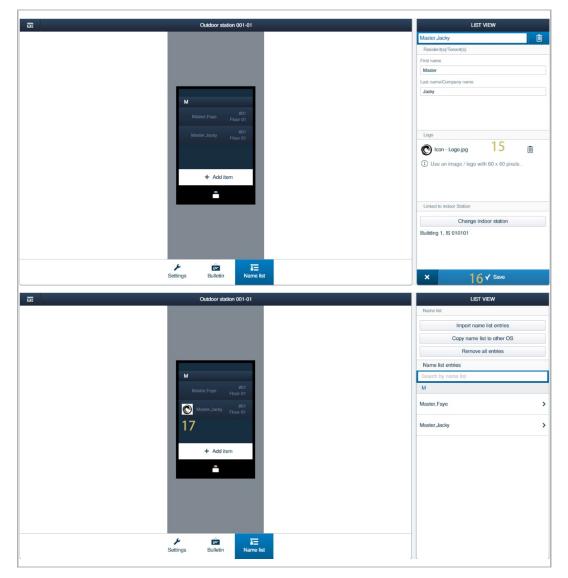
[14]Click "  $\checkmark$  " to confirm.

Guiddoor station 001-01	LIST VIEW
	Name list
	Import name list entries
	Copy name list to other OS
	Remove all entries
	Name list entries
м	Search by name list
Master Faye #01	м
	Master,Faye
Master_Jacky Floor 01	master, raye
	Master,Jacky 11 >
+ Add item	
ت 🖄 ۲	
Settings Bulletin Name list	
·	
GE Outdoor station 001-01	LIST VIEW
Cuidoor station 001-01	LIST VIEW
Cutdoor station 001-01	
Cutdoor station 001-01	Master,Jacky
टः Outdoor station 001-01	Master,Jacky 👘
Outdoor station 001-01	Master,Jacky   Readen(I)/Tenant(a)  First name  Master Last name/Company name
टः Outdoor station 001-01	Master,Jacky   Residen((s)/Tenant(s)  Final nume  Master
C Outdoor station 001-01	Master,Jacky   Readen(I)/Tenant(a)  First name  Master Last name/Company name
INFORMATION	Master,Jacky   Readen(I)/Tenant(a)  First name  Master Last name/Company name
INFORMATION Upload logo/image	Mastor,Jacky   Resident(s)/Tenant(s)  Find name  Master  Last name/Company name  Jacky
INFORMATION Upload logo/image	Mastor,Jacky   Resident(s)/Tenant(s)  Find nume  Master  Last nameCompany nume  Jacky  Logo
INFORMATION	Mastor,Jacky   Resident(s)/Tenant(s)  Find name  Master  Last nameCompany name  Jacky  Logo  Upload logo/image 12
INFORMATION Upload logo/image C:takepathDragon.jpg Browser 13	Mastor,Jacky   Resident(s)/Tenant(s)  Find nume  Master  Last nameCompany nume  Jacky  Logo
INFORMATION Upload logo/image	Mastor,Jacky   Resident(s)/Tenant(s)  Find name  Master  Last nameCompany name  Jacky  Logo  Upload logo/image 12
INFORMATION Upload logo/image C:\takepath\Dragon.jpg Browser 13 × 14 ✓	Mastor,Jacky   Resident(s)/Tenant(s)  Find name  Master  Last nameCompany name  Jacky  Logo  Upload logo/image 12
INFORMATION Upload logo/image C:takepathDragon.jpg Browser 13	Mastor,Jacky   Resident(s)/Terunt(s)  Find name Master Last name/Company name Last name/Company name Last name/Company name Last name/Logo Image 12  () Use an image / Logo with 60 x 60 pixels .
INFORMATION Upload logo/image C:\takepath\Dragon.jpg Browser 13 × 14 ✓	Mastor,Jacky   Resident(s)/Tenant(s)  Find name  Master  Last nameCompany name  Jacky  Logo  Upload logo/image 12
INFORMATION Upload logo/image C:\takepath\Dragon.jpg Browser 13 × 14 ✓	Mastor,Jacky   Resident(s)/Tervant(s)  First name Master Last name/Company name Last name/Company name Last name/Company name Last name/Logo Image Logo Logo Logo Logo Logo 12  Count of the second se
INFORMATION Upload logo/image C:\takepath\Dragon.jpg Browser 13 × 14 ✓	Mastor,Jacky   Resident(sy)Terxin(s)  First name  Master Last name/Company name Jacky  Logo  Upload logo/image 12  Upload logo/image Live an image / logo with 60 x 60 pixels .  Lived to indoor Station
INFORMATION Upload logo/image C:\takepath\Dragon.jpg Browser 13 × 14 ✓	Mastor,Jacky   Resident(s)/Tervant(s)  First name Master Last name/Company name Last name/Company name Last name/Company name Last name/Logo Image Logo Logo Logo Logo Logo Integration Last 60 indoor Station Change indoor station
INFORMATION Upload logo/image C:\takepath\Dragon.jpg Browser 13 × 14 ✓	Mastor,Jacky   Resident(s)/Tervant(s)  First name Master Last name/Company name Last name/Company name Last name/Company name Last name/Logo Image Logo Logo Logo Logo Logo Integration Last 60 indoor Station Change indoor station
INFORMATION Upload logo/image C:\takepath\Dragon.jpg Browser 13 × 14 ✓	Mastor,Jacky   Resident(s)/Tervant(s)  First name Master Last name/Company name Last name/Company name Last name/Company name Last name/Logo Image Logo Logo Logo Logo Logo Integration Last 60 indoor Station Change indoor station

[15]The logo is displayed in the list.

[16]Click "  $\checkmark$  " to save.

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



2. Copying the name list to other outdoor station

- [1] On the "Name list" screen, click "Copy name list to other OS".
- [2] Click to select the designated outdoor stations (only supports the IP touch 5 outdoor station).
- [3] Click "Import", followed by "  $\checkmark$  ".

ā	Outdoor station 001-01	LIST VIEW
	M Matter Jruye Food Matter Jacoby Food 01 + Add Item C Settings Eullelin EE Mame fat	Name list Import name list entries Copy name list to other OS Remove all entries Name list entries Search by name list M Master,Faye Master,Jacky
E	Cutdoor station 001-01  IFORMATION  Please select device  □	LIST VIEW  Inter list  Import name list entries  Copy name list office OS  Remove all entries  me list entries  rech by name list  ter, Faye  ter, Jacky
	Cancel 3 Import	

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

Outdoor station 001-04	LIST VIEW
Outdoor station 001-04	LIST VIEW       Name list       Import name list entries       Copy name list to other OS       Remove all entries       Beauch by name list       M       Master,Faye       4
איז פער	

3. Removing the logic address

Please follow the steps below:

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

[2] Click "  $\fbox{1}$  ", followed by "  $\checkmark$  " to confirm.

Outdoor station 001-01	LIST VIEW
	Name list
	Import name list entries
	Copy name list to other OS
	Remove all entries
м	Name list entries
	Search by name list
Master,Faye #01 Floor 01	1
Master,Jacky #01	Master,Faye 1
Master,Jacovy Floor 01	Master,Jacky
+ Add item	
ب <u>ش</u> ا	
Settings Bulletin Name list	
Outdoor station 001-01	LIST VIEW
Get Outdoor station 001 01	LIST VIEW
Cutdoor station 001-01	Master,Faye 2
Generation 001-01	
GE Outdoor station 001-01	Master,Faye 2 1
Get Outdoor station 001-01	Master,Faye 2
	Mastor,Faye 2 1
M	Mastor,Føye 2 Resident(s)/Tenant(s) First name Mader Last nameCompany name
	Mastor,Føye 2 Resident(s)/Tenant(s) First name Mader Last nameCompany name
M Muster Faye 101 Floor 01	Mastor,Faye 2 11
M Mader Floye 801 Poor 01	Mastor,Faye 2 10 Resident(s)/Tenant(s) First name Master Last nameCompany name Figre
M Muster Faye 101 Floor 01	Master,Faye  Pesident(s)/Tenant(s) First name Master Last nameCompany name Faye Logo Logo Upload togo/image
M Muster/Figre 1001 Floor 01 Muster/Jacky Floor 01	Mastor,Faye 2 10 Resident(s)/Tenant(s) First name Master Last nameCompany name Figre
M Muster Faye 101 Floor 01	Master,Faye  Pesident(s)/Tenant(s) First name Master Last nameCompany name Faye Logo Logo Upload togo/image
M Mader-Foye #01 Mader-Jacky #01 Hader-Jacky Foor 01 + Add item	Master,Faye  Pesident(s)/Tenant(s) First name Master Last nameCompany name Faye Logo Logo Upload togo/image
M Muster/Filipe 1001 Floor 01 Muster/Jacky Floor 01	Mastor,Faye
M Mader-Foye #01 Mader-Jacky #01 Hader-Jacky Foor 01 + Add item	Master, Faye Pesident(s)/Tenant(s) First name Mader Last name/Company name Faye Logo Logo Upload logo/image ① Use an image / logo with 60 x 60 pixels . Linked to indoor Station
M Mader-Foye #01 Mader-Jacky #01 Hader-Jacky Foor 01 + Add item	Master, Faye  Pesident(s)/Tenant(s) First name Master InstrumeCompany name Faye Logo Logo Upload logo/image ① Use an image / logo with 60 x 60 pixels . Linked to indoor Station Change indoor station
M Mader-Foye #01 Mader-Jacky #01 Hader-Jacky Foor 01 + Add item	Master, Faye Pesident(s)/Tenant(s) First name Master Last name/Company name Faye Logp Logp Upload logo/image ① Use an image / logo with 60 x 60 pixels . Linked to indoor Station
M Master Frye 101 Master Jacky 100 01 + Add Item	Master, Faye  Pesident(s)/Tenant(s) First name Master InstrumeCompany name Faye Logo Logo Upload logo/image ① Use an image / logo with 60 x 60 pixels . Linked to indoor Station Change indoor station
M Muster Frage Fool of Muster Jucky Fool of + Add item	Master, Faye  Pesident(s)/Tenant(s) First name Master InstrumeCompany name Faye Logo Logo Upload logo/image ① Use an image / logo with 60 x 60 pixels . Linked to indoor Station Change indoor station
M Master Frye 101 Master Jacky 100 01 + Add Item	Master, Faye  Pesident(s)/Tenant(s) First name Master InstrumeCompany name Faye Logo Logo Upload logo/image ① Use an image / logo with 60 x 60 pixels . Linked to indoor Station Change indoor station



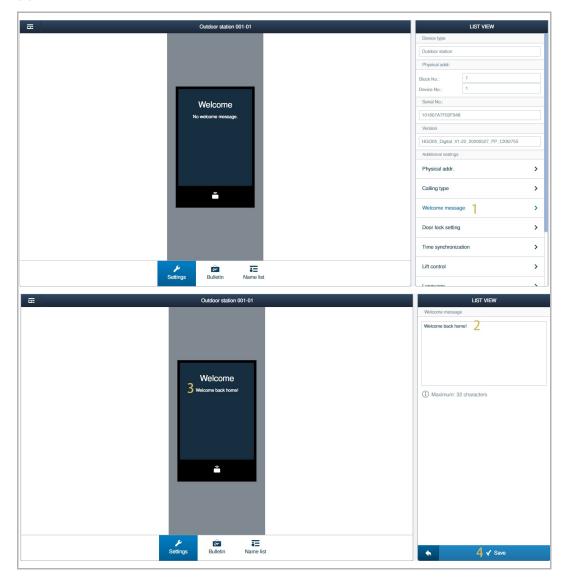
Note

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

#### 9.8.12 Managing the welcome message

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

- [1] On the designated outdoor station screen, click "Welcome message".
- [2] Enter the message (not more than 32 characters).
- [3] The result is displayed on the outdoor station screen.
- [4] Click "  $\checkmark$  " to save.



#### 9.8.13 Managing the developer information

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

- [1] On the designated outdoor station screen, click "Bulletin".
- [2] Click "Developer information".
- [3] Selet "Image" from the drop-down list.
- [4] Click "Upload image/logo" to select the image (e.g company logo).

GE Outdoor station 001-01	LIST VIEW
	Bulletin
	Developer information 2
	Bulletin >
Welcome Welcome	
Sotings 1 Bulletin Name list	
	LIST VIEW
	LST VIEW
	Developer information Image 3  ImageLogo
	Developer information           Image         3         ~           ImageLogo         Upload imageTogo         4
	Developer information Image 3

#### 9.8.14 Managing the bulletin

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

- [1] On the designated outdoor station screen, click "Bulletin".
- [2] Click "Bulletin".
- [3] Click "Add bulletin page" to select the image.

Outdoor station 001-01	LIST VIEW
	Bulletin
	Developer information >
	Bulletin 2
Welcome Welcome CO C C C C C C C C C C C C C C C C C C	a.
Cutdoor station 001-01	LIST VIEW Bulletin pages
Welcome Sunset Boulevard 1302	Add bulletin page 3
+ Add bulletin page	

#### 9.8.15 Managing the unlock QR code

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

- [1] On the designated outdoor station screen, click "Unlock mode setting".
- [2] Tick the check box "QR code unlocking" to enable the function.
- [3] Click "  $\checkmark$  " to save.

Gate station #32	LIST VIEW	
	Additional settings	
	Physical addr.	>
Welcome	Calling type	>
No welcome message.	Welcome message	>
	Door lock setting	>
	Time synchronization	>
	Language	>
≜ in the second s	Local firmware update	>
	Online firmware update	>
	List of trusted devices	>
br Settings Bulletin Name list	Unlock mode setting	>
Gate station #32	LIST VIEW	
Gate station #32	LIST VIEW	
Gate station #32		
Welcome No welcome message.	Unlock mode setting	



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

### 9.8.16 Updating the firmware

see chapter 13.4 "Updating the firmware" on page 309.

#### 9.9 Configuring the guard unit

#### Access the designated guard unit screen

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

❤ 📵 🗟 sc	as 🕦 🔋		MAIN MENU			
BUILDING STRUCTURE	RF WIRELESS CONNECTION	PLACE + LINK	USER MANAGEMENT	ACTIONS		DOOR ENTRY SYSTEM
Design a building by creating floors and rooms	Configurate the devices of the access control system e.g. cylinders, repeaters	Locating and linking devices	Add and edit users. Create user groups	Create and edit actions	Create time control	Configurate door entry system devices, e.g. indoor station, outdoor station
🛔 abb					Device configura	tion 🌣 Preferences

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

•						
				Ø	Guard unit	
Guard unit #01					Guard unit #01	>
	Outdoor stations Indoor stations	o IP actuator	1			

#### 9.9.1 Setting the device number

- [1] On the designated guard unit screen, enter a new device number.
- [2] Click "  $\checkmark$  " to save.
- [3] Click "  $\checkmark$  " to confirm.

Guard unit #01	LIST VIEW
	Device No.
	2
	Sorial No.:
INFORMATION	HGM53 Main V1.30 20190515 PP IMX6
	Additional settings
Configuration success	Local firmware update
3 🗸	Online firmware update
CONDA	
<b>پ</b> Settings	× 2 ✓ Save

#### 9.9.2 Viewing the serial number

Please follow the steps below:

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



### 9.9.3 Updating the firmware

see chapter 13.4 "Updating the firmware" on page 309.

#### 9.10 Configuring the IP actuator

#### Accessing the designated IP actuator screen

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

❤ 📵 🗟 sc	as 🕦 🔋		MAIN MENU			
BUILDING STRUCTURE	RF WIRELESS CONNECTION	PLACE + LINK	USER MANAGEMENT	ACTIONS		DOOR ENTRY SYSTEM
Design a building by creating floors and rooms	Configurate the devices of the access control system e.g. cylinders, repeaters	Locating and linking devices	Add and edit users. Create user groups	Create and edit actions	Create time control	Configurate door entry system devices, e.g. indoor station, outdoor station
🛔 abb					Device configura	tion 🌣 Preferences

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

O	IP ACTUATOR	ADD DEVICE	LIST VIEW
		Ø IP actu	ator
Pactuator		Block IP	A 001-01
Block IPA 001-01			
Public area		Public	area
	Cuidoor stations Indoor stations IP actuator		

#### 9.10.1 Viewing the serial number

Please follow the steps below:

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

æ	Block IPA 001-01	LIST VIEW		
		Device type		
	LAN	Building IPA ~		
		Physical addr.		
	GND DC+ LOCK+ LOCK- GND DS EXIT	Block No.: 1		
		Device No.: 1		
		Serial No.:		
	H8304	104807A7F02F5EF		
	IP Actuator ABB-Weicome IP	Version		
		HGM51_V1.03_20190301_PP_STM32F407VE		
		Additional settings		
	Status Reset Security Switch	Unlock setting		
	ERI 💩 🗏 CE	Local firmware update		
		Online firmware update		
		List of trusted devices >		
	Settings	× √ Save		

#### 9.10.2 Managing the physical address

There are 3 types devices for selection.

1. Network IPA

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

E Block IPA 001-01	LIST VIEW	
	Device type	
LAN	Network IPA	~
8 6 9 6 8 6	Physical addr.	
AND DC+ LOCK+ LOCK- GND DS EXIT	Device No.: 1	
	Serial No.:	
	104807A7F02F5EF	
H8304 IP Actuator	Version	
ABB-Welcome IP	HGM51_V1.03_20190301_PP_STM32F407VE	
	Additional settings	
Status Reset	Unlock setting	>
Security Switch	Local firmware update	>
EHE 💩 👱 CE	Online firmware update	>
NG COM NO (5) (5) (5)	List of trusted devices	>
and the second se		
Settings	× √ Save	

#### 2. Building IPA

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

Block IPA 001-01	LIST VIEW	
	Device type           Building IPA           Physical addr.           Block No.:         1           Device No.:         1	~
H8304 IP Actuator ABB-Vielcome IP Status Reset Security Switch	Seriel No.: 104807A/F02PSEF Version HGM51 V1 03 20190301 PP_STM32F407VE Additional settings Unlock setting	>
EHI ▲ ▲ C €	Local firmware update Online firmware update List of trusted devices	> >
Settings	X V Save	

#### 3. Private IPA

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

E Block IPA 001-01		LIST VIEW
a succession	Device type	
	Private IPA Physical addr.	v
UND DO - LOOK- LOOK- OND DS EXT	Block No.: Floor No.:	1
	Room No.:	1
H8304 IP Actuator	Device No.: Serial No.:	1
ABB-Welcome IP	104807A7F02F5EF Version	
Status Reset		90301_PP_STM32F407VE
ERE 💩 🖄 CE	Additional settings Unlock setting	>
NG COM NO	Local firmware up	odate >
© © ©	Online firmware u	pdate >
×	List of trusted dev	vices >
Settings	×	✓ Save

#### 9.10.3 Unlock setting

- [1] On the designated IP actuator screen, click "Unlock setting".
- [2] Set the output mode for "Lock-GND" among "AC output", "DC output (NC)" and ", "DC output (NO)".
- [3] Set the unlock time for "Lock-GND".
- [4] Set the output mode for "Relay lock" between "Unlock" and "Light".
- [5] Set the unlock time for "Relay lock".
- [6] Click " $\sqrt{}$ " to save.

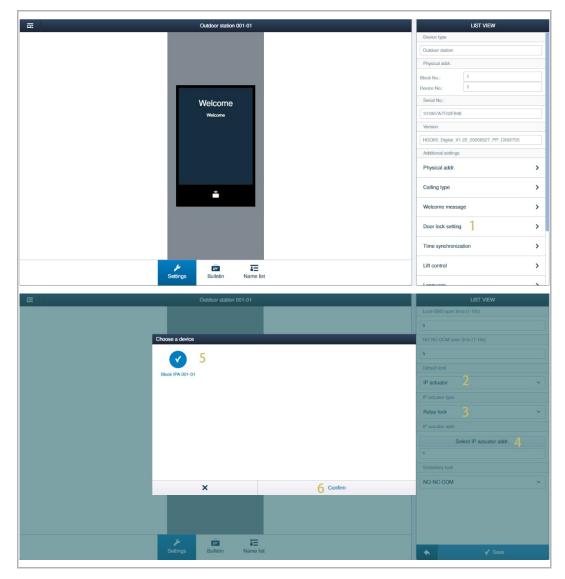
Block IPA 001-01	LIST VIEW
	Device type
LIN	Building IPA v
	Physical addr.
AND DC+ LOCK+ LOCK- AND DS EXIT	Block No.: 1
	Device No.: 1
	Serial No.:
H8304	104807A7F02F5EF
IP Actuator ABB-Welcome IP	Version
	HGM51_V1.03_20190301_PP_STM32F407VE
• •	Additional settings
Status Reset Security Switch	Unlock setting 1
	Local firmware update
	Online firmware update
	List of trusted devices >
Settings	× √ Save
豆 Block IPA 001-01	LIST VIEW
	Lock-GND
the second second	Output mode 2
	Output mode 2
8 6 8 8 8 8	Output mode 2
	Cutput mode 2 AC output Unlock lime - 5 + 3 Reity lock
	Output mode 2 AC output v Unicot time 5 + 3 Relay tock Relay mode
	Cutput mode 2 AC output Unlock lime - 5 + 3 Relay mode Light Time of light - 5
HB304 IP Actuator	Cutput mode 2 AC output v Unicot time - 5 + 3 Relay rock Relay mode Lights 4 v
	Cutput mode 2 AC output Unlock lime - 5 + 3 Reity lock Reity mode Lights 4 ~ Time of light - 5
H8304 IP Actuator	Cutput mode 2 AC output Unlock lime - 5 + 3 Reity lock Reity mode Lights 4 ~ Time of light - 5
H8304 IP Actuator	Cutput mode 2 AC output Unlock lime - 5 + 3 Reity lock Reity mode Lights 4 ~ Time of light - 5
H304 IP Actuator ABB-Welcome IP Status Reset Stervity Switch	Cutput mode 2 AC output Unlock lime - 5 + 3 Reity lock Reity mode Lights 4 ~ Time of light - 5
H304 IP Actuator ABB-Welcome IP Status Reset Stervity Switch	Cutput mode 2 AC output Unlock lime - 5 + 3 Reity lock Reity mode Lights 4 ~ Time of light - 5
HB304 IP Actuator ABB-Weicome IP Status Reset	Cutput mode 2 AC output Unlock lime - 5 + 3 Reity lock Reity mode Lights 4 ~ Time of light - 5
HB304 IP Actuator ABB-Weicome IP Status Status Reset Becurity Switch EFIL QOM NO	Cutput mode 2 AC output Unlock lime - 5 + 3 Reity lock Reity mode Lights 4 ~ Time of light - 5
HB304 IP Actuator ABB-Welcome IP Status Reset Encurity Switch Eff.	Cutput mode 2 AC output Unlock lime - 5 + 3 Reity lock Reity mode Lights 4 ~ Time of light - 5
HB304 IP Actuator ABB-Weicome IP Status Status Reset Becurity Switch EFIL QOM NO	Cutput mode 2 AC output Unlock lime - 5 + 3 Reity lock Reity mode Lights 4 ~ Time of light - 5

#### 9.10.4 Managing the trusted devices

see chapter 9.3.2 "Managing the trusted devices for IP actuator" on page 87.

#### 9.10.5 Releasing the IP actuator related to the outdoor station

- [1] On the designated outdoor station screen, click "Door lock setting".
- [2] Set door type to "IP actuator".
- [3] Select IP actuator type between "Power lock" and "Relay lock".
- [4] Click "Select IP actuator addr.".
- [5] Click to select the designated IP actuator.
- [6] Click "Confirm".



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

[8] Click "Add trusted devices".

[9] Click the designated outdoor station.

[10]Click "  $\checkmark$  " to save.

	Block IPA 001-01	LIST VIEW	
		Device type	
1	the of the second se	Building IPA	~
		Physical addr.	
		Block No.: 1	
		Device No.: 1	
		Serial No.:	
	H8304	104807A7F02F5EF	
	IP Actuator	Version	
	ABB-Welcome IP	HGM51_V1.03_20190301_PP_STM32F407VE	
	• •	Additional settings	
	Status Reset	Unlock setting	>
	Security Switch		,
	ERI 💩 🗏 CE	Local firmware update	>
1		Online firmware update	>
	NC COM NO	List of trusted devices 7	>
	يو Settings	× ✓ Save	
=	Block IPA 001-01	LIST VIEW	
æ	Block IPA 001-01 Add Inusted devices	of trusted devices	-
	Add trusted devices		
	Add trusted devices Please select device	of trusted devices	
- <del>-</del>	Add trusted devices Please select device D All D Lublic	of trusted devices	
- <del>-</del>	Add trusted devices Please select device All Pluic Building 1 Public Public	of trusted devices	
	Add trusted devices  Please select device  All  Public  Building1  Cuddor station 001-01	of trusted devices	
	Add trusted device Please select device All Public Building1 Culdoor station 001-01 Outdoor station 001-02 Outdoor station 001-03	of trusted devices	
æ	Add trusted devices  Please select device  All  Public  Public  Public  Outdoor station 001-01  Outdoor station 001-02	of trusted devices	
æ	Add trusted devices   Please select device  I All  Public  Dublic  Undoor station 001-01  Outdoor station 001-03  Outdoor station 001-04  Dublic  Master_Jacky	of trusted devices	
æ	Add trusted devices   Please select device  All  Public  Duidoor station 001-01  Outdoor station 001-02  Outdoor station 001-03  Outdoor station 001-04  Floor 1  Poor 1	of trusted devices	
Œ	Add trusted devices   Please select device  All  Public  Building1  Outdoor station 001-01  Outdoor station 001-02  Outdoor station 001-03  Outdoor station 001-04  Floor 1  Master_Jacky Stave Jacky	of trusted devices	
Œ	Add trusted devices   Please select device  All  Public  Building1  Outdoor station 001-01  Outdoor station 001-02  Outdoor station 001-03  Outdoor station 001-04  Floor 1  Master_Jacky Stave Jacky	of trusted devices	
Œ	Add trusted devices   Please select device  All  Public  Building1  Outdoor station 001-01  Outdoor station 001-02  Outdoor station 001-03  Outdoor station 001-04  Floor 1  Master_Jacky Stave Jacky	of trusted device rusted device 8 Add trusted devices	
Œ	Add trusted devices   Please select device  All  Public  Building1  Outdoor station 001-01  Outdoor station 001-02  Outdoor station 001-03  Outdoor station 001-04  Floor 1  Master_Jacky Stave Jacky	of trusted device rusted device 8 Add trusted devices	
E	Add trusted devices	of trusted device rusted device 8 Add trusted devices	
E	Add trusted devices   Please select device  All  Public  Building1  Outdoor station 001-01  Outdoor station 001-02  Outdoor station 001-03  Outdoor station 001-04  Floor 1  Master_Jacky Stave Jacky	of trusted device rusted device 8 Add trusted devices	
Ξ	Add trusted devices	of trusted device rusted device 8 Add trusted devices	
	Add trusted devices	of trusted device rusted device 8 Add trusted devices	

[11]Click "  $\checkmark$  " to save. [12]Click "  $\checkmark$  " to confirm.



#### 9.11 Removing the devices

#### 9.11.1 Removing the devices one by one

- [1] On the "Device configuration" screen, click a device (e.g. "Indoor station").
- [2] Click the designated device (e.g. "Indoor station 2").
- [3] Click " 🔟 ".
- [4] Click "  $\checkmark$  " to confirm.

			LIS	ST VIEW
Device type		Indoor station(2)		IS 001-0101-02
SmartAP(1)	>	#102807A7F02F605(XEH) IS 001-0101-01	>	Serialnumber: 102807A7F030593 Short ID: WAW
Ê Cylinder(0)	>	#102807A7F030593(WAW)		Software version: HGI17-CS_Main_V2.01_20200116_PP_IN Update firmware
Repeater(0)	>	IS 001-0101-02	2 >	Parameter
RF/IP gateway(0)	>			Block No.
IP camera(0)	>			
Outdoor station(2)	>			Floor No.
Indoor station(2)	>			Room No.
O- IP actuator(1)	>			
Guard unit(1)	>			Device No.
				Channels
		+		<b>*</b>
			LIS	ST VIEW
Device type SmartAP(1)	>	Indoor station(2) #102807A7F02F605(XEH)		
B Cylinder(0)	>	IS 001-0101-01	>	
Repeater(0)	>	#102807A7F030593(WAW)	>	
RF/IP gateway(0)	>			
🖕 IP camera(0)	>	INFORMATION		
Outdoor station(2)	>		0	
Indoor station(2)	>		(?) An	e you sure to delete?
O- IP actuator(1)	>			4.4
Guard unit(1)	>	×		4 ✓
		+		

#### 9.11.2 Removing the devices in batch

- [1] On the "Device configuration" screen, click a Door Entry System device (e.g. "Outdoor station").
- [2] Click " 🗹 ".
- [3] Click "Select all" to select all devices or click the designated device one by one to select multiple devices.
- [4] Click "Delete".

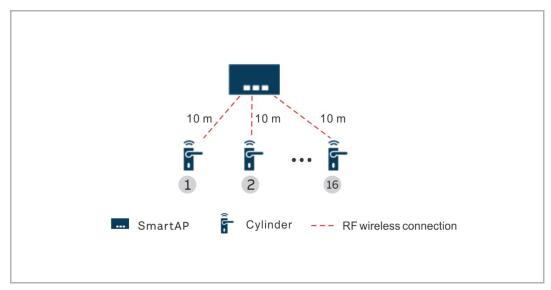
0		OUTDOOR STATIONS ADD D	EVICE		LIST VIEW	
			2 🖉	Outdoor stations		
Outdoor stations			-	Outdoor station 001-	01	>
B				Outdoor station 001-	02	>
Outdoor station 001-01	Outdoor station 001-02					
Public area				Public area		
		Cutdoor stations IP actuator Cuard unit				
=		OUTDOOR STATIONS			LIST VIEW	
		1000 CONSCIENT 2010 CONSCIENCE (CONSCIENCE)	Select all	Outdoor stations		
				Building1		
B	B			Outdoor station 001	-01	
Outdoor station 001-01	Outdoor station 001-02			Outdoor station 001	-02	
				Public area		
Public area						
						4
				×	Next	4 Delete
					- Host	Boloto

## 10 Operating the AccessControl devices

#### 10.1 AccessControl topology

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

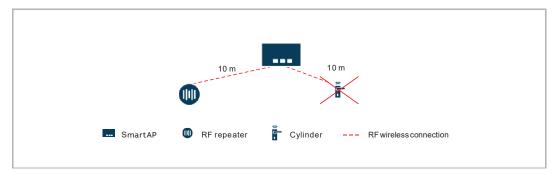
- 1. Preconditions
- The number of "Electronic locking cylinders" operated by "Smart Access Point" is  $\leqslant$  16 units.
- The distance from the furthest "Electronic locking cylinder" to "Smart Access Point" is  $\leqslant$  10 metres.
- 2. Capacity
- The radio range between each RF device is  $\leq$  10 metres.
- Up to 16 "Electronic locking cylinders" can be operated via a "Smart Access Point".



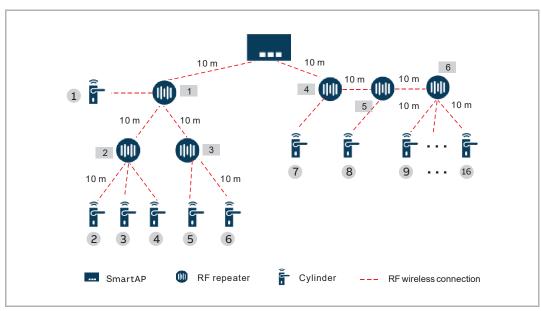
#### 3. Topology

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

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



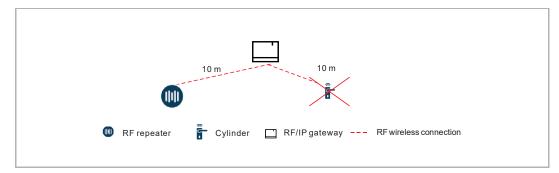
- 2. Capacity
- The radio range between each RF device is  $\leq$  10 metres.
- Up to 16 "Electronic locking cylinders" can be operated via one "Smart Access Point".
- Up to 6 "RF Repeaters" can be operated via one "Smart Access Point".
- Up to 3 "RF Repeaters" can be connected to one "Smart Access Point"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



#### 3. Topology

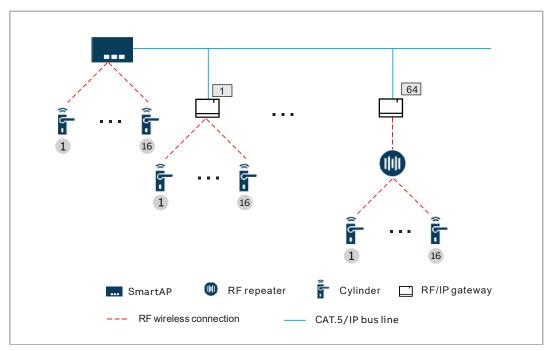
# Scenario 3: A large number of "Electronic locking cylinders" used and long distance between devices

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



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

#### 3. Topology

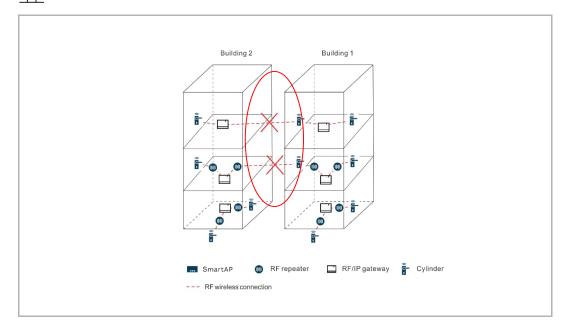




 $\cap$ 

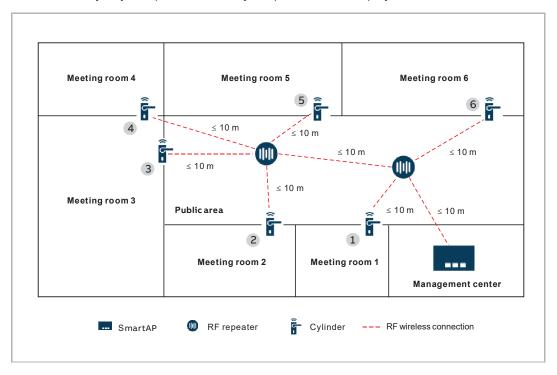
#### Note

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



#### Demo case

This demo case is used to familiarize yourself with the operations of AccessControl devices. You need to adjust your operations when you operate an actual project.



#### 10.2 Creating a building

### 10.2.1 Creating a building via "Smart Access Point"

The following operations are all based on the demo case. Please follow the steps below:

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

✓ 0 B SC	os 🕅 🖡		MAIN MENU			
	<b>O-O</b> Pr'WHILESS CONJECTION	PLACE + LINK	USER MANAGEMENT	КПОНЯ	Типерантной	DOOR ENTRY SYSTEM
Design a building by creating floors and rooms	Configurate the devices of the access control system e.g. cylinders, repeaters	Locating and linking devices	Add and edit users. Create user groups	Create and edit actions	Create time control	Configurate door entry system devices, e.g. indoor station, outdoor station
🛔 jacky					Device configura	tion 🔅 Preferences

[2] Click "Single building".

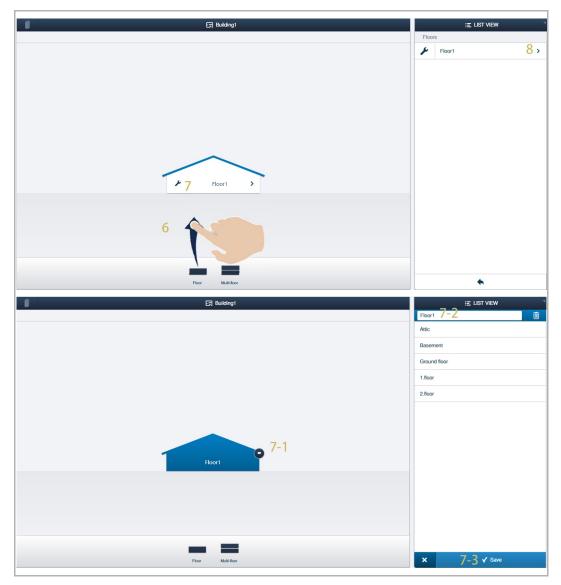
Select BULDING STRUCTURE TYPE         Please choose an option         Image: Comparison of the selection of th		
	Please choose an option           Image: Single building         Image: Single buildings	

[3] Click "Similar floors".

- [4] Drag the "Building" icon onto the floor plan.
- [5] Click ">" to continue.

SITE PLAN				:≣ LIST \	/IEW
	-	+	Buik	lings	
			4	Building1	5 >
J Building1					
4					
Building Building L					

- [6] Drag the "Floor" icon onto the floor plan.
- [7] Click " 🗲 " to edit the floor (optional).
  - 7-1, click the icon to change the floor shape.
  - 7-2, change the floor name.
  - 7-3, save the change.
- [8] Click ">" to continue.



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

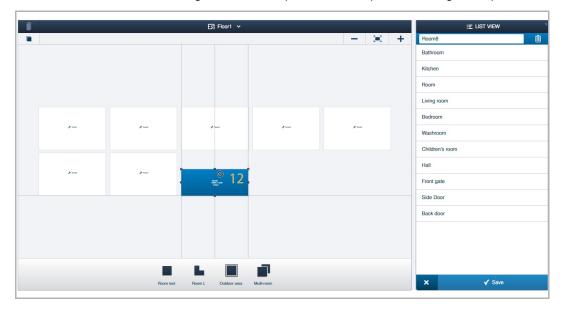
[10]Enter the room number (e.g. "8" for demo case 1).

[11]Click "Duplicate".

⊡ Floor1 ×	:E LIST VIEW
· · · · · · · · · · · · · · · · · · ·	Rooms
NEW ROOMS	
New rooms 10	
Duplicates _ 8 +	
× 11 Duplicate	
9	
Reom red Room L. Outdoor area Multi-room	•

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

- Click the icon " O O O O To change the height or the width of the room shape.
- Click the icon " <sup>•</sup> " to restore the room shape.
- Click the icon " <sup>•</sup> " to change the room shape from "Rectangle" shape to "L" shape.
- Click the icon " " to change the room shape from "L" shape to "Rectangle" shape.



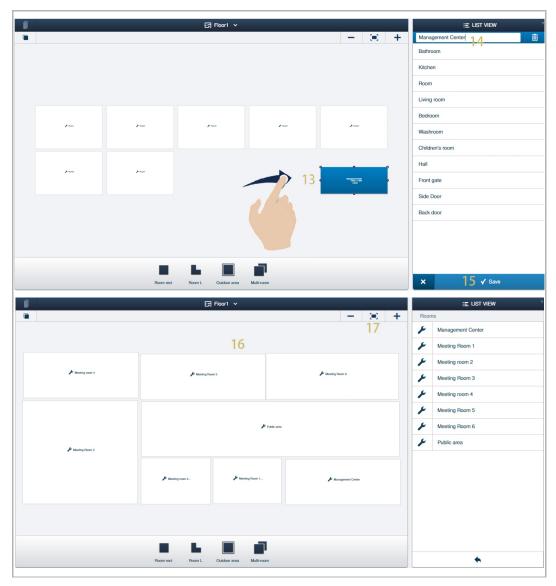
[13]Drag the designated room to move it.

[14]Edit the room name.

[15]Click "  $\checkmark$  " to save.

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

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

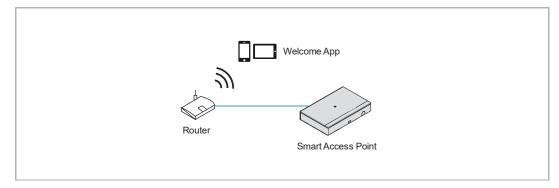


### 10.2.2 Creating a building via Welcome App

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

#### Precondition

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



#### Importing rule

Building structure will be overwritten according to the rules below:

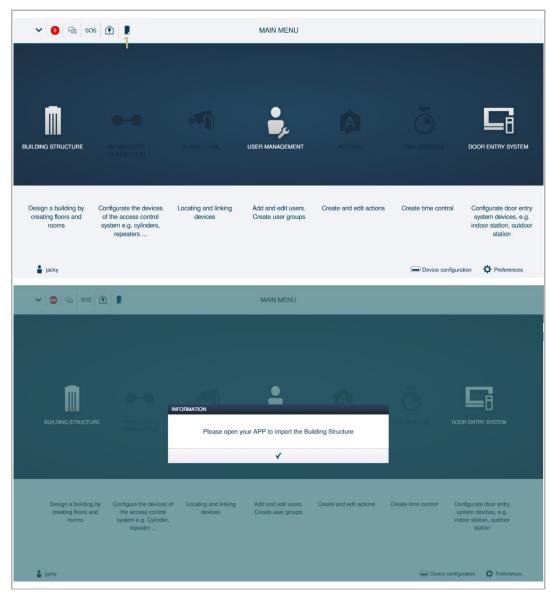
- A, B, C, D, E, F means building number.
- B and B+ has the same building number.
- + means the building structure has been changed.

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

## Importing the building from Welcome App

Please follow the steps below:

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



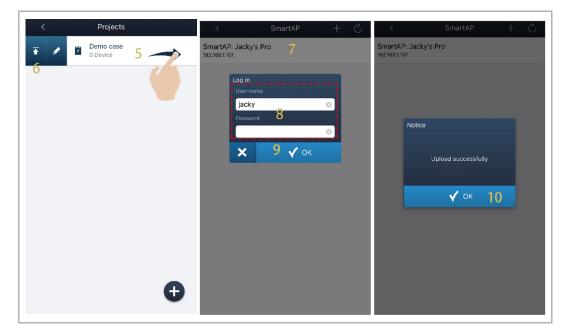
- [2] On the Welcome App "Home" screen, tap " $\vee$ ".
- [3] Tap "Configuration mode".
- [4] Tap "  $\checkmark$  " to continue.

✓ → Home	A Home		A Home
"jacky" iPhone, No events	Settings		Settings
Jucky in Hole, No events	Pair Devices	>	Pair Devices >
	Account name and license information		Account name and license information
	SOS	>	Notifications and Sounds
$\wedge$	Call Guard Unit	>	Configu Are you sure you want to switch to
"jacky" iPhone	Notifications and Sounds	>	Firmwai
jacky iPhone	Configuration mode 3	>	About 🗙 🗸 ок 4
	Firmware upgrade	>	Log out >
	About	>	
Events 🔨	Log out	>	
▲ <b>≕</b> ,			

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

- [6] Tap " 🚺 ".
- [7] Tap a designated "Smart Access Point".
- [8] Enter the account and password of "Smart Access Point".
- [9] Tap "  $\checkmark$  " to continue.

[10]Tap "  $\checkmark$  " to finish.



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

[12]Click "  $\checkmark$  " to finish.

🗸 🧶 🗟 sos 👔	E		MAIN MENU			
BUILDING STRUCTURE		IMPORT BUILDING STRI Project na				DOOR ENTRY SYSTEM
Design a building by creating floors and rooms	Configure the devices of the access control system e.g. Cylinder, repeater	Locating and linking devices	Add and edit users. Create user groups	Create and edit actions	Create time control	Configurate door entry system devices, e.g. indoor station, outdoor station
🛔 jacky					Device	configuration 🏠 Preferences

The building imported from Welcome App does not include the shape and location. You need to adjust it on "Smart Access Point". see chapter 10.2.1 "Creating a building via "Smart Access Point" on page 180.

		5 1.Floor ソ		_				∷≣ LIST VIEW
				-		+	Roor	ns
							۶	Management center
							×	Meeting room 1
							×	Meeting room 2
							×	Meeting room 3
							×	Meeting room 4
€ Manyout selfe	France	🖋 Madag saw 1	Je Maring and 2		Maling care 3		۶	Meeting room 5
							×	Meeting room 6
							×	Public area
Je Maning ann A	الم المعادية من المعادية المراجع المعادية المعادية المراجع المحادثة المراجع المحادثة المحادثة المحادثة المحادثة	Je Maning same K						
	Room rect	Room L Outdoor area	Multi-room					*

## 10.3 Adding and locating the devices

# Access the "Device configuration" screen

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

BUILDING STRUCTURE	RF WIRELESS CONNECTION	PLACE + LINK	USER MANAGEMENT	ACTION D	TIME CONTINUE	DOOR ENTRY SYSTEM
Design a building by creating floors and rooms	Configure the devices of the access control system e.g. Cylinder, repeater	Locating and linking devices	Add and edit users. Create user groups	Create and edit actions	Create time control	Configurate door entry system devices, e.g. indoor station, outdoor station
🛔 jacky						configuration

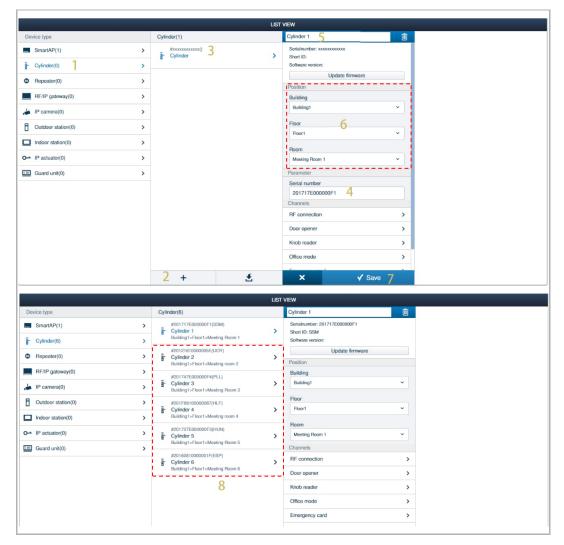
## 10.3.1 Locating "Smart Access Point"

- [1] On the "Device configuration" screen, click "SmartAP".
- [2] Click "Smart Access Point".
- [3] Set the position from the drop-down list (e.g. "Building 1>>Floor 1>> Public area" for demo case 1).
- [4] Click "  $\checkmark$  " to save.

	LIST	VIEW
Device type	SmartAP(1)	Smart Access Point
Device type           Im SmartAP(1)           Image: SmartAP(1)	SmartAP(1)  PI05907/37000734(PGA) 2	Smart Access Point Serialnumber: 105807A7F030734 Shot 10: RGA Software version: V5.21 MCU version: V1.08_2019129 RF MCU version: V1.07 RF module version: V1.05 Update firmware Profition Building Buildi
		Citaritwits Doorheit ring Alarm alert Binary input Binary output Tamper alarm
		× 4 ✓ Save

### 10.3.2 Adding and locating "Electronic locking cylinders"

- [1] On the "Device configuration" screen, click "Cylinder".
- [2] Click "+".
- [3] Click "Cylinder".
- [4] Enter the serial number of the "Electronic locking cylinder".
- [5] Change the name of the "Electronic locking cylinder".
- [6] Set the position from the drop-down list (e.g. "Building 1>>Floor 1>> Meeting room 1" for demo case 1).
- [7] Click "  $\checkmark$  " to save.
- [8] Repeat steps 2-7 to add the "Electronic locking cylinder" one by one. (e.g. "Cylinder 2~Cylinder 6" for demo case 1).



#### 10.3.3 Adding and locating "RF Repeaters"

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

- [1] On the "Device configuration" screen, click "Repeater".
- [2] Click "+".
- [3] Click "Repeater".
- [4] Enter the serial number of the "RF Repeater".
- [5] Change the name of the "RF Repeater".
- [6] Set the position from the drop-down list (e.g. "Building 1>>Floor 1>> Public area" for demo case 1).
- [7] Click "  $\checkmark$  " to save.
- [8] Repeat steps 2-7 to add the "RF Repeater". (e.g. "Repeater 2" for demo case 1).

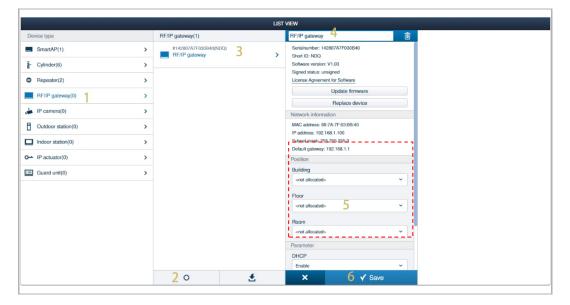
			LIS	T VIEW		
Device type		Repeater(1)		Repeater 1 5		面
SmartAP(1)	>		з ,	Serialnumber: x000000 Short ID:	200002	
- Cylinder(6)	>			Software version:	pdate firmware	
Repeater(0)	>			Position		
RF/IP gateway(0)	>			Building		
JP camera(0)	>			Building1		
Outdoor station(0)	>			Floor Floor1 6		
Indoor station(0)	>			1		—i
O- IP actuator(0)	>			Room Public area		~
Guard unit(0)	>			Parameter		1
				Serial number		
				241310100000D Channels	D 4	
				RF connection		>
		2 +	٠	×	7 🗸 Save	
		2 +	٤		7 √ Save	
Device have				t view	7 √ Save	÷
Device type		Repeater(2)	LIS	T VIEW Repeater 1		Û
SmartAP(1)	>	Repeater(2) #2413101000000DD(P Repeater 1	OF)	T VIEW Repeater 1 Serialnumber: 2413101 Short ID: POF		Û
SmartAP(1) - Cylinder(6)	>	Repeater(2) #2413101000000DD(P Repeater 1 Building1s-Floor1s-Public #241640100000084(RE	OF) ic area	T VIEW Repeater 1 Serialnumber: 2413101 Short ID: POF Software version:		1
SmartAP(1)  Cylinder(6)  Repeater(2)	>	Repeater(2) #2413101000000DD(P Repeater 1 Building15-Floor1>Publi	OF) ic area	T VIEW Repeater 1 Serialnumber: 2413101 Short ID: POF Software version:	000000DD	Û
SmartAP(1) - Cylinder(6)	>	Repeater(2)           #2413101000000DD(P           Repeater 1           Building1>Floor1>Publi           #24164010000008(Ri           Repeater 2	OF) ic area	T VIEW Repeater 1 Serialnumber: 2413101 Short ID: POF Software version: Up Position Building	000000DD	
SmartAP(1)  Cylinder(6)  Repeater(2)	>	Repeater(2) #2413101000000DD(P Repeater 1 Building1s-Floor1>Public #24164010000008(RB Repeater 2 Building1s-Floor1>Public	OF) ic area	T VIEW Repeater 1 Softainumbor: 2413101 Short ID: POF Software version: Up Position Building Building	000000DD	· ·
SmartAP(1) Cylinder(6) Repeater(2) RF/IP gateway(0)	>	Repeater(2) #2413101000000DD(P Repeater 1 Building1s-Floor1>Public #24164010000008(RB Repeater 2 Building1s-Floor1>Public	OF) ic area	T VIEW Repeater 1 Serialnumber: 2413101 Short ID: POF Software version: U Position Building Building1 Floor	000000DD	
SmartAP(1) Cylinder(6) Cylinder(7) Repeater(2) RF/IP gateway(0) IP camera(0)	> > > >	Repeater(2) #2413101000000DD(P Repeater 1 Building1s-Floor1>Public #24164010000008(RB Repeater 2 Building1s-Floor1>Public	OF) ic area	T VIEW Repeater 1 Serialnumber: 2413101 Short ID: POF Software version: UI Position Building Building Building Floor Floor	000000DD	•
SmartAP(1) Cylinder(5) Ropostor(2) RF/IP gateway(0) IP camera(0) Culdoor station(0)	> > > >	Repeater(2) #2413101000000DD(P Repeater 1 Building1s-Floor1>Public #24164010000008(RB Repeater 2 Building1s-Floor1>Public	OF) ic area	T VIEW Repeater 1 Serialnumber: 2413101 Short ID: POF Software version: U Position Building Building1 Floor	000000DD	•
SmartAP(1) Cylinder(6) Repeater(2) RF/IP gateway(0) IP camera(0) Cutdoor station(0) Indoor station(0)	> > > > > >	Repeater(2) #2413101000000DD(P Repeater 1 Building1s-Floor1>Public #24164010000008(RB Repeater 2 Building1s-Floor1>Public	OF) ic area	T VIEW Pepeater 1 Serialnumber: 2413101 Short ID: POF Software version: Ut Position Building Building Floor Floor Floor1 Room	000000DD	~
SmartAP(1)     SmartAP(1)     Popatar(2)     Repeatar(2)     RF/IP gateway(0)     IP camera(0)     Outdoor station(0)     Indoor station(0)     C ← IP actuator(0)	> > > > > > >	Repeater(2) #2413101000000DD(P Repeater 1 Building1s-Floor1>Public #24164010000008(RB Repeater 2 Building1s-Floor1>Public	OF) ic area	T VIEW  Repeater 1  Serialnumber: 2413101 Short ID POF Software version:  Ut Position Building Building1 Floor Floor1 Room Public area	000000DD	~
SmartAP(1)     Cylinder(6)     Roposter(2)     RF/IP gateway(0)     IP camera(0)     Outdoor station(0)     Indoor station(0)     C ← IP actuator(0)	> > > > > > >	Repeater(2) #2413101000000DD(P Repeater 1 Building1s-Floor1>Public #24164010000008(RB Repeater 2 Building1s-Floor1>Public	OF) ic area	T VIEW  Repeater 1  Sorialnumbor: 241310 Short ID POF Software version:  Up Position Building Building Building1 Floor Floor Floor1 Room Public area Channels	000000DD	•
SmartAP(1)     Cylinder(6)     Roposter(2)     RF/IP gateway(0)     IP camera(0)     Outdoor station(0)     Indoor station(0)     C ← IP actuator(0)	> > > > > > >	Repeater(2) #2413101000000DD(P Repeater 1 Building1s-Floor1>Public #24164010000008(RB Repeater 2 Building1s-Floor1>Public	OF) ic area	T VIEW  Repeater 1  Sorialnumbor: 241310 Short ID POF Software version:  Up Position Building Building Building1 Floor Floor Floor1 Room Public area Channels	000000DD	× ×
SmartAP(1)     Cylinder(6)     Roposter(2)     RF/IP gateway(0)     IP camera(0)     Outdoor station(0)     Indoor station(0)     C ← IP actuator(0)	> > > > > > >	Repeater(2) #2413101000000DD(P Repeater 1 Building1s-Floor1>Public #24164010000008(RB Repeater 2 Building1s-Floor1>Public	OF) ic area	T VIEW  Repeater 1  Sorialnumbor: 241310 Short ID POF Software version:  Up Position Building Building Building1 Floor Floor Floor1 Room Public area Channels	000000DD	× ×
SmartAP(1)     SmartAP(1)     Popatar(2)     Repeatar(2)     RF/IP gateway(0)     IP camera(0)     Outdoor station(0)     Indoor station(0)     C ← IP actuator(0)	> > > > > > >	Repeater(2) #2413101000000DD(P Repeater 1 Building1s-Floor1>Public #24164010000008(RB Repeater 2 Building1s-Floor1>Public	OF) ic area	T VIEW  Repeater 1  Sorialnumbor: 241310 Short ID POF Software version:  Up Position Building Building Building1 Floor Floor Floor1 Room Public area Channels	000000DD	•
SmartAP(1)     Cylinder(6)     Roposter(2)     RF/IP gateway(0)     IP camera(0)     Outdoor station(0)     Indoor station(0)     C ← IP actuator(0)	> > > > > > >	Repeater(2) #2413101000000DD(P Repeater 1 Building1s-Floor1s-Public #241640100000088(Ri Repeater 2 Building1s-Floor1s-Public	OF) ic area	T VIEW  Repeater 1  Sorialnumbor: 241310 Short ID POF Software version:  Up Position Building Building Building1 Floor Floor Floor1 Room Public area Channels	000000DD	× ×
SmartAP(1)     Cylinder(6)     Roposter(2)     RF/IP gateway(0)     IP camera(0)     Outdoor station(0)     Indoor station(0)     C ← IP actuator(0)	> > > > > > >	Repeater(2) #2413101000000DD(P Repeater 1 Building1s-Floor1s-Public #241640100000088(Ri Repeater 2 Building1s-Floor1s-Public	OF) ic area	T VIEW  Repeater 1  Sorialnumbor: 241310 Short ID POF Software version:  Up Position Building Building Building1 Floor Floor Floor1 Room Public area Channels	000000DD	•
SmartAP(1)     SmartAP(1)     Popatar(2)     Repeatar(2)     RF/IP gateway(0)     IP camera(0)     Outdoor station(0)     Indoor station(0)     C ← IP actuator(0)	> > > > > > >	Repeater(2) #2413101000000DD(P Repeater 1 Building1s-Floor1s-Public #241640100000088(Ri Repeater 2 Building1s-Floor1s-Public	OF) ic area	T VIEW  Repeater 1  Sorialnumbor: 241310 Short ID POF Software version:  Up Position Building Building Building1 Floor Floor Floor1 Room Public area Channels	000000DD	× ×

## 10.3.4 Adding and locating "RF/IP Gateways"

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

- [1] On the "Device configuration" screen, click "RF/IP Gateway".
- [2] Click " <sup>O</sup> ".
- [3] Click "RF/IP Gateway".
- [4] Change the name of the "Electronic locking cylinder".
- [5] Set the position from the drop-down list.
- [6] Click "  $\checkmark$  " to save.

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



### 10.4 Connecting the devices

#### Access the RF connecting screen

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

	CONNECTION					
Design a building by	Configure the devices of	Locating and linking	Add and edit users.	Create and edit actions	Create time control	Configurate door entry
creating floors and rooms	the access control system e.g. Cylinder, repeater	devices	Create user groups			system devices, e.g. indoor station, outdoor station

Please follow the steps below:

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

BUILDINGS		E LIST VIEW	
В	Search		
в	В		
	Building 1	1	>
Building 1			
Buildings(1)			



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

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

۵	⊡ Floor1 ×		:Ξ LIST VIEW
		+	Floor1
		3	All
			Meeting Room 3
Meeting room 4	Justing Room 5	Meeting Room 6	Meeting room 4
( <b>9</b>		(P	Meeting Room 5
			Meeting Room 6
<b>19</b>	ر 🔮		Public area
	0,	Public area	Meeting room 2
F Meeting Room 3			Meeting Room 1
	Heeting from 1_	Managararet Certer	Management Center
	Meeting room 2	Management Certor	
	_		-
	RF/IP gateway		•

#### Connecting the AccessControl devices in a sequence

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

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

## 10.4.1 Connecting "RF Repeaters"

Please follow the steps below:

- [1] On the floor screen, click a "RF Repeater" (e.g. "Repeater 1" for demo case 1).
- [2] Currently no parent device is displayed in the list.
- [3] Click its parent device on the floor plan (e.g. "Smart Access Point" for demo case 1).

	뎡 Floor1 v	+	:≣ LIST VIEW Repeater 1
<b>≠</b> thorage ones 4	€ tweing from 5	المورية	2 Repeater 1
<b>(</b> 9	Meeting room 5	• unital process	
€ Maning Rose 3	@ ,	* Materians 🕑 1	
	€ Sector from 2 ↓ Meeting mon 2	A Background Carter	
	RF/IP gateway		•

#### [4] Wait for the pairing process

<u>0</u>	더 Floor1 🗸				;≝ LIST VIEW
			- 🙁	Ŧ	Repeater 1
i Mantang mana s	★ Manny From 5	🖌 Meeting Phon			
Promytions		ocessing, please wait!	4	1	
	€ F theory out 2 F theory theor	0	eriorit Carator		
	RF/IP gatoway				*

- [5] Coupling between the two devices is indicated by a dashed line if successful.
- [6] Parent device is displayed on the list.
- [7] Click " <sup>†</sup> " to turn back to the floor screen.

Ô	⊡ Floort V		:Ξ LIST VIEW
		- 8 +	Repeater 1
الله Montry som 4		₽ Montry from 6	Parent Devices 6 Smart Access Point
Musing from 3	Image: Second	Productorease 5 Management Control	
	FF/IP galaway		7 •



#### Note

"RF Repeater" must unpair itself with its exist parent device before it is paired with a new device. see chapter 10.11.2 "Disconnecting "RF Repeaters"" on page 256.

## 10.4.2 Connecting "Electronic locking cylinders"

Please follow the steps below:

- [1] On the floor screen, click an "Electronic locking cylinder" (e.g. "Cylinder 1" for demo case 1).
- [2] Currently no parent device is displayed in the list.
- [3] Click its parent device (e.g. "Repeater 1" for demo case 1).

Û	뎡 Floor1 ×			E LIST VIEW	
		- 33	+	Cylinder 1	Ū
				Cylinder 1	
€ Meeting scom 4	Jr Meeting Room 5	€ Meeting Room 6			
		( <b>1</b> 9			
.0	@,	Prate and 3			
🖌 Meeting Room 3					
	Music con 2.	Managarent Carter			
	RF/IP gateway			•	

[4] Wait for the pairing process.

6	뎡 Floor1 v				🗄 LIST VIEW	
			- 🗵	+	Cylinder 1	Û
					Cylinder 1	
if thereginese t	F Maning Provide	Jr Meeting Frank E				
٥		ocessing, please wait!				
	F Maring room 2.	Funger	n Cantor			
	RF/IP gateway				*	

- [5] Hold the maintenance card on the slave "Electronic locking cylinders".
- [6] Click "  $\checkmark$  " to continue.

	뎡 Floor1 ×	E LIST VIEW
	+	Cylinder 1
	Confirm the pairing process(201717E000000F1) 1/3	Cylinder 1 Ê
i danayana t	Ê	
۰		
₽ Maring Trans 3	Activate device Please hold maintenance card on cylinder to proceed	
	Hide the window 6	
	Rif AP gateway	•

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



[8] Wait for the online check.

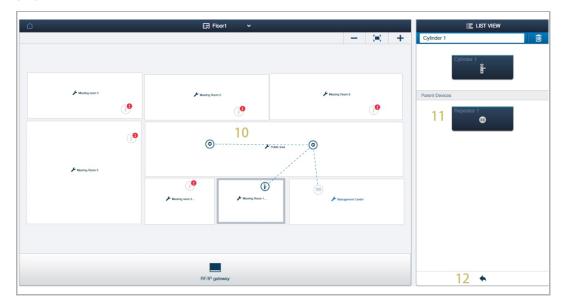
Δ.	뎡 Floor1	:≣ LIST VIEW
Je Marry con 4	Confirm the pairing process(201717E000000F1) 3/3	Cylinder 1
	FiFAP gateway	•

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

۵.	团 Floor1 V	E LIST VIEW
	+	Cylinder 1
	Confirm the pairing process(201717E000000F1) 3/3	Cylinder 1
₽ Metry par 4		
	Ê	
€ Maning News 3	Online check     Im Device is online, pairing is successful	
,	<b>√</b> 9	
	RF/IP gateway	*

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

[11]Parent device is displayed on the list.



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



## Note

"Electronic locking cylinder" must unpair itself from its existing parent device before it is paired with a new device. Page 252.

## 10.4.3 AccessControl device is offline

### Displaying an offline icon when AC devices are offline

An offline icon "9 " will be displayed on the AccessControl device if it is offline.

1. "RF Repeater" is offline

When you find "<sup>1</sup> on a "RF Repeater", please carry out the following operations:

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



#### 2. "Electronic lock cylinder" is offline

When you find "<sup>1</sup> on an "Electronic lock cylinder", please carry out the following operations:

- Check if the battery of the "Electronic lock cylinder" is empty. Page 213.
- Check if its parent device "RF Repeater" is offline.
- Check if the distance between the "Electronic lock cylinder" and its parent device exceeds 10 metres.





#### Note

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

### 10.5 Assigning permissions

#### **10.5.1** Assigning permissions to a user

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

#### Access the designated user screen

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

Users Users     Users     admin1   basic1   cleaner1   jacky   master1   jacky     master1		
Users Users	USERS	E LIST VIEW
Adjuar     basic1     basic1     claner1       admin1     basic1     claner1     jacky     master1		Users
Users		admin1
A     B     C     U     M       admini     basici     cleaneri     jacky       masteri     masteri		basic1
L		cleaner1
	admin1 basic1 cleaner1 jacky master1	jacky
		master1
Users doubs	Users groups	

1. Assigning the ID authentications to a user

Please follow the steps below:

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

īΞ			jacky			: <u>≡</u> LIST VIEW	
						jacky	Û
						User role: Admin	
						Device sharing	
	1					Email address	
:::			Ē		Β	Invitation code :	
Users groups(1)	ID authentication	Pairing devices	Cylinder	IP camera	Outdoor station		
8(·)			-,			User information	
						Personal data	>
						Change password	>
						User permission settings	
						Users groups(1)	>
						ID authentication	>
						Pairing devices	>
						Cylinder	>
						IP camera	>
						Outdoor station	>
		please set user permissi	on under each category			•	
I							

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

2 iacky	E LIST VIEW
ADD NEW AUTHENTIFICATION METHOD Card type Add authentication For access control	ID authentication
Profile Users groups(1) ID authentication Pairing devices Cylinder IP camera Outdoor station	

- [4] Enter the card name.
- [5] Set card type to "RFID".
- [6] Set validity period, there are 2 options:
  - Unlimited validity, it this type is selected, you can continue to the next step.
  - Limited validity, if this type is selected, you need to set the start date and end date by clicking " <sup>131</sup>
- [7] Select any "Electronic locking cylinder" from the drop-down list for swiping the ID authentications.

+ Add authenticiation	ADD AUTHENTICATION	D withentication
	New identity authentication	
	Card name Card - Jacky 4	
	Card type RFID 5	Y
	Validity period Unlimited validity 6	<b>*</b>
	Card reader Select reader	~
	Card number Select reader	
	Cylinder 1 7	
	X Cylinder 2	·
	Cylinder 3	
	ID sutherstication	



#### Note

"Electronic locking cylinder" needs to be paired in a radio line before swiping the ID authentications. see chapter 10.4.2 "Connecting "Electronic locking cylinders"" on page 198.

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

ri⊈in jimiy	i≝ List View
ADD AUTHENTICATION	
Nev add New Keycard/Tag	
Cast Please hold the keycard/lag in front of the card reader to register the credentials to the system. Time out: 119 second	
Stert Step 1 (1)	21
Card	
Card 1 X	

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

E	🛔 jacky	E LIST VIEW
+ Add authentication	Card - Jacky 00210221 1205525818203254	ID authentication Card - Jacky >
Profile	Users groups(1) D authentication(1) Pairing devices Cylinder IP camera Outdoor station	

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



#### Note

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

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

Please follow the steps below:

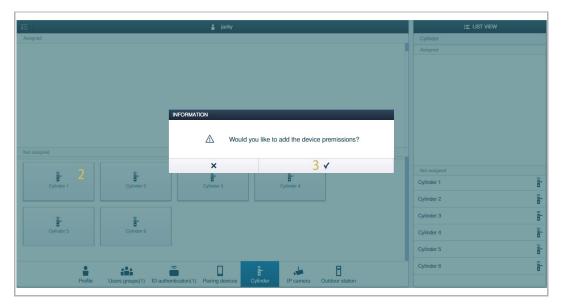
[1] On the designated user screen, click "Cylinder".

Æ			jacky			:Ξ LIST VIEW	
						jacky	Û
						User role: Admin	
						Device sharing	
			1			Email address	
:*:	â		E		8	Invitation code :	
Users groups(1)	ID authentication(1)	Pairing devices	Cylinder	IP camera	Outdoor station		
						User information	
						Personal data	>
						Change password	>
						User permission settings	
						Users groups(1)	>
						ID authentication(1)	>
						Pairing devices	>
						Cylinder	>
						IP camera	>
						Outdoor station	>
		please set user permissi	on under each category			•	

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

[3] Click "  $\checkmark$  " to confirm.

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



## 10.5.2 Assigning the permission to users

You can assign the permission for multiple users by assigning the permission to the user group. Please follow the steps below:

- [1] On the designated user group screen, click "Cylinder".
- [2] Click the designated "Electronic locking cylinder" on the "Not assigned" section.
- [3] Click "  $\checkmark$  " to confirm.

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

Æ	Admin			:E LIST VIEW
			Ad	dmin 🔟
				User permission settings
			U	Jsers(2)
	1		Т	Time Profile >
	· آ	(L) (F	c	Cylinder >
	Profile Cylinder	IP camera Outdoo		P camera >
			0	Dutdoor station >
	please set user permission under each ca	tegory		•
	Admin			
Assigned	Admin		C	;≘ LIST VIEW
Anigred Anigred Retainspred Cylinder=0101	INFORMATION	u like to add the device premise	sions?	IS LIST VIEW

#### 10.5.3 Setting the offline day

In some cases, "Electronic locking cylinder" will be offline. see chapter 10.4.3 "AccessControl device is offline" on page 202.

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



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

#### Offline day

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

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

- [1] On the configuration screen, click "Device configuration", click "Cylinder".
- [2] Click the designated "Electronic locking cylinder".
- [3] Click "Knob reader".
- [4] Enter the number for the offline day. If the offline day is set to "0", only emergency cards can be used. see chapter 10.5.4 "Managing the emergency cards" on page 211.

			LIS	T VIEW					
Device type		Cylinder(6)		Cylinder 1		Knob reader			
SmartAP(1) Cylinder(6)	>	#201717E000000F1(SSM Cylinder 1 Building1>Floor1>Meetin	) ) )	Serialnumber: 201717E000000F1 Short ID: SSM Software version: V1.11		Knob	reader		
Repeater(2)	>	#20121810000005E(UO)	>	Update firmware		_	0		
RF/IP gateway(1)	>	Building1>Floor1>Meetin		Building					
IP camera(1)	>	Cylinder 3 Building1>Floor1>Meetin	g room 3	Building1	~				
Outdoor station(0)	>	#201F8810000087(HLF	>	Floor Floor1	~				
Indoor station(0)	>	Building1>Floor1>Meetin #201737E000000F3(HU)		Room					
IP actuator(0)	>	Cylinder 5 Building1>Floor1>Meetin	>	Meeting room 1	~				
Guard unit(0)	>	#20160810000001F(ESP	) >	Channels RF connection	>				
		Building1>Floor1>Meetin	g room 6	Door opener	>	Parameter Access for users in	offline mode: M	ax.	
				Knob reader 3	>	duration (days) of an device is offline. "0": emergency access of	Only users wit	h	
				Office mode	>	emergency access o	o 0	+	4
				Emergency card Battery status	>	Timeout (seconds) Communication with	SmartAP		
						- [	5	+	
		+	£	*			*		

#### 10.5.4 Managing the emergency cards

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

1. Adding the emergency cards

- [1] On the configuration screen, click "Device configuration", click "Cylinder".
- [2] Click the designated "Electronic locking cylinder".
- [3] Click "Emergency card".
- [4] Click "Emergency card".
- [5] Tick the check box to add the emergency cards.
- [6] Click "  $\checkmark$  " to confirm.

	LIST	VIEW	
Device type	Cylinder(6)	Cylinder 1	Emergency card
SmartAP(1) >	#201717E000000F1(SSM) Cylinder 1 Building1>Floor1>Meeting room 1	Serialnumber: 201717E000000F1 Short ID: SSM Software version: V1.11	Emergency card 4
Repeater(2)	#20121810000005E(UOY) Cylinder 2 > Building1>Floor1>Meeting room 2	Update firmware Position	
■ RF/IP gateway(1) >	#201747E000000F4(PLL) Cylinder 3 > Building1>Floor1>Meeting room 3	Building Building1 ~	
Outdoor station(0)	#201F88100000087(HLF) Cylinder 4 Building15Floor1>Meeting room 4	Floor Floor1 ~	
Indoor station(0)  IP actuator(0)	#201737E000000F3(HUN)	Room Meeting room 1	
Guard unit(0)	Building1>Floor1>Meeting room 5 #20160810000001F(ESP) Cylinder 6 >	Channels RF connection	
	Building 1-Floor1-Meeting room 6	Door opener     >       Knob reader     >       Office mode     >       Emergency card     3       Battery status     >	
	+ 🛃	- view	*
Device type	Cylinder(6)	Cylinder 1	Emergency card
SmartAP(1)	#201717E000000F1(SSM)	Serialnumber: 201717E000000F1	
jr Cylinder(6) >	EMERGENCY CARD Select Name	Card No.	
Repeater(2)	Gard 1 - jacky	00219222	
RF/IP gateway(1)	Card 1 - Faye	00435801 00435810	
IP camera(1)			
Outdoor station(0)			
Indoor station(0)			
O- IP actuator(0)			
Guard unit(0)			
	×	6 🗸	
		Office mode > Emergency card > Battery status >	
	+ 2	*	*

2. Removing the emergency cards

- [1] On the configuration screen, click "Device configuration", click "Cylinder".
- [2] Click the designated "Electronic locking cylinder".
- [3] Click "Emergency card".
- [4] Click "Emergency card".
- [5] Untick the check box to remove the emergency cards.
- [6] Click "  $\checkmark$  " to confirm.

		LIST	VIEW	
Device type	Cylinder(6)		Cylinder 1	Emergency card
SmartAP(1) >	#201717E000000F1(S Cylinder 1 Building1>Floor1>Mee	Z >	Serialnumber: 201717E000000F1 Short ID: SSM Software vension: V1.11	Emergency card 4
Repeater(2)	#20121810000005E(U Cylinder 2 Building1>Floor1>Mee	>	Update firmware Position	
RF/IP gateway(1) >	#201747E000000F4(P	ш)	Building Building1	
Outdoor station(0)	Building1>Floor1>Mee #201F88100000087(H		Floor Floor1	
Indoor station(0)     IP actuator(0)	Building1>Floor1>Mee #201737E000000F3(H	ting room 4	Room Meeting room 1	
Guard unit(0)	Cylinder 5     Building1>Floor1>Mee		Channels	
	#20160810000001F(E) Cylinder 6 Building1>Floor1>Mee	>	RF connection >	
			Knob reader	
			Office mode	
			Battery status	
	+	4	*	*
		LIST	VIEW	
Device type	Cylinder(6)		Cylinder 1	Emergency card
SmartAP(1)	#201717E000000F1(S			Emergency card
	EMERGENCY CARD		Cylinder 1	
SmartAP(1)     Cylinder(6)     Repeater(2)     RF/IP gateway(1)	EXERCISE Civinder 1 EMERGENCY CARD Select	SM) Name	Cylinder 1 Serialrumbar: 201717E000000F1 Shore IN- RDM Card No.	
■ SmartAP(1)         > <sup>*</sup> Cylinder(6)             >               ● Repeater(2)             >	EXERCITAL TEOROGOULE I (S CAUNTER - 1 EMERGENCY CARD Select 5 2 X	SM) Name Card 1 - jacky Card 1 - Faye	Cylinder 1 Seriahumber: 2017/17E000000F1 Share (IN, POM Card No. 00219222 00435801	
SmartAP(1)     Cylinder(6)     Repeater(2)     RF/IP gateway(1)     IP camera(1)	EXERCITAL TEOROGOULE I (S CAUNTER - 1 EMERGENCY CARD Select 5 2 X	SM) Name Card 1 - jacky Card 1 - Faye	Cylinder 1 Seriahumber: 2017/17E000000F1 Share (IN, POM Card No. 00219222 00435801	
SmartAP(1)         > <sup>*</sup> Cylinder(6)             > <b>R</b> Product(6)             > <b>R</b> Pr/IP gateway(1)             > <b>I</b> IP camera(1)             > <b>O</b> Outdoor station(0)             >	EXERCITAL TEOROGOULE I (S CAUNTER - 1 EMERGENCY CARD Select 5 2 X	SM) Name Card 1 - jacky Card 1 - Faye	Cylinder 1 Seriahumber: 2017/17E000000F1 Share (IN, POM Card No. 00219222 00435801	
SmartAP(1)     >       iii     Cylinder(6)     >       iiii     Repeater(2)     >       iiiii     ReF/IP gateway(1)     >       iiiiii     IP camera(1)     >       iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii	EVERATIVE CONCOURT IS CONTACT EVERACENCY CARD Select 5 2 2 2 2 2 2 2 2 2 2 2 2 2	SM) Name Card 1 - jacky Card 1 - Faye	Cylinder 1 Serialrumber: 2017/175000000F1 Store I/N-80M Card No. 0219222 00435801 00435810	
SmartAP(1)         >           Cylinder(6)         >           Repeater(2)         >           RF/IP gateway(1)         >           IP camera(1)         >           Outdoor station(0)         >           Indoor station(0)         >           Indoor station(0)         >	EXERCITAL TEOROGOULE I (S CAUNTER - 1 EMERGENCY CARD Select 5 2 X	SM) Name Card 1 - jacky Card 1 - Faye	Cylindor 1 Setialnumber: 201717E00000F1 Card No. 0219222 0435801 00435810	
SmartAP(1)         >           Cylinder(6)         >           Repeater(2)         >           RF/IP gateway(1)         >           IP camera(1)         >           Outdoor station(0)         >           Indoor station(0)         >           Indoor station(0)         >	EVERATIVE CONCOURT IS CONTACT EVERACENCY CARD Select 5 2 2 2 2 2 2 2 2 2 2 2 2 2	SM) Name Card 1 - jacky Card 1 - Faye	Cylinder 1 Serialrumber: 2017/175000000F1 Store I/N-80M Card No. 0219222 00435801 00435810	
SmartAP(1)         >           Cylinder(6)         >           Repeater(2)         >           RF/IP gateway(1)         >           IP camera(1)         >           Outdoor station(0)         >           Indoor station(0)         >           Indoor station(0)         >	EVERATIVE CONCOURT IS CONTACT EVERACENCY CARD Select 5 2 2 2 2 2 2 2 2 2 2 2 2 2	SM) Name Card 1 - jacky Card 1 - Faye	Cylinder 1 Setialnumber: 201717E00000F1 Dor HV. 2017 Card No. 0219222 00435801 00435810 04435810	Emergency card

### 10.6 Configuring the devices

# 10.6.1 Configuring "Electronic locking cylinders"

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

			LIST	VIEW	r
Device type		Cylinder(6)		Cylinder 1	2
SmartAP(1)	>	#201717E000000F1(SSM)	>	Serialnumber: 201717E000000F1 3 Short ID: SSM	
Cylinder(6)	>	Building1>Floor1>Meeting room 1		Software version: V1.11	
Repeater(2)	>	#20121810000005E(UOY) Cylinder 2 Building1>Floor1>Meeting room 2	>	Update firmware Position	
RF/IP gateway(1)	>	#201747E000000F4(PLL)		Building	
IP camera(1)	>	Cylinder 3 Building1>Floor1>Meeting room 3	>	Building1	~
Outdoor station(0)	>	#201F88100000087(HLF)	>	Floor 6	~
Indoor station(0)	>	Building1>Floor1>Meeting room 4	1	Room	
O- IP actuator(0)	>	#201737E000000F3(HUN) Cylinder 5 Building1>Floor1>Meeting room 5	>	Meeting room 1	•
Guard unit(0)	>	#20160810000001F(ESP)		Channels	
		Cylinder 6	>	RF connection	>
		Building1>Floor1>Meeting room 6		Door opener 8	>
				Knob reader 9	>
				Office mode 10	>
				Emergency card 11	>
				Battery status 12	>
		+ 13	£	•	

No.	Description
1	Rename the device.
2	Remove the device The "Electronic locking cylinder" needs to be unpaired before removing.
3	Serial number of the device.
4	Firmware version of the device.
5	Update the firmware via the website.
6	Assign the location for the device.
7	View RF connection status of the device.
8	Set the unlock time for the "Electronic locking cylinder".
9	Set the offline day for the cylinder see chapter 10.5.3 "Setting the offline day" on page 210.
10	Enable/disable the "Office mode" function see chapter 10.6.4 "Office mode" on page 220.
11	Managing emergency cards see chapter 10.5.4 "Managing the emergency cards" on page 211.
12	Check the battery status of the device.
13	Update the firmware locally or remotely for several devices in batch.

## 10.6.2 Configuring "RF Repeaters"

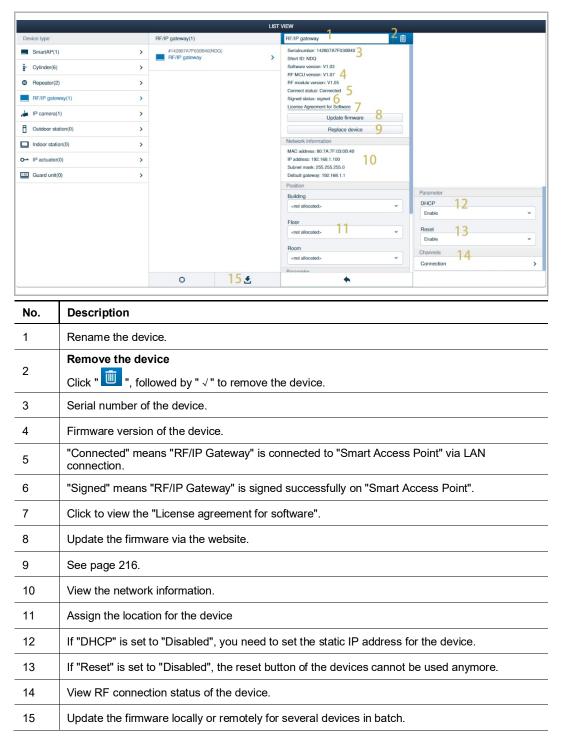
On the configuration screen, click "Device configuration", "Repeater", "Repeater 1" to access the configuration screen.

Device type         Repeater (2)         Prepeater 1         2 (1)           SmatAP(1)			LIST	VIEW
iiii Coulou (r)       iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii	Device type		Repeater(2)	Repeater 1 2
C Cylindri(b) S   Repeater(2) Peppeter 2   Biding1>Foor 1>Public area   C Outdoor station(0)   C Indoor station(0)   D Indoor station(0)   C Indoor station(0)   D Indoor station(0)   C Indoor s	SmartAP(1)	>	Repeater 1	
<ul> <li>Repeater(2)</li> <li>Repeater(2)</li> <li>Peopeater(2)</li> <li>Dubing(1)-Foor(-)-Public area</li> <li>Poolion</li> <li>Bubling(1)</li> <li>Bubling(1)</li> <li>Coundoor station(0)</li> <li>Indoor station(0)</li> <li>Indoor station(0)</li> <li>Guard unit(0)</li> <li>Guard unit(0)</li> <li>Repeater(2)</li> <li>Peopeater(2)</li> <li>Peopeat</li></ul>	- Cylinder(6)	>		5
RF/IP gateway(1)       >         IP camora(1)       >         Outdoor station(0)       >         Indoor station(0)       >         IP actuator(0)       >         Guard unit(0)       >         Refine gateway(1)       >         Refine gateway(1)       >         Refine gateway(1)       >         Pactuator(0)       >         Refine gateway(1)       >         Refine gateway(1) <t< th=""><th>Repeater(2)</th><th>&gt;</th><th>Repeater 2</th><th></th></t<>	Repeater(2)	>	Repeater 2	
Percencer(1) Ouddoor station(0) Indoor station(0) Poor Poor Poor Point area Channels RF connection RF connection RF connection To a station of the state of the	RF/IP gatew	ay(1) >	Building1>Hoor1>Hublic area	
Condoor station(0)       >         Indoor station(0)       >         Guard unit(0)       >         Guard unit(0)       >         RF connection       7         NF connection       7	IP camera(1)	>		Building1 ~
Indoor station(0)   Indoor station(0)   Indoor station(0)   Image: Statistic (0)   Image: Statistic (0) <tr< th=""><th>Outdoor stat</th><th>ion(0) &gt;</th><th></th><th>Floor 6</th></tr<>	Outdoor stat	ion(0) >		Floor 6
Image: Packuator(0)       >         Image: Guard unit(0)       >         Reconnection       7         RF connection       7	-			Floor1
Channels RF connection 7 >	Indoor station	n(0) >		Room
RF connection 7 >	O- IP actuator(0	) >		Public area V
RF connection 7 >	Guard unit(0	) >		Channels
+ 8 £ .				RF connection 7 >
			+ 8 £	*
	1	Rename the dev	ice.	

110.	Decomption
1	Rename the device.
2	Remove the device The device needs to be unpaired before removing.
3	Serial number of the device.
4	Firmware version of the device.
5	Update the firmware via the website.
6	Assign the location for the device.
7	View RF connection status of the device.
8	Update the firmware locally or remotely for several devices in batch.

### 10.6.3 Configuring "RF/IP Gateways"

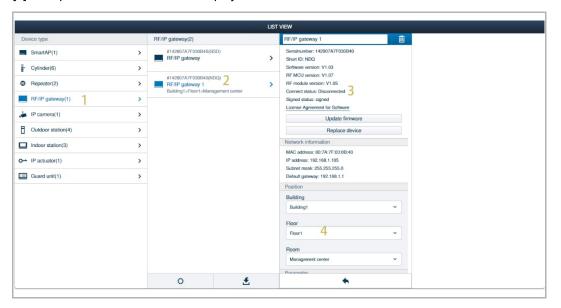
On the configuration screen, click "Device configuration", "RF/IP Gateway", "Cylinder 1" to access the configuration screen.



#### Replacing a new device

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

- [1] On the "Device configuration" screen, click "RF/IP Gateway".
- [2] Click the "RF/IP Gateway 1".
- [3] The connected status should be "Disconnected" if this old one is broken.
- [4] The position of the old one is displayed on the screen.



- [5] Add a new one without position. see chapter 10.3.4 "Adding and locating "RF/IP Gateways"" on page 193.
- [6] The connected status of the new one should be "Connected".
- [7] The position of the new one is empty currently.
- [8] Click "Replace device" on the new one.
- [9] Click the old one on the list.
- [10]Click "  $\checkmark$  " to continue if the device is replaced successfully.

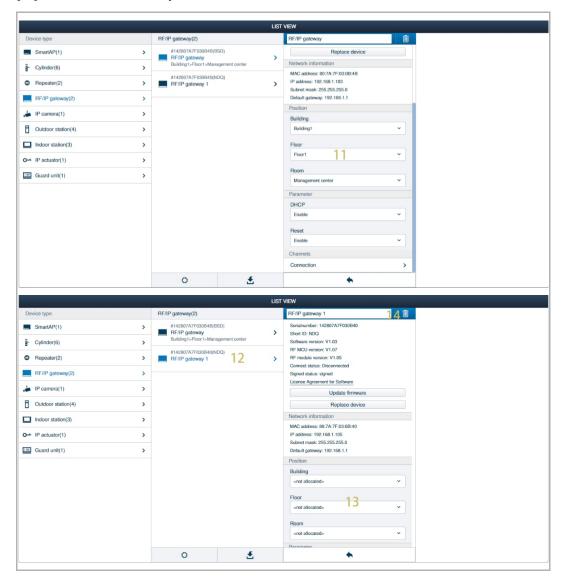
			IST VIEW	
Device type		RF/IP gateway(2)	RF/IP gateway	Ū
SmartAP(1)	>	#142807A7F030B4B(BSD)	Serialnumber: 142807A7F030B4B Short ID: BSD	
- Cylinder(6)	>	#142807A7F030B40(NDQ)	Software version: V1.03 RF MCU version: V1.07	
Repeater(2)	>	Bridding1>Floor1>Management center	RF module version: V1.05 Connect status: Connected 6	
RF/IP gateway(2)	>		Signed status: signed License Agreement for Software	
IP camera(1)	>		Update firmware	
Outdoor station(4)	>		Replace device 8	
Indoor station(3)	>		Network information MAC address: 80:7A:7F:03:0B:4B	
O- IP actuator(1)	>		IP address: 192.168.1.103 Subnet mask: 255.255.255.0	
Guard unit(1)	>		Default gateway: 192.168.1.1	
			Position Building	
			<not allocated=""></not>	~
			Floor	
			<not allocated=""> 7</not>	~
			Room	
			<not allocated=""></not>	*
		0 <u>£</u>	Paramotor.	
		U 2		
			IST VIEW	
			RF/IP gateway	
SmattAP(1)				
Ē- Cγlinder(6)		Replace device		
C Repeator(2)		Serialnumber: 142807A7F030B40 RF/IP gateway 1		,
		RF/IP gateway 1 9		
IP camera(1)		INFORMATION		
Outdoor station(4)		Succeed to replace the second seco	e device, reload the webpage to get	
Outdoor station(4)  Indoor station(3)		Succeed to replace the the device settings.	e device, reload the webpage to get	
		the device settings.		
Indoor station(3)		the device settings.	e device, reload the webpage to get	
Indoor station(3)		the device settings.		
Indoor station(3)		the device settings.	) 🗸	
Indoor station(3)		the device settings.		
Indoor station(3)		the device settings.	) 🗸	
Indoor station(3)		the device settings.	) ✓ Floor	
Indoor station(3)		the device settings.	► Floo: -rec attocated=	-
Indoor station(3)		the device settings.	► Floor -roo attocateds Poor	

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

[12]Click the old one.

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

[14]Click "  $\fbox$  ", followed by "  $\checkmark$  " to remove the old one.



[15]Click the new one.

[16]Rename the new one.

[17]Click "  $\checkmark$  " to save.

E.

		LIS	T VIEW
Device type		RF/IP gateway(1)	RF/IP gateway 1 0
SmartAP(1)	>	#142807A7F030B4B(BSD) 15 Bilding1s-Roorts-Management center	Serialnumber: 142807A7F030B4B Short ID: BSD
Cylinder(6)	>	Printing 121 1001 (218) and generate Control	Software version: V1.03 RF MCU version: V1.07
Repeater(2)	>		RF module version: V1.05
RF/IP gateway(1)	>		Connect status: Connected Signed status: signed License Agreement for Software
IP camera(1)	>		Update firmware
Outdoor station(4)	>		Replace device
Indoor station(3)	>		Network information
O- IP actuator(1)	>		MAC address: 80:7A:7F:03:0B:4B IP address: 192.168.1.103 Subnet mask: 255.255.255.0
Guard unit(1)	>		Default gateway: 192.168.1.1
			Position
			Building V
			Floor
			Floor1 v
			Room
			Management center v
			Paramotor
		0 🛃	× 17 ✓ Save

### 10.6.4 Office mode

## Access the "Time control" screen

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

		PLACE + LINK	USER MANAGEMENT	ACTIONS		DOOR ENTRY SYSTEM
Design a building by creating floors and rooms	Configure the devices of the access control system e.g. Cylinder, repeater	Locating and linking devices	Add and edit users. Create user groups	Create and edit actions	Create time control	Configurate door entry system devices, e.g. indoor station, outdoor station
🛔 jacky					Device	e configuration 🏾 🔅 Preferences

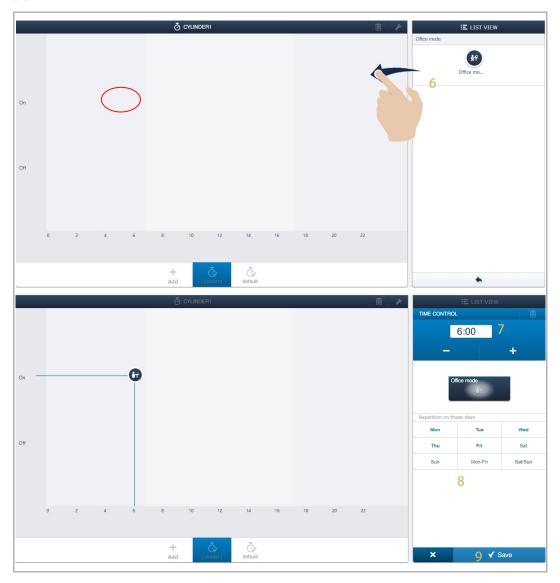
1. Adding "Office mode" time profile for the designated "Electronic locking cylinder" Please follow the steps below:

- [1] On the "Time control" screen, click "Add".
- [2] Enter the name (e.g. "Cylinder1").
- [3] Click "  $\checkmark$  " to save.

				î >	E LIST VIEW
Selected profile V Mon	Tue W	fed Thu	Fri Sat	Sun	
	CREATE TIME PROFILE				All
	Cylinder1				Central Functions >
	State	Cylinder1			Buildingt >
	Name	Cylinder1 2			
	Copy time profile	You can choose another timers. They will be copi	time profile and integrate ied to this time profile.	its	
		↑ default			
*					
Day/night swit 0 2 4 6:00 8					
	×		3 √		
	1 + Č	ult			

- [4] Click "Building1">>"Floor 1">>"Meeting room 1" to access the location of the designated "Electronic locking cylinder".
- O CYLINDER1 E LIST VIEW ۶ Selected profile Tue Wed Thu ~ Fri Sat All Central Functions Building1 4 default + Add ē, × Ö CYLII ١. E LIST VIEW Selected profile Sat Cylinder 1 (Office mode) 5 **(†**7 default + Add Ō, -
- [5] Click the designated "Electronic locking cylinder" (e.g. "Cylinder 1")

- [6] Drag the "Office mode" icon onto the "On" position on the screen.
- [7] Enter the precise time.
- [8] Click the designated day to cancel the selection (optional).
- [9] Click "  $\checkmark$  " to save.

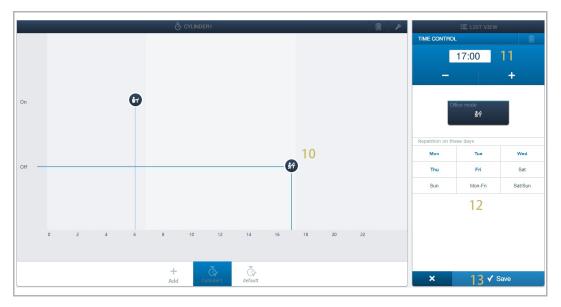


[10]Drag the "Office mode" icon into the "Off" position on the screen.

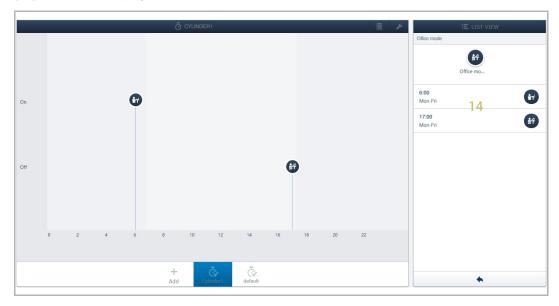
[11]Enter the precise time.

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

[13]Click "  $\checkmark$  " to save.



[14]The result is displayed on the screen.



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

- On the "Time control" screen, click the designated "Electronic locking cylinder" (e.g. "Cylinder 1").
- [2] Click " 🗡 ".
- [3] Enter a new name.

	õ	CYLINDER1				1 4	\Xi LIST VIEW
Selected profile	Mon	Tue	Wed Th	u Fri	Sat	Sun 🕹	Meeting room 2
	EDI	T TIME PROFILE				-1	Cylinder 2 (Office mode)
		Cylinder1					
		State	Cylinder1	<b>x</b>			
		Name	Cylinder1	3			
G							
Office mode							
0 2 4 6:00	8	×	¢		×		
	+ Add	Cylinder1	default				*

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

- On the "Time control" screen, click the designated "Electronic locking cylinder" (e.g. "Cylinder 1").
- [2] Click " 🔟 ".
- [3] Click "  $\checkmark$  " to confirm.

	Q CATIND	R1				2 🕮 🖌	E LIST VIEW
Selected profile ~	_	Wed	Thu	Fri	Sat	Sun	All
							All
							Central Functions >
							Building1 >
		Confirmation					
		? ·	Vould like to remov	e this timer prof	le?		
		×		3√			
G			<b>k</b> t				
0 2 4 6:00	8 10 12	14 16	Office mod 17:00	e 18	20	22 0	
	+	<u>مَ</u> رَق	×				
	Add	ylinder1 defa	uit				

## 10.7 Controlling the devices via "Smart Access Point"

### Accessing the control screen

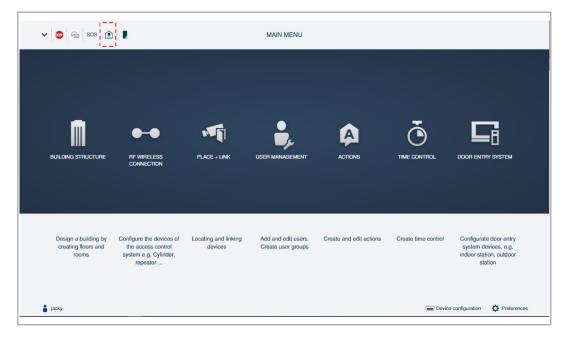
1. The following operation can be operated by all users:

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

ل. ا	lacky's Pro
PLEASE LOGIN	
amon	
🛔 faye	
	CONTROL

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

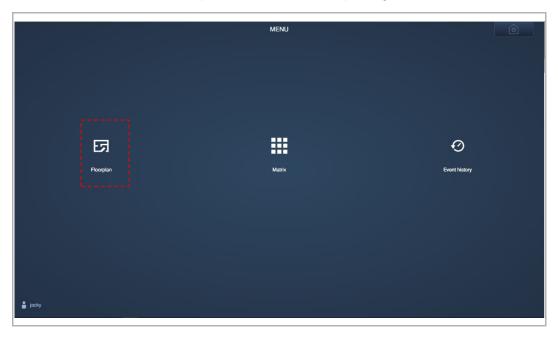
On the configuration screen, click " 🗊 " to access the control screen.



## 10.7.1 Controlling the devices via floorplan

#### Accessing the floorplan screen

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

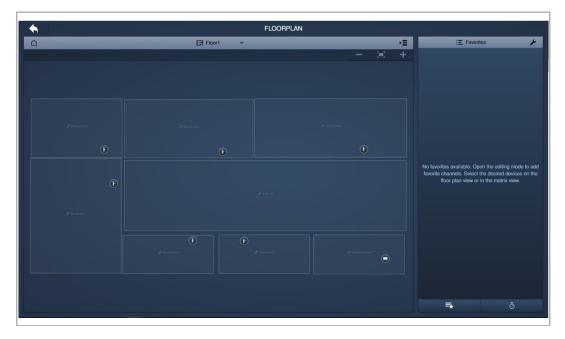




## Note

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

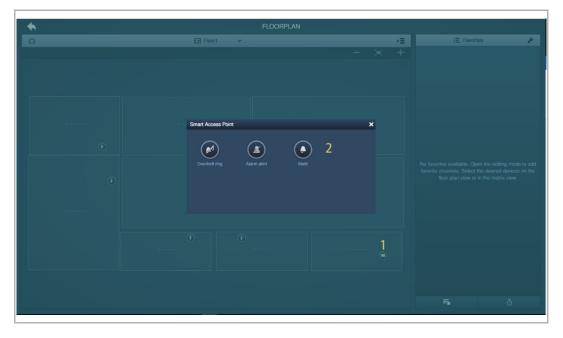
Click "Building 1", "Floor 1" to access the floorplan screen.



1. Control the function of "Smart Access Point"

Please follow the steps below:

- [1] On the floorplan screen, click "Smart Access Point".
- [2] Click a function icon to operate the function.



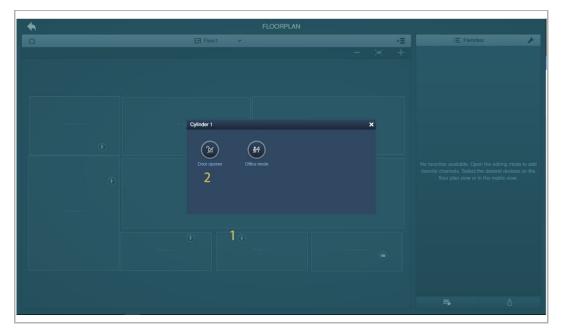
2. Release the designated "Electronic locking cylinder"

- [1] On the floorplan screen, click the designated "Electronic locking cylinder" (e.g. "Cylinder 1" for demo case 1).
- [2] Click "Door opener" icon to release the "Electronic locking cylinder".



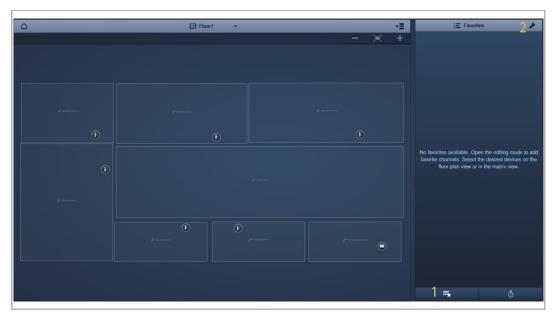
3. Enable/disable the office mode for the designated "Electronic locking cylinder"

- [1] On the floorplan screen, click the designated "Electronic locking cylinder" (e.g. "Cylinder 1" for demo case 1).
- [2] Click "Office mode" icon to enable/disable the "office mode" function, see chapter 10.6.4 "Office mode" on page 220.

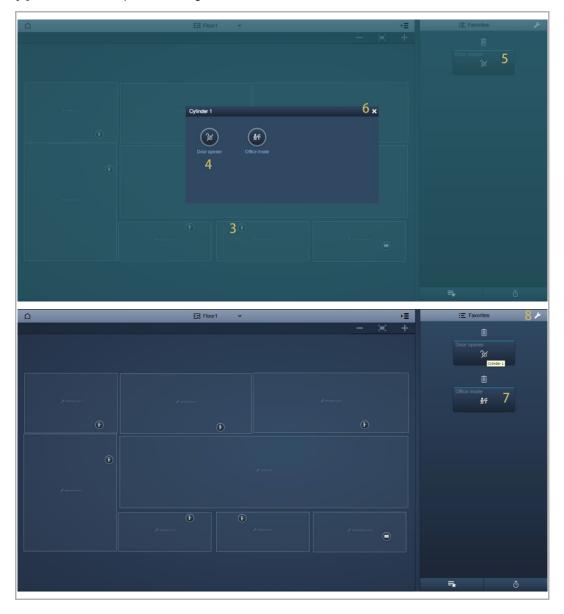


4. Add the designated operations to the favorites list

- [1] On the floorplan screen, click "  $\blacksquare$  ".
- [2] Click " 📕 ", a highlight indicates the setting status.

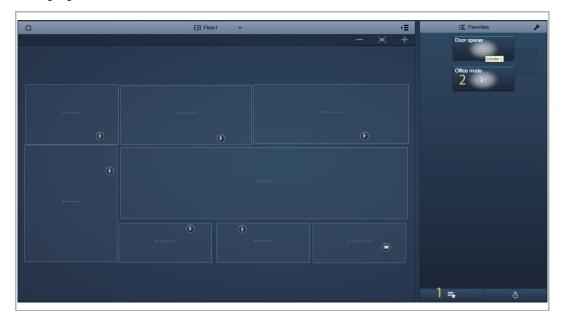


- [3] On the setting status, click an AccessControl devices (e.g. "Cylinder 1").
- [4] Click a function icon (e.g. "Door opener").
- [5] The function icon will be added to the favorites list.
- [6] Click "x" to close the pop-up window.
- [7] Repeat the steps 3~6 to add other operations one by one.
- [8] Click "



5. Operate the functions on the favorite list

- [1] On the floorplan screen, click "  $\blacksquare$  ".
- [2] Click the designated function icon on the favorites list to activate/deactivate the function, the highlight indicates the activated status.



6. Remove the functions from the favorites list

- [1] On the floorplan screen, click "  $\blacksquare$  ".
- [2] Click " I , a highlight indicates the setting status.
- [3] Click " 🔟 " to remove it directly.



7. Enable/disable the time profiles

Please follow the steps below:

- [1] On the floorplan screen, click " Ŏ ".
- [2] Click " 📕 ", a highlight indicates the setting status.

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

۵	G Floort V		•≡	
				edual & 3
¢				
Đ		Ð		
Jenneser				
			0	
				=, 1 <sub>ð</sub>

## 10.7.2 Controlling the devices via matrix

#### Accessing the matrix screen

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



# Note

The operations on the matrix screen are the same to floorplan screen. see chapter 10.7.1 "Controlling the devices via floorplan" on page 228.

Ο

#### 10.8 Controlling the devices via Welcome App

## 10.8.1 Pairing "Smart Access Point" with Welcome App

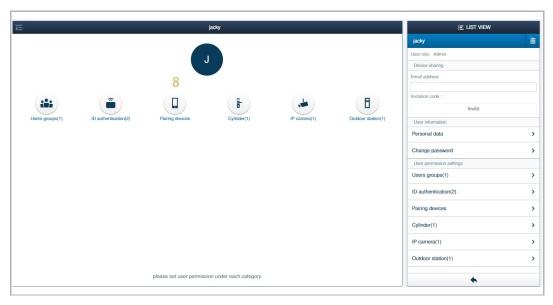
Please follow the steps below:

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

❤ 🥝 🗟 sos 🕅			MAIN MENU			
BUILDING STRUCTURE		PLACE + LINK	USER MANAGEMENT	ACTIONS	TIME CONTROL	DOOR ENTRY SYSTEM
Design a building by creating floors and rooms	Configure the devices of the access control system e.g. Cylinder, repeater	Locating and linking devices	Add and edit users. Create user groups	Create and edit actions	Create time control	Configurate door entry system devices, e.g. indoor station, outdoor station

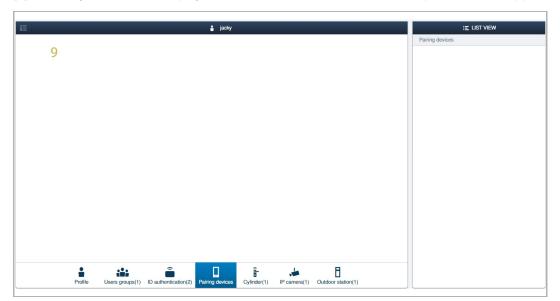
- [2] Click "MyBuildings Account".
- [3] Click "Connection".
- [4] Enter the account, password and friendly name.
- [5] Tick "Enable" to activate "Remote access" function. (optional).
- [6] Click "Login".
- [7] Check the pair status and connect status. Green " √" will be displayed if the connection is successful.

	C PREFE	RENCES					
Preferences	MyBuildings Account	MyBuildings Account					
System information >	Connection 3	Please use your MyBuildings account information to register this device with MyBuildings. If you do not have account yet, you can register here. For more information about MyBuildings, refer to the help.					
Network settings >	License >	At present, the remote function is temporarily in the trial operation phase.					
Localization >		Pair: 🗸 Connect: 🖌 7					
Project backups >		User name jackycheng003					
Firmware updates >		Password 4					
MyBuildings Account 2		Friendly name Jacky's Pro					
Service >		UUID 56871711-7a15-4d0c-9d1e-e931c9cd2fa9					
Wi-Fi access point mode settings		Remote access C Enable 5					
Third party authority >							
Abnormal devices >							
Onvif IPC list							
Misc settings >							
	4	♠					



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

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



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

[11]Tap "Pair devices".

[12]Tap "SmartAP".

✓ 10 Home	∧ Home	< Pair Devices
"jacky" iPhone, No events	Settings	IP Gateway/Touch Panel
	Pair Devices 11	
	Account name and license information	IP Camera
		SmartAP 12
	Notifications and Sounds	
$\wedge$	Configuration mode	
	Firmware upgrade	
"jacky" iPhone	About >	
	Log out	
Events 🔨		
🔺 💀 🏓 🕅		

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

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

[15]Tap "  $\checkmark$  " to confirm.

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

< SmartAP	E C	<	SmartAP	C (	<	SmartAP	E C
Token ID 1358 13AC					Token ID 1		
Paired					Paired		
Remote device					Remote de		
Jacky's Pro 13 2eba80010d5f(192.168.1.101)	Pair			Pair	Jacky's I 2eba8001		Pair
Local device		Local device			Local devi		
		Notice				Notice	
		Account jacky	14			1 Please enter the token ID : 138 13AC on the SmartAP.	
		×	15 🧹 Resend pairing	j request		🗙 🗸 ок	

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

E	🛔 jacky		:Ξ LIST VIEW	
			Pairing devices	
L 17			"jacky" iPhone	>
"jacky" iPhone				
Pairing				
<b>:</b> : <b>:</b> : 🔒	📘 🔓 🦊	8		
Profile Users groups(1) ID authentication(2	2) Pairing devices(1) Cylinder(1) IP camera(1)	Outdoor station(1)		

[18]Click "Pairing".

[19]Enter the token ID (refer to step 16).[20]Click "√" to confirm.

ΤΞ	🛔 jacky	:≣ LIST VIEW
E Vacy Krow Parag	PARING MOBILE DEVICE WITH "JACKY" IPHONE Please enter the token code in your Welcome app to pair your mobile device.           1       3       5       8       1       3       A       C	Ist UST VIEW       Tacky "Phone       Paring operation       Paring 18       Device information       usid : earl/98ce.eb8e-4739-9cx9-9cb91tcd8cr6d
Profile Users groups(1) ID auther		•

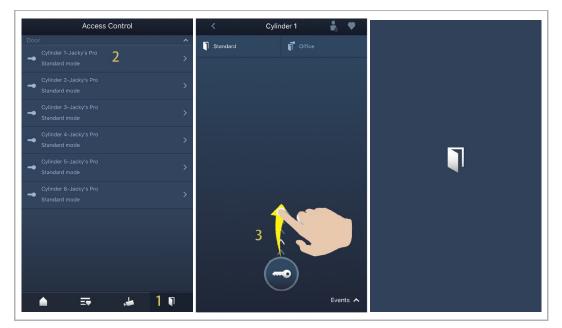
[21]"Paired" status is displayed on the screen if successful.

E	🛔 jacky				E LIST VIEW
••				Pairing devices	
jacky IPhone 21				"jacky" iPhone	>
Paired					
÷ :•:	â .	î 🎍	8		
Profile Users groups(1)	ID authentication(2) Pairing devices(1)	Cylinder(1) IP camera(1)	Outdoor station(1)		

## 10.8.2 Controlling "Electronic locking cylinders" via Welcome App

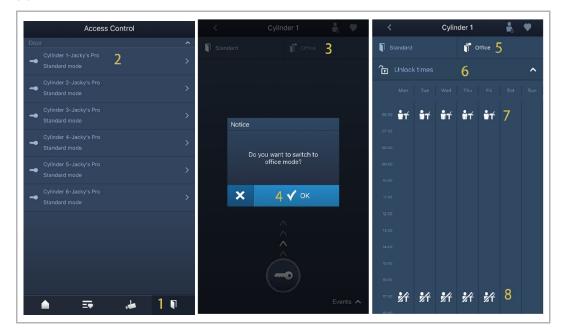
#### Releasing the "Electronic locking cylinder"

- [1] On the Welcome App "Home" screen, tap " 🗊 ".
- [2] On the AccessControl screen, tap the designated "Electronic locking cylinder" to access the corresponding screen.
- [3] Swiping the lock icon up to release the "Electronic locking cylinder".



#### Enable/disable "Office mode"

- [1] On the Welcome App "Home" screen, tap "
- [2] On the AccessControl screen, tap the designated "Electronic locking cylinder" to access the corresponding screen.
- [3] Click "Office".
- [4] Click " $\sqrt{}$ " to confirm.
- [5] Click "Office".
- [6] Click "Unlock times".
- [7] Office mode is enabled on the time.
- [8] Office mode is disabled on the time.



## 10.9 Managing the backup

It is important to create a backup regularly.

For more information, see chapter 13.5 "Managing the backup" on page 317.

			RENCES			
Preferences		Project backups	Backup for the AccessControl devides - 20200801			
System information >	>	Create new project backup +	Description	Backup for the AccessControl devides 1. Creating a building - Done 2. Adding and locating the devices - Done		
Network settings	>	Import project backup		<ol> <li>Connecting the devices - Done</li> <li>Adding users and user groups - Done</li> <li>Assigning the users to the user groups - Done</li> </ol>		
Localization	>	Auto backuped, at 2020-07-30 16:35:47. Router firmware ID: 0149, Router firmware ver >		6. Assigning the permission to users - Done 7. Assigning the permission to user groups - Done 8. Configuring the devices - Done 9. Controlling the devices via "Smart Access Poin" - Done		
Project backups	>	2020-07-30 16:35:48	48	10. Controlling the devices via Welcom App - Done		
Firmware updates	>	Auto backuped, at 2020-07-30 16:35:07. Router firmware ID: 0149, Router firmware ver > 2020-07-30 16:35:07				
MyBuildings Account	>	Auto backuped, at 2020-07-30 16:26:11.				
Service	>	Router firmware ID: 0149, Router firmware ver > 2020-07-30 16:26:12				
Wi-Fi access point mode settings	>	Auto backuped, at 2020-07-30 16:23:56. Router firmware ID: 0149, Router firmware ver >				
Third party authority	>	2020-07-30 16:23:57				
Abnormal devices	>	Auto backuped, at 2020-07-30 16:22:40. Router firmware ID: 0149, Router firmware ver > 2020-07-30 16:22:40				
Onvif IPC list	>					
Misc settings	>	Auto backuped, at 2020-07-30 16:22:31. Router firmware ID: 0149, Router firmware ver > 2020-07-30 16:22:31				
		Auto backuped, at 2020-07-30 16:21:40.				
		*	×	4 ✓ Save		

#### 10.10 Removing permissions

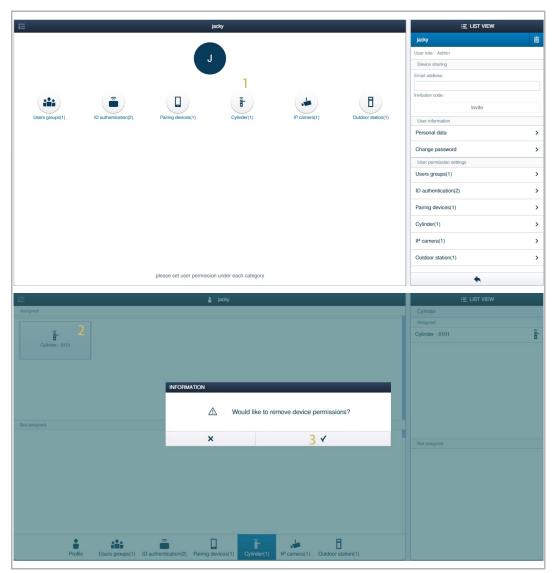
#### 10.10.1 Removing permissions for a user

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

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

- [1] On the designated user screen, click "Cylinder".
- [2] Click the designated "Electronic locking cylinder" on the "Assigned" section.
- [3] Click "  $\checkmark$  " to confirm.

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

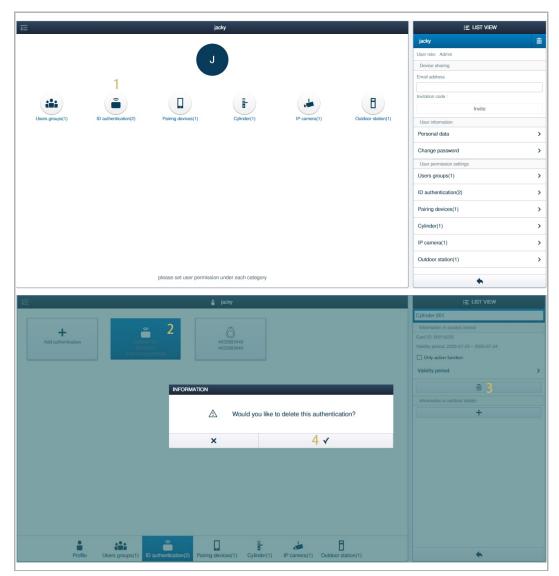


2. Removing the designated ID authentications from a user

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

- [1] On the designated user screen, click "ID authentication" to access the corresponding screen.
- [2] Click the designated ID authentication.
- [3] Click " 🔟 ", if the card belongs to "Emergency card", please remove the emergency card first. see chapter 10.5.4 "Managing the emergency cards" on page 211.
- [4] Click "  $\checkmark$  " to confirm.

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



#### 10.10.2 Removing the permissions for the users in a group

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

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

- [1] On the designated group screen, click "Cylinder".
- [2] Click the designated "Electronic locking cylinder" in the "Assigned" section.
- [3] Click "  $\checkmark$  " to confirm.

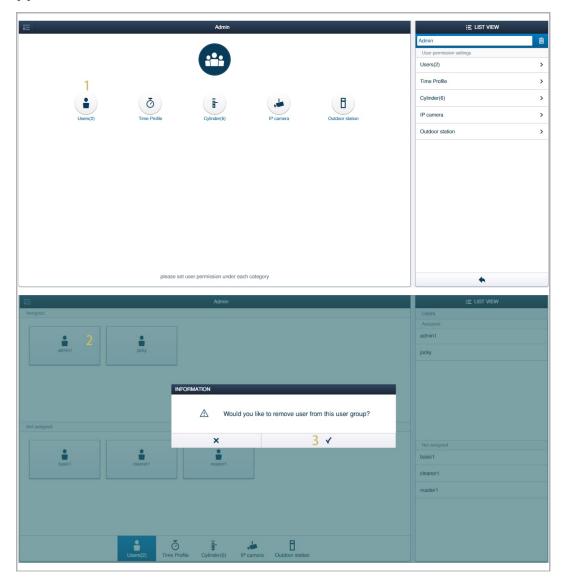
Æ		Admin			E LIST VIEW	v
					Admin	Û
					User permission settings	
					Users(2)	>
		1			Time Profile	>
	• (ð	( <b>-</b>	4	8	Cylinder(6)	>
	Users(2) Time Profile	Cylinder(6)	IP camera	Outdoor station	IP camera	>
					Outdoor station	>
	ple	ease set user permission under each cate	egory		•	
·						
Assumed		Admin			i≣ List viev	v
Assigned		Admin				v
Assigned	ede	Admin B- 2	cube		E LIST VIEW	v ملط
	Cylinteer 6		Cylinder 5:		Cylinder Assigned	6.dba
ŝ		Ē 2			E LIST VIEW	edus edus
Cylinder 2	Cylinder 6	ë 2 <sub>Cylinder 1</sub>			E LIST VIEW Cylinder Assigned Cylinder 2 Cylinder 6	ceps ceps
Cylinder 2	Cylinder 5	Ē 2			E LIST VIEW Cylinder 2 Cylinder 1 Cylinder 1	copio copio copio
Cylinder 2	Cylinder 6	Cylinder 1 2		permissions?	E LIST VIEW Cylinder Assigned Cylinder 2 Cylinder 1 Cylinder 5 Cylinder 3	adao adao adao adao adao
Cylinder 2	Cylinder 6	Cylinder 1 2	Cytinder 5		E LIST VIEW	copio copio copio
Gyindar 2	Cylinder 6	Cylinder 1 2	Cytinder 5	permissions?	E LIST VIEW Cylinder Assigned Cylinder 2 Cylinder 1 Cylinder 5 Cylinder 3	adao adao adao adao adao
Gyindar 2	Cylinder 6	Cylinder 1 2	Cytinder 5		E LIST VIEW	adao adao adao adao adao
Gyindar 2	Cylinder 6	Cylinder 1 2	Cytinder 5		E LIST VIEW	adao adao adao adao adao
Gyindar 2	Cylinder 6	Cylinder 1 2	Cytinder 5		E LIST VIEW	adao adao adao adao adao
Gyindar 2	Cylinder 6	Cylinder 1 2	Cytinder 5		E LIST VIEW	adao adao adao adao adao
Gyindar 2	Cylinder 6	Cylinder 1 2	Cytinder 5		E LIST VIEW	adao adao adao adao adao
Gyindar 2	Cylinder 6	INFORMATION A Would X	Cylinder 5		E LIST VIEW	adao adao adao adao adao
Gyindar 2	Cylinder 6	Controler 1 2	Cylinder 5		E LIST VIEW	adao adao adao adao adao

2. Removing designated users from the user group

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

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

- [2] Click the designated user on the "Assigned" section.
- [3] Click "  $\checkmark$  " to confirm.



### 10.11 Disconnecting the devices

#### Accessing the RF connections screen

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

	RF WIRELESS CONNECTION	PLACE + LINK	USER MANAGEMENT			DOOR ENTRY SYSTEM
Design a building by creating floors and rooms	Configure the devices of the access control system e.g. Cylinder, repeater	Locating and linking devices	Add and edit users. Create user groups	Create and edit actions	Create time control	Configurate door entry system devices, e.g. indoor station, outdoor station

Please follow the steps below:

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

BUILDINGS		E LIST VIEW	
В	Search		
в	В		
	Building 1	1	>
Building 1			
Buildings(1)			



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

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

	⊡ Floor1 ×			E LIST VIEW	
		—	) = +	Floor1	
			3	All	
				Meeting Room 3	
Jr Meeting more 4	Meeting floom 5	Meeting Room 6 کی		Meeting room 4	
<b>P</b>	· seeing room s		P	Meeting Room 5	
	U			Meeting Room 6	
<b>•</b>	<b>e</b>	town CO		Public area	
	0	F Public area		Meeting room 2	
Meeting Room 3				Meeting Room 1	
	Justing room 2	m L. Management Cer		Management Center	
	Meesing nome_	Anagement La	ar .		
				•	

#### Disconnecting the AccessControl devices in a sequence

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

- [1] Disconect the "Electronic locking cylinder" with its parent devices.
- [2] Disconnect the "RF Repeater" with its parent devices.

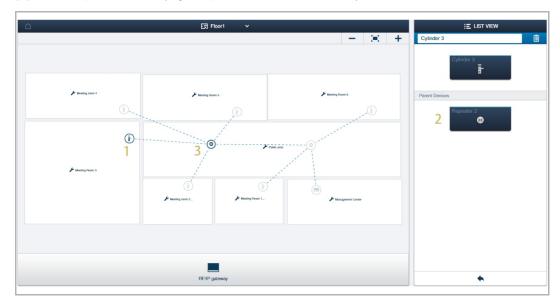
## 10.11.1 Disconnecting "Electronic locking cylinders"



#### Attention!

It is recommended the "Electronic locking cylinder" to be unpaired when online. If the "Electronic locking cylinder" is unpaired when online, it can be used normally in other system. If it is forcibly unpaired when offline, it can only be used in current system and cannot be used in other system. see chapter 10.4.3 "AccessControl device is offline" on page 202.

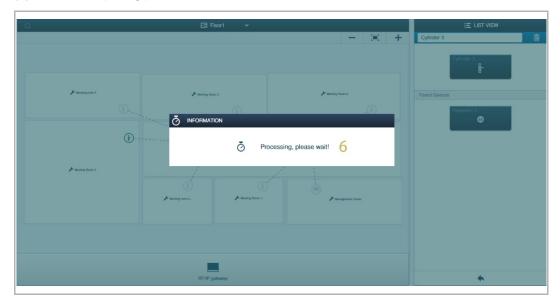
- [1] On the floor screen, click an "Electronic locking cylinder" (e.g. "Cylinder 3" for demo case 1).
- [2] Its parent device is displayed on the list.
- [3] Click its parent device (e.g. "Repeater 2" for demo case 1).



- [4] Enter the serial number of the "Electronic locking cylinder".
- [5] Click "  $\checkmark$  " to confirm.

۵.	团 Floor1 v		E LIST VIEW
			Cylinder 3
	✓ Meeting Rese 5 Confirm unpairing operation	Jr Marry Ross 6	Parent Devices Preparator 2
بند مربع به مربع المربع	Please enter the serialnumber of devic Serialnumber 201747E00000		
	F thereignen 2	P theypert Carte	
	-		
	RF/IP gateway		*

[6] Wait for the pairing process.



[7] Click "  $\checkmark$  " to continue.

۵.	더 Floor1 🗸			:Ξ LIST VIEW	
			<b>—</b> +		١.
_	Confirm unpairing operation(201747E000000F4	i) 1/3	-	Cyloder 3 B	
F Many cont		Ì		Parent Devices Fargemente 2	
i interesting the state	Deactivate device		-		
	Hide the window	7 ✓			
	RF/IP gatuway			*	

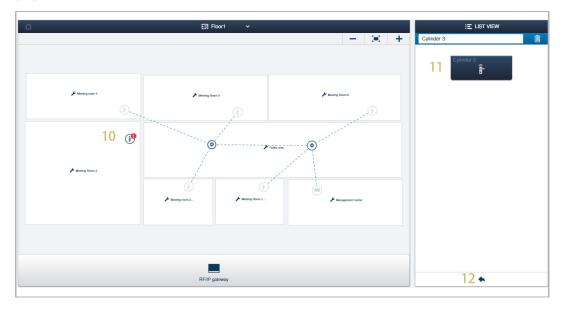
[8] Wait for the LED on the "Electronic locking cylinder" to flash green or sound a beep.[9] Click " √ " to continue.

☐	E LIST VIEW
	Cylinder 3
Confirm unpairing operation(201747E000000F4) 23	Cylinder 3
_	
RF/A <sup>P</sup> gateway	*

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

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

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



## 10.11.2 Disconnecting "RF Repeaters"



#### Attention!

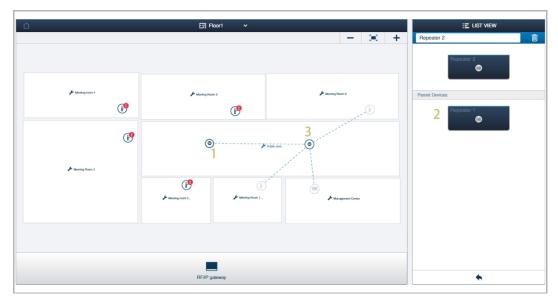
The "RF Repeater" needs to be restore to factory default settings before being use in other system by holding the reset button for 3 seconds. see chapter 10.4.3 "AccessControl device is offline" on page 202.



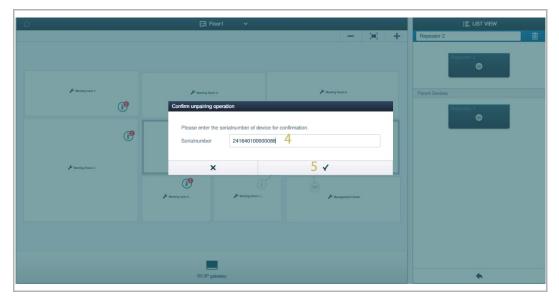
## Attention!

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

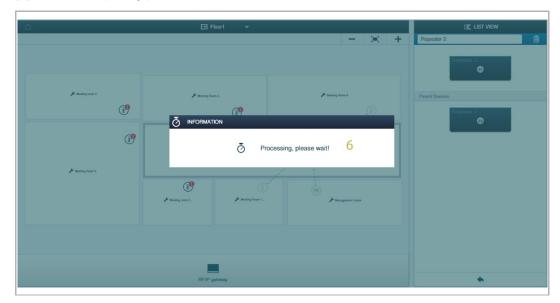
- [1] On the floor screen, click a "RF Repeater" (e.g. "Repeater 2" for demo case 1).
- [2] Its parent device is displayed on the list.
- [3] Click its parent device (e.g. "Repeater 1" fore demo case 1).



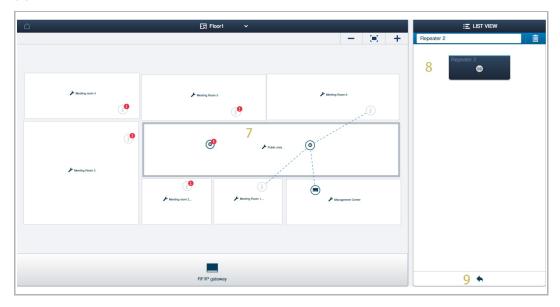
[4] Enter the serial number of the "RF Repeater" (e.g. "Repeater 2" for demo case 1).



[6] Wait for the pairing process.



- [7] No dashed line is displayed between the two devices.
- [8] No parent device is displayed on the list.
- [9] Click " < " to turn back to the floor screen.



## 10.12 Removing the devices

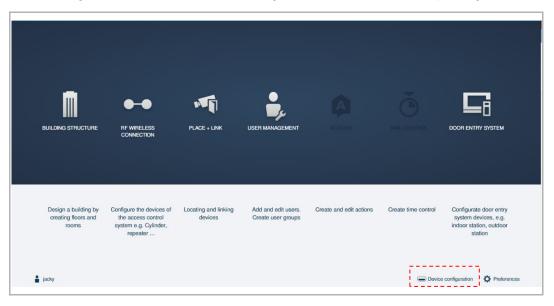


#### Note

The AccessControl device cannot be deleted if it is paired. Please unpair it first. see chapter 10.11 "Disconnecting the devices" on page 250.

#### Accessin the "Device configuration" screen

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



## 10.12.1 Removing "Electronic locking cylinders"

- [1] On the "Device configuration" screen, click "Cylinder".
- [2] Click the designated "Electronic locking cylinder" (e.g. "Cylinder 6").
- [3] Click " 🔟 ".
- [4] Click "  $\checkmark$  " to confirm.

				LIST	VIEW	
Device type		Cylinder(6)			Cylinder 6	Ŵ
SmartAP(1)	>	#201717E000000F1 Cylinder 1 Building1>Floor1>M		>	Serialnumber: 20160810000001F Short ID: ESP Software version: V1.11	3
Repeater(2)	>	Cylinder 2 Building1>Floor1>M		>	Update firmware Position	
RF/IP gateway(1)	>	#201747E000000F4 Cylinder 3 Building1>Floor1>M		>	Building Building1	•
Outdoor station(0)     Indoor station(0)	>	#201F8810000087 - Cylinder 4 Building1>Floor1>M		>	Floor Floor1	•
O- IP actuator(0)	>	#201737E000000F3 Cylinder 5 Building1>Floor1>M		>	Room Meeting room 6	×
Guard unit(0)	>	#20160810000001F Cylinder 6 Building1>Floor1>M	Ζ.	>	Channels RF connection	>
					Door opener Knob reader	>
					Office mode Emergency card	>
					Battery status	>
		+	٤		*	
				LIST	VIEW	
Device type SmartAP(1)	>	Cylinder(6) #201717E000000F1				
and Onio Da (1)				>		
- Cylindor(6)	>	Cylinder 1 Building1>Floor1>M				
Repeater(2)	> >	# Cylinder 1 Building1>Floor1>M #20121810000005E Cylinder 2 Building1>Floor1>M	(VOV)	>		
		Building1>Floor1>M #20121810000005E E Cylinder 2	(UCY) soling room 2			
Repeater(2)     RF/IP gateway(1)	>	Building1>Floor1>M #201218100000005E Cylinder 2: Building1>Floor1>M #201747E00000F4 INFORMATION	(UCY) soling room 2			ł
Repeater(2)     RF/IP gateway(1)     IP camera(1)	> > >	Building1>Floor1>M #20121810000005E Building1>Floor1>M #201747E000000F4	(UCY) soling room 2		you sure to delete?	1
Repeater(2)  RF/IP gateway(1)  IP camera(1)  Cutdoor station(0)  Indoor station(0)  IP actuator(0)	> > >	Building1>Floor1>M #201218100000005E Cylinder 2: Building1>Floor1>M #201747E00000F4 INFORMATION	(UCY) soling room 2			1
	> > >	Building 1-Floor1-5M B20121810000005 Cylinder 2 Building 1-Floor1-5M B101747E00000054 B101747E0000054 B101747E0000054 B101747E0000054 B101747E0000054 B101747E0000054 B101747E0000054 B101747E0000054 B101747E0000054 B101747E0000054 B101747E0000054 B101747E0000054 B101747E0000054 B101747E0000054 B101747E0000054 B101747E0000054 B101747E00000054 B101747E0000054 B101747E0000054 B101747E0000054 B101747E00000054 B101747E00000054 B101747E00000054 B101747E00000054 B101747E00000054 B101747E00000054 B101747E00000054 B101747E00000054 B101747E00000054 B101747E0000054 B101747E0000054 B101747E0000054 B101747E00000054 B101747E00000054 B101747E0000054 B101757E0000054 B101757E000000000000000000000000000000000	uory : veting room 2 (PLL) x x ESSP)		you sure to deleto? 4 √	1

## 10.12.2 Removing "RF Repeaters"

- [1] On the "Device configuration" screen, click "Repeater".
- [2] Click the designated "RF Repeater" (e.g. "Repeater 2").
- [3] Click " 🔟 ".
- [4] Click "  $\checkmark$  " to confirm.

Device type         Repeater(2)         Repeater 2         SenatruP(1)
Image: Singer AP(1)         Image: Several AP(2)
• Repeater(2)               • Repeater 2             Building1               • Peoplicin                 • RF/RP gateway(1)               • Building1-FRoot-3-Rubbic area               Building1               • Building1               • Building1               • Floor               Building1               • Floor
Image: Promonal (1)       >         Image: Promonal (2)
□       Indicion station(0)       >         □       Indicon station(0)       >         □       Channels       Channels         Indicon station(0)       +       Indice station(0)         Indicon station(0)       +       Indice station(0)         Indicon station(0)       +       Indice station(0)         Indice station(0)       Indice station(0)       Indice statio(0)         Indice station
Poom         Poom           Poom         Poom           Datador(0)         >           Channols         Channols           RF connection         RF connection           +            Total variety            Poom         Nationality           Poom         Nationality           Poom         Nationality           Poom         Nationality           Poom         Poom           Poom         Nationality           Poom         Poom           Poom
Image: Channels         Channels           Guard unt(0)         FF connection           FF connection         FF connection           +         S           Channels         Channels           FF connection         FF connection
Image: space of the s
LST VIEW           Device type         Repeater(2)           Im SmartAP(1)         Image: Provide the state of the stateo
LST VIEW           Device type         Repeater(2)           Im SmartAP(1)         Image: Provide the state of the stateo
Device type         Repeater(2)           Im SmarAP(1)         Image: Cylinder(5)           Image: Cylinder(5)         Building1>-Floor(>Public areat
Image: SmartAP(1)         >         #C41310100000000P(POF)         >           Image: SmartAP(1)         Properties         Building1-3Floor1>Public area         >
F Cylinder(5)     Building1>Floor1>Public area
E Cymoer(5)
#24164010000088(RBP)
Repeater 2     Repeater 2     Reference 2     Repeater 2     Repeater 2     Reful pateway(1)
IP camera(1)     INFORMATION
Cutdoor station(0)
Indoor station(0)  Are you sure to delete?
o⊷ (Pactuator(0) > X 4 ✓
Guard unit(0)

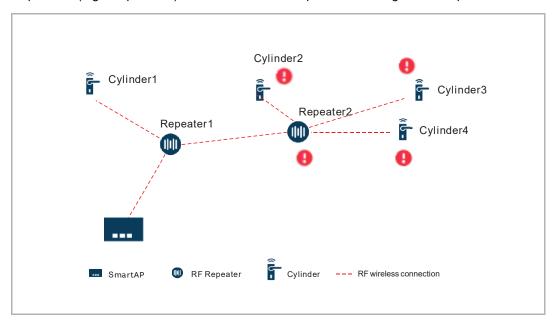
## 10.12.3 Removing "RF/IP Gateways"

- [1] On the "Device configuration" screen, click "RF/IP Gateway".
- [2] Click the designated "RF/IP Gateway".
- [3] Click " 🔟 ".
- [4] Click "  $\checkmark$  " to confirm.

	LIST	T VIEW
Device type	RF/IP gateway(1)	RF/IP gateway
Cylinder(5)	<pre>#142807A7F030B40(NDQ) RF/IP gateway </pre>	Serialnumber: 142807A7F030840 3 Storiu Dr. NOO Software version: V1.03
		RF MCU version: V1.07
Repeater(2)	>	RF module version: V1.05 Connect status: Disconnected
RF/IP gateway(1)	>	Signed status: signed
HP camera(1)	>	License Agreement for Software Update firmware
Outdoor station(0)	>	Replace device
Indoor station(0)	>	Network information
O- IP actuator(0)	>	MAC address: 80:7A:7F:03:0B:40 IP address: 192.168.1.100
Guard unit(0)	>	Subnet mask: 255-255.0 Default gateway: 192.168.1.1
Course analos		Position
		Building
		<not allocated=""></not>
		Floor
		<not allocated=""></not>
		Room
		<not allocated=""></not>
		Paramator
	o <u>£</u>	•
	1.000	T VIEW
Device type	RF/IP gateway(1)	
SmartAP(1)	#142807A7F030840(NDQ)     RF/IP gateway	
E Cylinder(5)	>	
Repeater(2)	»	
RF/IP gateway(1)	>	
🗯 IP camera(1)	INFORMATION	
Outdoor station(0)		
Indoor station(0)	> Are	you sure to delete?
O- IP actuator(0)	>	4 🗸
Guard unit(0)	×	Y

## 10.13 Replacing the damaged "RF Repeater"

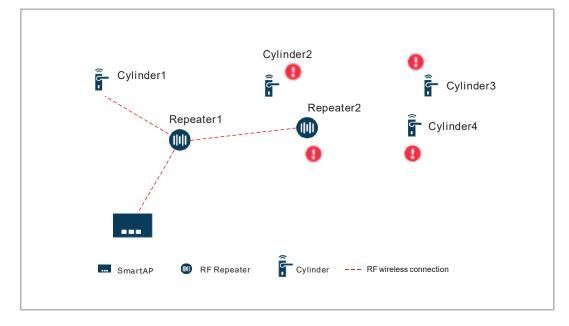
If a "RF Repeater" is damaged (e.g. "Repeater2" is damaged on the below diagram), all "RF Repeaters" and all "Electronic locking cylinders" paired to it will be offline. A new "RF Repeaters" (e.g. "Repeater3") needs to be used to replace the damaged "RF Repeaters".



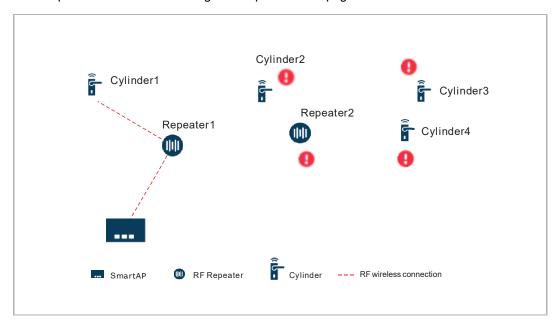
Please follow the steps below:

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

see chapter 10.11.1 "Disconnecting "Electronic locking cylinders"" on page 252



[2] Forcibly unpair the damaged "RF Repeater" from its parent device. see chapter 10.11.2 "Disconnecting "RF Repeaters"" on page 256



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

see chapter 10.12.2 "Removing "RF Repeaters"" on page 261

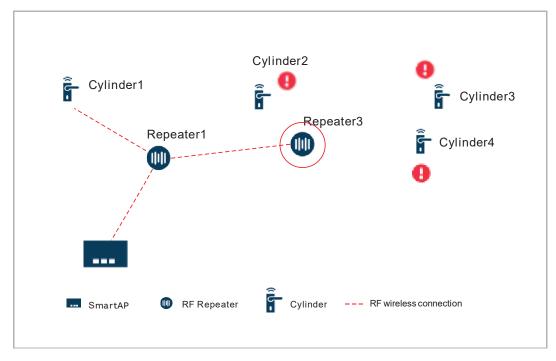
[4] Add a new "RF Repeater"

see chapter 10.3.3 "Adding and locating "RF Repeaters"" on page 192

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

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

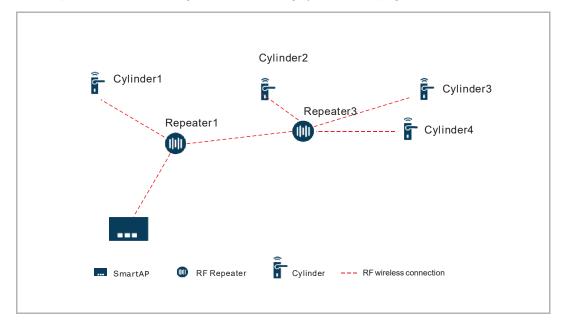
see chapter 10.4.1 "Connecting "RF Repeaters"" on page 196



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

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

see chapter 10.4.2 "Connecting "Electronic locking cylinders"" on page 198



#### 10.14 Managing the link between the devices

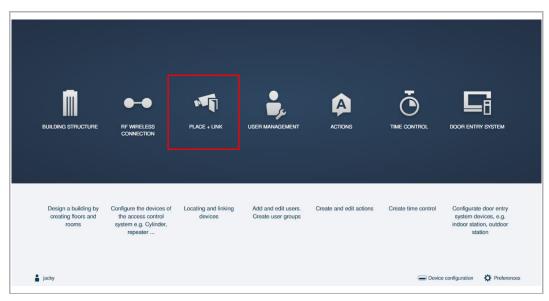
On "Smart Access Point", 2 AccessControl devices can be linked together. When one is triggered, the other can output an action.

#### Demo case

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

#### Access the floor plan screen

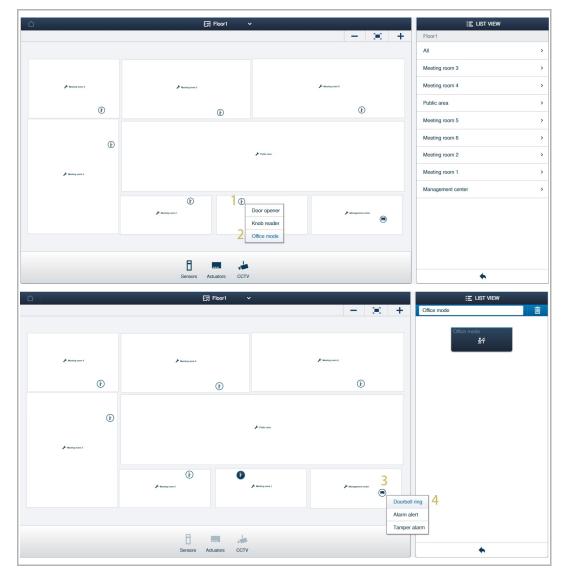
On the configuration screen, click "Place + Link", "Building 1", "Floor 1" to access the floor plan screen.



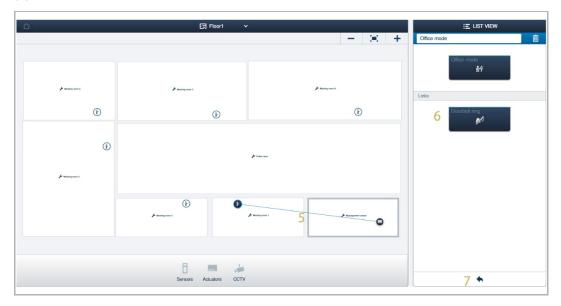
## 10.14.1 Adding the link

Following operations are based on demo case. see chapter 10.1 "AccessControl topology" on page 174.

- [1] On the floor plan screen, click the designated "Electronic locking cylinder".
- [2] Click "Office mode".
- [3] Click "Smart Access Point".
- [4] Click "Doorbell ring".

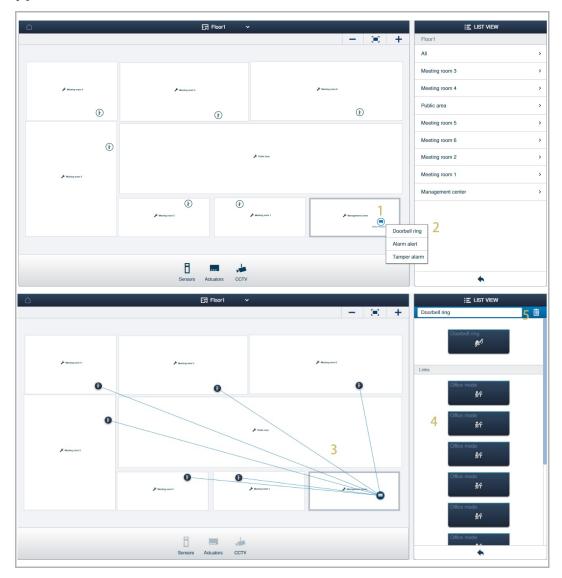


- [5] Pairing between the two devices is indicated by a line if successful.
- [6] Linked device is displayed on the list.
- [7] Click " <sup>†</sup> " to turn back to the floor screen.



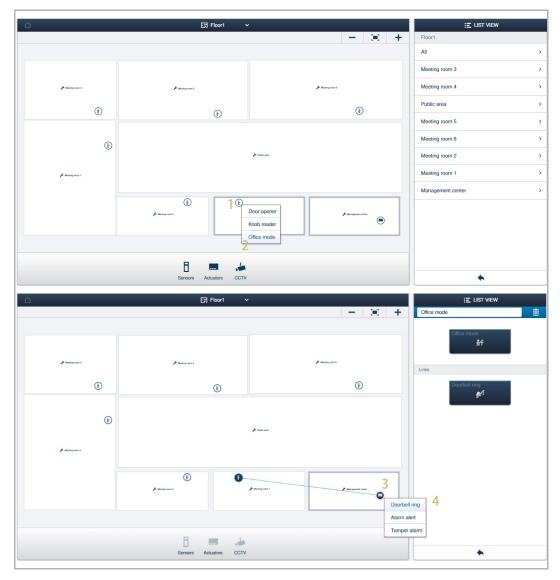
## 10.14.2 Managing the link

- [1] On the floor plan screen, click "Smart Access Point".
- [2] Click "Doorbell ring".
- [3] The links are displayed on the floor plan.
- [4] The linked devices are also displayed on the list.
- [5] The channel cannot be removed if it has more than 2 links.

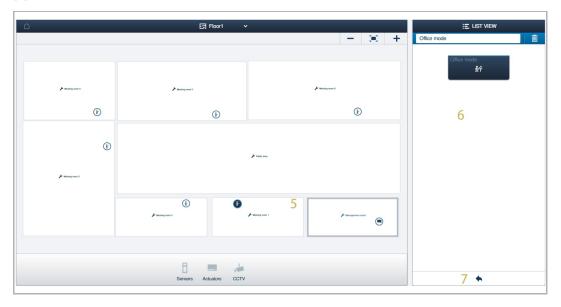


## 10.14.3 Removing the link

- [1] On the floor plan screen, click the designated "Electronic locking cylinder".
- [2] Click "Office mode".
- [3] Click "Smart Access Point".
- [4] Click "Doorbell ring".



- [5] No link is displayed between the two devices if successful.
- [6] No linked device is displayed on the list.
- [7] Click " <sup>†</sup> " to turn back to the floor screen.



# 11 Managing actions

## Access the "Action" screen

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

BUILDING STRUCTURE		PLACE + LINK	USER MANAGEMENT	ACTIONS	TIME CONTROL	DOOR ENTRY SYSTEM
Design a building by creating floors and rooms	Configure the devices of the access control system e.g. Cylinder, repeater	Locating and linking devices	Add and edit users. Create user groups	Create and edit actions	Create time control	Configurate door entry system devices, e.g. indoor station, outdoor station
🛔 jacky						e configuration 🛛 🏠 Preference

#### Demo case

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

## 11.1 Adding an action

Following operations are based on demo case.

- [1] On the "Actions" screen, click "+".
- [2] Enter the name for the action.
- [3] Click "  $\checkmark$  " to save.
- [4] On the designated action screen, click "Add precondition", followed by "Time".

	۵ A	ACTIONS			
	CREATE NEW ACTION				
	Action Action				
	New action				
	Name Cyliner 1 is offline 2				
	×	3∢			
1 +					
		Add			
	A CYLINER 1 IS OF	Add	<b>i</b> <i>F</i>		
Precondition		Add	Notification		
Precondition	@ CYLINER 1 IS OF	Add FUNE Actuator			
Select one or several preconditions which	CYLINER 1 IS OF	Add FUNE Actuator Select one or several actuators which are to	Notification		
E Contraction de la contractio	D CYLINER 1 IS OF	Add FLINE Actuator	Notification		
Select one or several preconditions which have to be met before an event can be	CYLINER 1 IS OF	Add FUNE Actuator Select one or several actuators which are to	Notification		
Select one or several preconditions which have to be met before an event can be	CYLINER 1 IS OF	Add FUNE Actuator Select one or several actuators which are to	Notification		
Select one or several preconditions which have to be met before an event can be	CYLINER 1 IS OF	Add FUNE Actuator Select one or several actuators which are to	Notification		
Select one or several preconditions which have to be met before an event can be	CYLINER 1 IS OF	Add FUNE Actuator Select one or several actuators which are to	Notification		
Select one or several preconditions which have to be met before an event can be	CYLINER 1 IS OF	Add FUNE Actuator Select one or several actuators which are to	Notification		
Select one or several preconditions which have to be met before an event can be	CYLINER 1 IS OF	Add FUNE Actuator Select one or several actuators which are to	Notification		

- [5] Click "Mon-Fri" to select the days from Monday to Friday.
- [6] Enter the start time and end time.
- [7] Click "OK" to save.

				15.9491	54-54 - 54 - 54 - 54 - 54 - 54 - 54 - 5
			CYLINER 1 IS OF		۴ ش
Time			Event	Actuator	Notification
Start	08:00	б	C.	Õ	
	17:00		Select one or several sensors which are to trigger the event.	Select one or several actuators which are to be activated during an event.	Define a notification which is to be sent when the event occurs.
Repetition on these days					
Mon	Tue	Wed			
Thu	Fri	Sat			
Sun	Mon-Eri 5	Sat/Sun			
	-				
×	<b>7</b> oi	ĸ	Add event	Add actuator	Add notification
			- <del> </del> Add	Cyliner 1 is o	

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

Actuator         Notification           Precondition         RF connection         Actuator         Notification	<i>بر</i> (10)
Image: Star: 08:00       Exe: 17:00         Exe: 17:00       Repetition on these days: Mon - Fri         Image: Online       Image: Select one or several actuators which are to be activated during an event.         Image: Online       Image: Select one or several actuators which are to be activated during an event.	sent when
Add precondition X 9 OK Add actuator Add notification	
+ Rev Add Cyliner 1 is a	

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

[11]Enter the delay time between when the actuator is activated and the event is triggered. [12]Click "OK".

	CYLINER	IS OFFLINE	<b>前</b>
Precondition	Event	Doorbell ring	Notification
Time Start: 08:00 End: 17:00 Repetition on these days: Mon - Fri	Access control Device: Cylinder 1 (201777E00000F1- SSM) Channel: RF connection Offine	During • Occurrence of the event Delay(s) - 0 + 11	Define a notification which is to be sont when the event occurs.
Add precondition	Add event	<b>×</b> 12 ок	Add notification
	Ac		

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

[14]Enter the description.

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

[16]Select "Occurrence of the event".

[17]Click "Filter".

	🖗 CYLINER 1 IS OFFLINE								
Precondition	Event	Actuator							
Time Start: 08:00 End: 17:00 Repetition on these days: Mon - Fri	Access control Device: Cylinder 1 (201717E000000F1- SSM) Charnel: IF connection Office	SmarAP Device: SmarAccess Point (105607AFP30734- RGA) Channel: Doorbell ring During: Occurrence of the event Delay: 0 s	Subject Cylinder 1 is offline 13 Message (max. 160 letters) Cylinder 1 is offline 14 Cylinder 1 is offline 14 Cylinder 1 is offline 16 Cylinder 1 is offline 16 Cylinder 1 is offline 16 Cylinder 1 is offline 16 Cylinder 1 is offline 17 Cylinder 1 is offline 16 Cylinder 17 Cylinder 17 Cylinde						
Add precondition	Add event	Add actuator	🗙 ок						
	- <del> </del> Add	Cyliner 1 is o							

[18]Click to select the users.[19]Click "OK" to save.

	CYLINER 1 IS O	FFLINE		Û	×
Precondition	Event	Actuator			Ū
Time Start: 08:00 Facebition on these days: Mon - Fri	Access control Device: Cylinder 1 (2017)77/E00000F1- SSM) Channel: RF connection Offline	SmartAP Device: Smart Access Point (105807A7F030734- RGA) Channe: Doorbell ring During: Occurrence of the event Delay: 0 s	A admin1 B basic1 C cleaner1 J jacky M master1 Filter	18	*
Add precondition	Add event	Add actuator	× 19	ок	

[20]The result is displayed on the screen.

	CYLINER 1 IS	OFFLINE	<u>ن</u> ۲
Precondition	Event	Actuator	Notification
Time       Start: 18.00       End: 17.00       Repetition on these       days: Mon - Fri	F       Access control       Device: Cylinder 1       (201717E00000F1-       SSM)       Charnet: FF connection       Office	Characteria SmartAP Device: SmartAccess Point (105807A7F030734- RGA) Charnet: Doorbell ring During: Occurrence of the event Delay: 0 s	Cylinder 1 is offline Cylinder 1 is offline admin1,jacky During: Occurrence of the event
Add precondition	Add event	Add actuator	Add notification
	+ Add	Cyliner 1 is o	

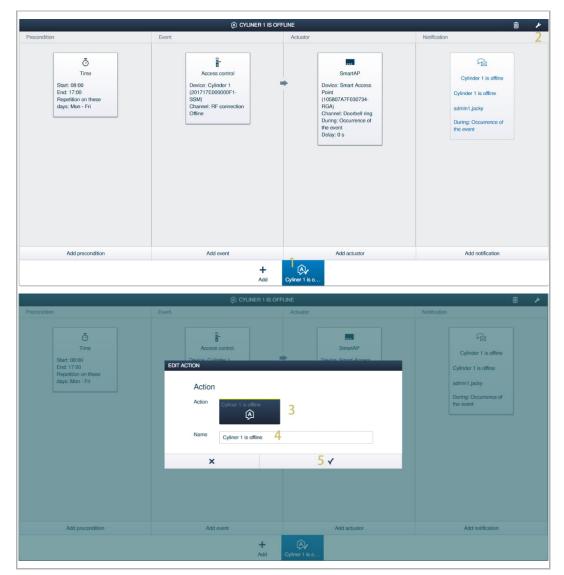
#### 11.2 Managing the action

Please follow the steps below:

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

[2] Click " 🗾 ".

- [3] Click the icon to disable or enable the action.
- [4] Rename the action.
- [5] Click " $\sqrt{}$ " to save.



## 11.3 Removing the action

Please follow the steps below:

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

[2] Click " 道 ".

[3] Click " $\sqrt{}$ " to save.

		R 1 IS OFFLINE	211 - 2
Precondition	Event	Actuator	Notification
Time           Start: 08:00           End: 17:00           Repetition on these days: Mon - Fri	Access control Device: Cylinder 1 (2017)7500000F1 SSM) INFORMATION	Device: SmartAP Device: Smart Access Point (105807A7F030734-	Cylinder 1 is offline Cylinder 1 is offline admin1 jacky During: Occurrence of the event
	×	3 √	
Add precondition	Add event	Add actuator	Add notification
		+ Cyliner 1 is o	

## 12 Cyber security

#### 12.1 Disclaimer

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

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

#### 12.2 Performance and service and network performance

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

#### D0401. "Smart Access Point" network performance

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

D0401. "Smart Access Point" Port and service

## D04031 "RF/IP Gateway" network performance

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

## D04031 "RF/IP Gateway" Port and service

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

#### 12.3 Deployment guideline

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

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

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

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

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

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

#### 12.4 Upgrading

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

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

#### 12.5 Backup/restore

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

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

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

## 12.6 Data purging

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

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

On the configuration screen, follow the steps below:

	3 🕐   🛛					
	nf wineless connection	PLACE + LINK		ACTIONS		
Design a building by creating floors and rooms	Configurate the devices of the access control system e.g. cylinders, repeaters	Locating and linking devices	Add and edit users. Create user groups	Create and edit actions	Create time control	Configurate door entr system devices, e.g indoor station, outdoo station
🛔 abb			* PREFERENCES		Device configura	tion 🌣 Preferences
Preferences	5	Service				
System information	› s	Service				
Network settings	>	Restore default setting	gs 3 This option r be lost.	esets the device to its factor	y defaults. All configuration	on data of this device w
Localization	>	Restart	Restart the S	Smart Access Point.		
Project backups	>					
Firmware updates	>					
	>					
MyBuildings						
	>					
Service 2						
MyBuildings Service 2 WI-FI access point mode Third party authority						

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

#### 12.7 Malware prevention solution

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

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

#### 12.8 Default passwords and user accounts

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

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

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

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

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

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

#### 12.9 Password rule

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

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

## 12.10 Logging

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

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

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

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

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

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

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

# 13 Appendix

## 13.1 Registering an account on the MyBuildings portal

Access the link: https://mybuildings.abb.com and click "Register". Fill in the form as required to register an account. Then activate the user account when you receive the email sent from the MyBuildings portal.

ABB Home + Offerings + Smarte	r Building + MyBuildings portal + Login	۵ ۵
	Welcome to MyBuildings portal powered by ABB Ability <sup>TM</sup>	
	Login <sup>Username</sup>	
	Username Password Password	
	Login	
	Register Sign-in help?	
Contact   Imprint   Terma of use   Privacy, provi	alons	

## 13.2 Resetting the password for the primary admin

Press and hold the reset button for 10 s.

	]	
	Res	et button
	AP 1	nodeswitch
LED		

## 1. Reset option = Without MyBuildings account

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

Please ch	ange password first!
User name	jacky
Password	
Repeat passw	

## 2. Reset option = With MyBuildings account

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

Note
------

0

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

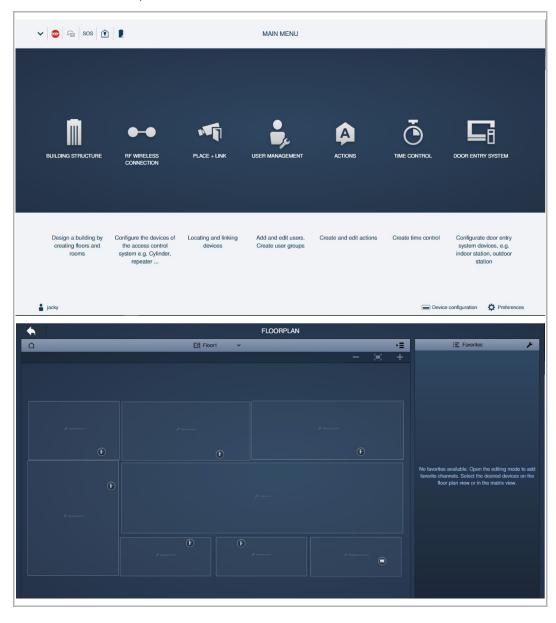
Sent 2140 For y	adf9ea2c / ivanst	tAP (cac28e69-816b agecn) A maximum of 25 e-n		be	
	Please cha	nge password	first!		
	Password				
	Repeat passw				
	Verify code	92OJJ88K			
		Finis	h		

## 13.3 User management

### 13.3.1 User roles

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

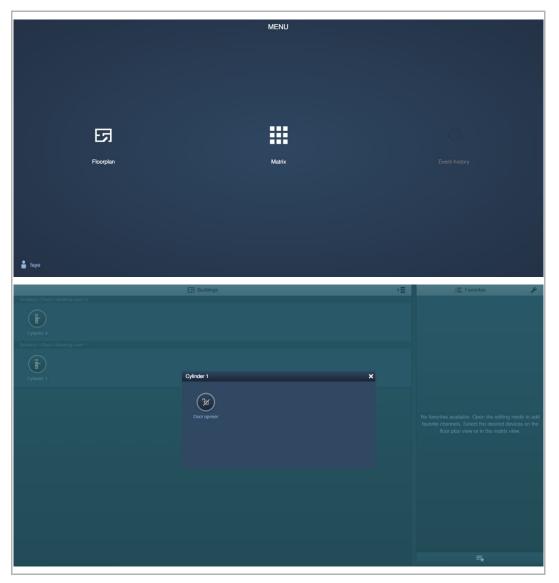
- 1. Admin users
- The primary admin user is created only during the initial setup. The other admin users can be created by the primary admin user or other admin users. see chapter 8.3 "Initial setup" on page 26.
- Admin users can manage other admin users, master users, basic users and 3rd party users.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



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

ENDERHAGE STITUKETERARE.	O-O HE WHILE LISS COMMICTION	Marce + Lank	USER MANAGEMENT	ACTIONS	Тіме сом	<b>)</b> TROL	EE Doom earliev system
Design a building by creating floors and rooms	Configure the devices of the access control system e.g. Oylinder, repeater	Locating and linking devices	Add and edit users. Create user groups	Create and edit actions	Create tim		Configurate door entry system devices, e.g. indoor station station
		E Buildings			→≡		i≘ Favorites 🖌
Building1-Floor1-Meeting room 1 Cylinder 1 Building1-Floor1-Management center Smatt Access Pon						favorite chi floc	s available. Open the editing mode to add unrelic. Select the desired devices on the r plan view or in the matrix view.

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



- 4. 3rd party users
- 3rd party users can be created by admin users and master users.
- 3rd party users can operate only the "Electronic locking cylinders" assigned to them during the specified duration.



# 13.3.2 Adding users

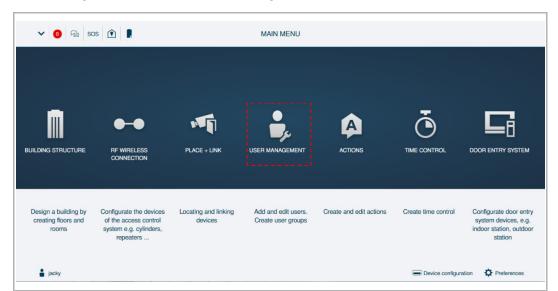


Note

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

# Accessing the "Users" screen

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



# Adding users

1. Adding admin users

Please follow the steps below:

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

USERS USERS	:E LIST VIEW
+ 1 Add scer	jaoky
Users	
Josha J jady	
Users groups	

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

- [3] Select "Admin" from the drop-down list.
- [4] Enter the password according to the password rules displayed on the screen.
- [5] Enter the password again
- [6] Click "OK" to save.

Repeat steps 1-6 to add admin users.

			USERS	E LIST VIEW
		1	ADD NEW USER	admin1
Users			New user	basic1
A	в	C	User name Admin1 2	cleaner1
admin1	basic1	cleaner1	First name	jacky
			User role Admin 3 ~	master1
			Password 4 Akada 10 d	naracters Jowercase letters special character number
			Repeat password 5	
			Users Users groups	

2. Adding master users

Please follow the steps below:

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

USERS 4	:E LIST VIEW
	Users
+ 1 Add user	jacky
Users	
jadky	
Users groups	

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

- [3] Select "Master" from the drop-down list.
- [4] Enter the password according to the password rules displayed on the screen.
- [5] Enter the password again.
- [6] Click "OK" to save.

Repeat steps 1-6 to add master users.

	USERS	:≣ LIST VIEW
		Users
	ADD NEW USER	admin1
Users	New user	basic1
A B C	User name Master1 2	cleaner1
admin1 basic1 cleaner1	First name	jacky
	User role Master 3	master1
	Password ··· 4	
	Repeat password 5	
	× 6 √	

3. Adding basic users

Please follow the steps below:

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

USERS 4	:E LIST VIEW
	Users
+ 1 Add user	jacky
Users	
jadky	
Users groups	

[2] Enter the username, this username cannot be the same as the existing username.

- [3] Select "Basic" from the drop-down list.
- [4] Enter the password according to the password rules displayed on the screen.
- [5] Enter the password again.
- [6] Click "OK" to save.

Repeat steps 1-6 to add basic users.

		USERS	:≡ LIST VIEW
		ADD NEW USER	admin1
Users		New user	basic1
AB	C	User name Basic1 2	cleaner1
admin1 basic1		First name	jacky
		User role Basic 3 ~	master1
		Password ··· 4	
		Repeat password 5	
		× 6 √	
		Users groups	

4. Adding 3rd users

Please follow the steps below:

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

USERS	:≡ LIST VIEW
	Users
+ 1 Add user	jacky
Users	
o jody	
Users Users groups	
	3

- [2] Enter the username, this username cannot be the same as the existing username.
- [3] Select "3rd party" from the drop-down list.
- [4] Enter the password according to the password rules displayed on the screen.
- [5] Enter the password again.
- [6] Select "Limited validity" from the drop-down list.
- [7] Set the start date via clicking " 31 ".
- [8] Set the end date via clicking " 3 ".
- [9] Click "OK" to save.

Repeat steps 1-9 to add 3rd party users.

								i≡ LIST VIEW
			+					admin1
			ADD NEW USER					admin
			User name	Cleaner1 2				
Users								basic1
			First name					
A		C	Last name					cleaner1
admin1	basic1	cleaner1		3rd party 3		~		
aumin		Cleatier (	User role	3rd party 3		~		jacky
			Password	- 4		1	×At least 10 chara y/Uppercase to low ×At least one spec	acters wercase letters
			Repeat password	E			×At least one spec ×At least one num	chi character iber
			Repeat password	)				
			Validity period	Limited validity	6	~		
				A		7		
			Start	Aug 1, 2020		7 🖽		
			End	Aug 1, 2020		8 🛙		
			×		9√	0		
			×		9 4	_	_	
			_					
				ers groups				

# 13.3.3 Adding user groups

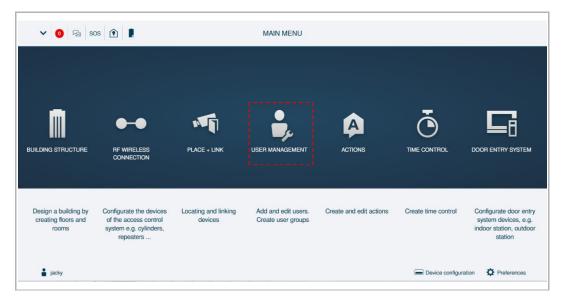
(	С	)	
_			

#### Note

User group is a collection of the users. All the users in the group have the same permission for the devices. All the users in the group change permissions automatically when some permissions are changed.

# Accessing the "User groups" screen

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



🐸 USERS GROUPS	:E LIST VIEW
+ Add user group	
Users groups	
Users Users groups	

On the "Users" screen, click "User groups" to access the "User groups" screen.

# Adding user groups

Please follow the steps below:

- [1] On the "User groups", click "Add user group".
- [2] Enter the group name.
- [3] Select a group icon from the drop-down list.
- [4] Click "  $\checkmark$  " to save.

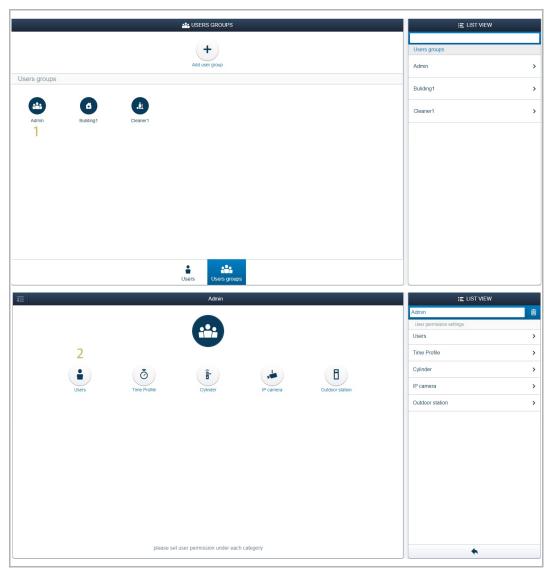
Repeat steps from 1-4 to add user groups.

🎎 USERS GROUPS	:E LIST VIEW
+ 1 Add uner grup	
Add new user group          New user group         Group name       Admin 2         Group icon       3         X       4	
Users Users	

# 13.3.4 Assigning the users to a user group

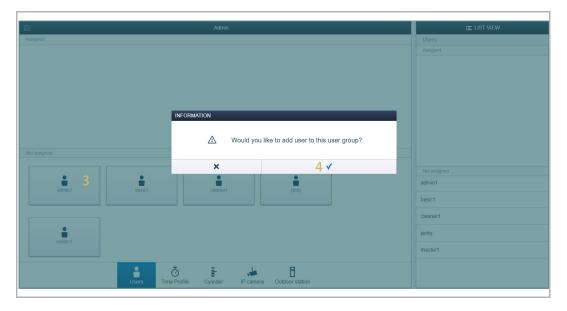
Please follow the steps below:

- [1] On the "User groups" screen, click a user group.
- [2] Click "Users".



- [3] On the designated user group screen, click the designated user on the "Not assigned" section.
- [4] Click "  $\checkmark$  " to confirm.

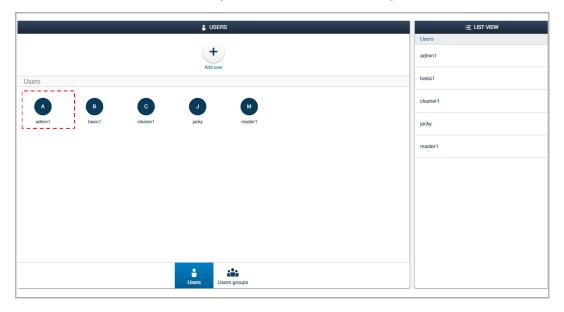
Repeat steps 3-4 to assign the designated users to a user group.



# 13.3.5 Configuring a user

# Accessing the designated user screen

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



1. View the user role

On the designated user screen, the user role can be viewed on the screen.

_			ıdmin1			:= LIST VIEW	
Ξ		ł	iomin 1			<u>:</u> LISI VIEW admin1	Ū
		A				User role: Admin Device sharing Email address	
***	â		đ		B	Invitation code :	
Users groups(1)	ID authentication(1)	Pairing devices	Cylinder	IP camera	Outdoor station	User information	
						Personal data	>
						Change password	>
						User permission settings	
						Users groups(1)	>
						ID authentication(1)	>
						Pairing devices	>
						Cylinder	>
						IP camera	>
						Outdoor station	>
·		please set user permissi	on under each category			•	

2. Changing the user name

On the designated user screen, follow the steps below:

- [1] Click "Personal data".
- [2] Enter the first name and the last name.
- [3] Click "  $\checkmark$  " to save.

Ξ	admin1	;≘ LIST VIEW
		admin1
	A	User role: Admin
	-	Email address
	Personal data	Invitation code :
l i i i i i i i i i i i i i i i i i i i		Invite
Users groups(1) ID authentication(1)	Personal data	User information
	First name 2	Personal data >
		Change password >
	Last name	User permission settings
	× 3 v	Users groups(1)
	^ <b>J</b> Y	ID authentication(1)
		Pairing devices >
		Cylinder >
		IP camera >
		Outdoor station >
	please set user permission under each category	•

3. Changing the password

On the designated user screen, follow the steps below:

- [1] Click "Change password".
- [2] Enter the password twice according to the password rule displayed on the screen.
- [3] Click "  $\checkmark$  " to save.

admint admint	:Ξ LIST VIEW	
A	User role: Admin	
	Device sharing	
	Emuil address	
	Invitation code :	
	Invite	
Users groups(1) ID authentication(1) Pairing devices uldoor station	User information	
New password News understeen where we have a set of the	Personal data	>
Repeat password	Change password	>
	User permission settings	
× 3 🗸	Users groups(1)	>
	ID authentication(1)	>
	Pairing devices	>
	Cylinder	>
	IP camera	>
	Outdoor station	>
please set user permission under each category	*	

4. Changing the validity period



**Note** It is only applicable to 3rd party user.

On the designated user screen, follow the steps below:

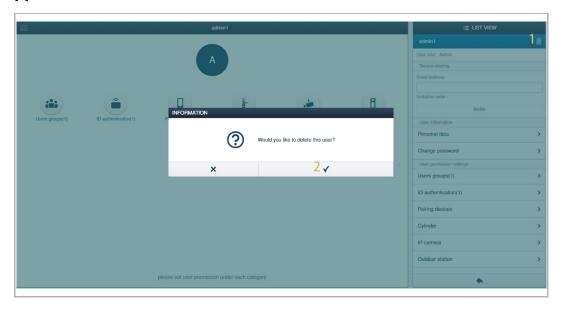
- [1] Click "Validity period".
- [2] Select "Limited validity" from the drop-down list.
- [3] Set the start date via clicking " 3 ".
- [4] Set the end date via clicking " 3 ".
- [5] Click "OK" to save.

TE .	cleaner1		:≡ LIST VIEW	
1			cleaner1	
			User role: 3rd party	
	С			
			Email address	
	Validity period		Invitation code :	
	Validity period		Invite	
Users groups ID authentication			*Please connect to MyBuildings	
	Validity period Limited valid			
	Start Aug 4, 2020	3 🖬	Personal data	>
	End Aug 4, 2020	<mark>4</mark> භ	Change password	>
		4	Validity period	×
	×	5 √	Usor permission settings	
			Users groups	>
			ID authentication	>
			Pairing devices	>
			Time Profile	>
			Cylinder	>
	please set user permission under each	category	•	

5. Removing a user

On the designated user screen, follow the steps below:

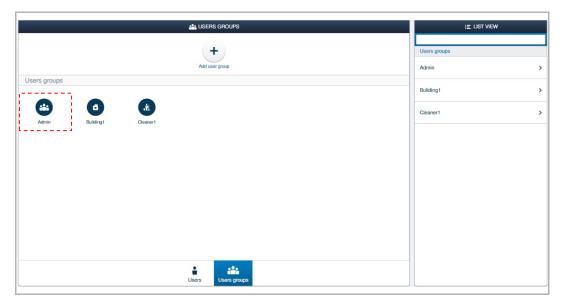
- [2] Click "  $\checkmark$  " to save.



# 13.3.6 Configuring a user group

# Accessing the designated group screen

On the "User groups" screen, click the designated group to access the designated group screen.



1. Changing the group name

On the designated group screen, click the group name and enter a new one.

4E			Admin			:≡ LIST VIEW	
						Admin	Ĩ
						User permission settings Users(2)	>
						Time Profile	>
		ō			Β	Cylinder	>
	Users(2)	Time Profile	Cylinder	IP camera	Outdoor station	IP camera	>
						Outdoor station	>
		please set	user permission under eac	h category		•	

# 13.4 Updating the firmware

## 13.4.1 Updating the firmware for "Smart Access Point"

1. Updating the firmware via local PC

Please follow the steps below:

- [1] On the "Preference" screen, click "Firmware updates".
- [2] Tick the check box "Automatic download of firmware update". "Smart Access Point" will download the latest firmware from the website automatically.
- [3] The latest firmware version is displayed here. Tick the designated check box.
- [4] Click "Install firmware".

Preferences	Firmware updates
System information	FIRMWARE UPDATES
Network settings	Here you specify whether the Smart Access Point is to download new updates automatically. Or you can search on the website for updates yourself and then download them.
Localization	Automatic download of firmware updates 2
Project backups	Transmit firmware to device
Firmware updates	New firmware available
MyBuildings Account	3
Service	install firmware 4
Wi-Fi access point mode settings	
Third party authority	>
Abnormal devices	·
Misc settings	>
	<b>*</b>

 $\hat{\mathbb{T}}$ 

#### Note

"Smart Access Point" can only be updated to newer firmware.

2. Updating the firmware via website

Please follow the steps below:

- [1] On the "Device configuration" screen, click "SmartAP".
- [2] Click "Smart Access Point".
- [3] Click "Update firmware".

LIST VIEW					
Device type		SmartAP(1)	Smart Access Point		
SmartAP(1)         1           i         Cylinder(1)           i         Repeater(0)           I         RF/IP gateway(0)           ,         IP camera(0)	> > > >	#105807A7F030734(RGA) ■ Sranaf Access Point Building15Floot1sLiving room	Smart Access From: Serialnumber: 105807AF7030734 Stort ID: RGS Software version: V5.21 MCU version: V1.07 RF MCU version: V1.07 RF module version: V1.05 Update firmware Position		
Outdoor station(2)     Indoor station(2)     Or IP actuator(1)	> > >		Building1 × Floor Floor1 ×		
Guard unit(1)	>		Room Living room  Channels Doorboll ring Alarm alert Binary input Binary output Tamper alarm		
			*		



# Note

"Smart Access Point" can only be updated to newer firmware.

# 13.4.2 Updating the firmware for Door Entry System devices

1. Updating the devices one by one

Please follow the steps below:

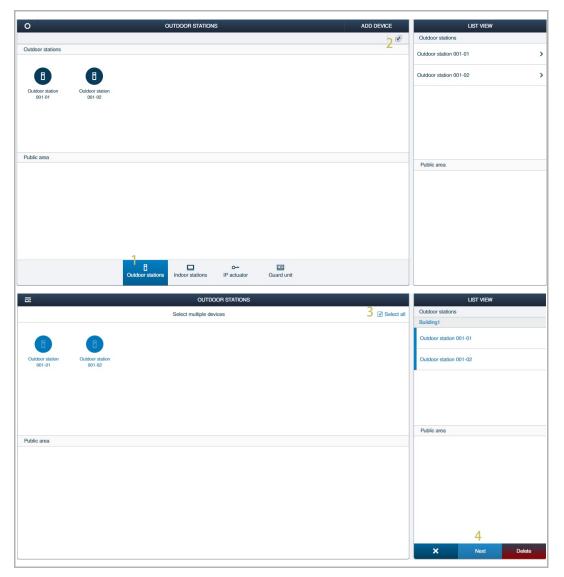
- [1] On the "Device configuration" screen, click a Door Entry System device (e.g. "Indoor station").
- [2] Click the designated Door Entry System device (e.g. "Indoor station 001").
- [3] Click "Update firmware".

		LIS	VIEW
Device type		Indoor station(2)	IS 001-0101-01
SumrAP(1)  Cylinder(1)  Repeater(0)  RF/IP gateway(0)  IP camera(0)  Cutdoor station(2)  Indoor station(2)	> > > > > >		IS 00-307-50 Seriauruber 102807A7F02F605 Short ID: XEH Software version: HG16 Main: V9.99.20190711_PP_JMX6 Update firmware 3 Parameter Block No.
Indoor station(2)	>		Hoon No.
		+	♠

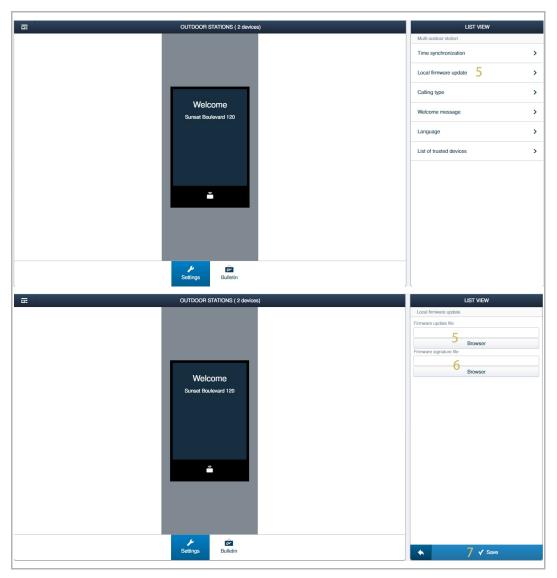
2. Updating the same types of devices in batches

Please follow the steps below:

- On the "Device configuration" screen, click a Door Entry System device (e.g. "Outdoor station").
- [2] Click " 🗹 ".
- [3] Click "Select all" to select all devices or click the designated device one by one to select multiple devices.
- [4] Click "Next".



- [5] Click "Local firmware update".
- [6] Upload the firmware.
- [7] Upload the signature.
- [8] Click "  $\checkmark$  " to save.



3. Updating the different types of devices in batche

Please follow the steps below:

- [1] On the configuration screen, click "  $\clubsuit$  ".
- [2] The devices to be updated are displayed on the screen.
- [3] Click "Update all" to update all the devices in batches.

♥ <b>①</b> ि⊴ sos ♠	<b>₽</b>			MAIN MENU			
BUILDING STRUCTURE		Online firmware update Device ID Geref ant #1 Biol 94 00-01	Current versio	n 2	New version 1.33 1.45	5 Xontrol	DOOR ENTRY SYSTEM
Design a building by creating floors and rooms	Configure the o the access system e.g. ( repeater		e all		Ask me next time	time control	Configurate door entry system devices, e.g. indoor station, outdoor station
🚆 jacky						Device	configuration Preferences



## Note

Only the Door Entry System devices which are placed on the public areas (e.g. Guard unit, building IPA, network IPA etc.) can be updated via this method.

# 13.4.3 Updating the firmware for AccessControl devices

1. Updating the firmware via local PC

Please follow the steps below:

- [1] On the "Device configuration" screen, click an AccessControl device (e.g. "Cylinder").
- [2] Click the designated AccessControl device (e.g. "Cylinder2").

[3] Click " 🖆 ".

- [4] Click "Upload local firmware".
- [5] Browse your PC to select the firmware.

[6] Click "√".

LIST VIEW					
Device type	Cylinder(1)	Cylinder 2			
SmartAP(1)	E Cylinder 2 Southarts-Elving room	Serialnumber: 20121810000005E Short ID: UOY			
Ē Cylinder(1) >		Software version: V1.11			
Repeater(0)		Update firmware Position			
RF/IP gateway(0)		Building			
JP camera(0)	FIRMWARE UPDATE	× .			
Outdoor station(2)	4 • Upload local firmware O Downlo				
Indoor station(2)		Browser 💙			
O→ IP actuator(1) >					
Guard unit(1)	×	6 √			
		RF connection >			
		Door opener >			
		Knob reader >			
		Office mode >			
		Emergency card			
		Battery status >			
	+ 3 🛃	*			

2. Updating the firmware via website

Please follow the steps below:

- [1] On the "Device configuration" screen, click an AccessControl device (e.g. "Cylinder").
- [2] Click the designated AccessControl device (e.g. "Cylinder2").
- [3] Click "Update firmware".

	LIST VIEW							
Device type	Cylinder(1)	Cylinder 2						
Image: SmartAP(1)         >           Image: SmartAP(1)         >	so i ra i noovoose (u/Y) Cylinder 2 Building 15 Floor 15 Living noon 2	Sorialsumbre: 20121 81 0000005E Sorialsumbre: 20121 81 000005E Sorialsumbre: 20121 81 000005E Building Building Building Building Building Building Building Building Building Building Floor Floor Floor Floor Floor Floor Floor Floor Floor Floor Floor Channels RF connection Sor opener Sor op						
	+ 🛃	•						

# 13.5 Managing the backup

#### Overview of the backup

The following information will be stored in the backup:

- Device settings, user settings, building structure, place & link, message & logs.
- RF connections of the AccessControl devices.
- RF connections of "RF/IP Gateways".
- Certificates.



## Attention!

A project backup is very important and necessary for the AccessControl devices. If no backup is created in advance, all the AccessControl devices will be invalid when current "Smart Access Point" is broken. These AccessControl devices can't be used by a new "Smart Access Point" directly without a backup. You have to send these devices back to the factory to repair.

### Access the backup screen

On the configuration screen, click ""Preferences", followed by "Project backups" to access the backup screen.

There are some auto-saved backups displayed in the list.

		🔅 PREFI	RENCES	
Preferences		Project backups	Auto backuped, at 2020-07-30 16:35:47.	一直
System information	>	Create new project backup +	Date	2020-07-30 16:35:48
Network settings	>	Import project backup	Author	Automatic backup
Localization	>	Auto backuped, at 2020-07-30 16:35:47. Router firmware ID: 0149. Router firmware ver >		Router firmware ID: 0149, Router firmware version: 0107, Node Firmware Id: 0143, Node Firmware Version: 0105, Manufacture Date: 12060F, MAC: 000000
Project backups	>	2020-07-30 16:35:48		deviceid: 2413101000000DD, parentid: deviceid: 241640100000088, parentid: 2413101000000DD deviceid: 201717E000000FL, parentid: 2413101000000DD
Firmware updates	>	Auto backuped, at 2020-07-30 16:35:07. Router firmware ID: 0149, Router firmware ver > 2020-07-30 16:35:07		deviced: 2015081000005F, parentid: 24131000000DD deviced: 2012181000005F, parentid: 24164010000088 deviced: 2017#E00000FH, parentid: 24164010000088 deviced: 2017#E00000FH, parentid: 24164010000088 deviced: 2017#E00000FH, parentid: 24164010000088
MyBuildings Account	>	Auto backuped, at 2020-07-30 16:26:11.		base64 param:
Service	>	Router firmware ID. 0149, Router firmware ver > 2020-07-30 16:26:12		Restore project backup
Wi-Fi access point mode settings	>	Auto backuped, at 2020-07-30 16:23:56. Router firmware ID: 0149, Router firmware ver >		The password is used to encrypt the project backup file. You need to enter this password when importing thebackup. Please keep it safe.
Third party authority	>	2020-07-30 16:23:57	Password	
Abnormal devices	>	Auto backuped, at 2020-07-30 16:22:40. Router firmware ID: 0149, Router firmware ver >		
Onvif IPC list	>	2020-07-30 16:22:40		Export
Misc settings	>	Auto backuped, at 2020-07-30 16:22:31. Router firmware ID: 0149, Router firmware ver > 2020-07-30 16:22:31		
		Auto backuped, at 2020-07-30 16:21:40.		
		*		<b>•</b>

# 13.5.1 Creating the backup

Please follow the steps below to create a backup and save it on the current "Smart Access Point":

- [1] On the backup screen, click " + ".
- [2] Enter the name.
- [3] Enter the description.
- [4] Click "  $\checkmark$  " to save.

Preferences	Project backups	Backup for the AccessControl devides - 20200801	2				
System information	Create new project backup	Description		Backup for the AccessControl devides 1. Creating a building - Done 2. Adding and locating the devices - Done			
Network settings	> Import project backup		3	3. Connecting the devices - Done 4. Adding users and user groups - Done 5. Assigning the users to the user groups - Done 6. Assigning the permission to users - Done			
Localization	Auto backuped, at 2020-07-30 16:35:47. Router firmware ID: 0149, Router firmware ver >			<ol> <li>Assigning the permission to user groups - Done</li> <li>Configuring the devices - Done</li> <li>Controlling the devices via "Smart Access Poin" - Done</li> </ol>			
Project backups	> 2020-07-30 16:35:48			10. Controlling the devices via Welcom App - Done			
Firmware updates	Auto backuped, at 2020-07-30 16:35:07.   Router firmware ID: 0149, Router firmware ver > 2020-07-30 16:35:07						
MyBuildings Account	Auto backuped, at 2020-07-30 16:26:11.						
Service	Router firmware ID: 0149, Router firmware ver >     2020-07-30 16:26:12						
Wi-Fi access point mode settings	Auto backuped, at 2020-07-30 16:23:56. Router firmware ID: 0149, Router firmware ver >						
Third party authority	> 2020-07-30 16:23:57						
Abnormal devices	Auto backuped, at 2020-07-30 16:22:40. Router firmware ID: 0149, Router firmware ver > 2020-07-30 16:22:40						
Onvif IPC list	Auto backuped, at 2020-07-30 16:22:31.						
Misc settings	Router firmware ID: 0149, Router firmware ver >     2020-07-30 16:22:31						
	Auto backuped, at 2020-07-30 16:21:40.			A			
	<b>*</b>	×		4 ✓ Save			



# Attention!

The backup is saved to the current "Smart Access Point". It is recommended to export the backup to PC in case the current "Smart Access Point" is broken.

# 13.5.2 Restoring the backup

Please follow the steps below to restore a backup from the current "Smart Access Point":

- [1] On the backup screen, click the designated backup.
- [2] Click "Restore project backup".

		🗘 PREF	ERENCES	
Preferences		Project backups	Backup for the AccessControl devides - 20200801	Ū
System information	>	Create new project backup +	Date	2020-08-01 16:34:37
Network settings	>	Import project backup	Author	jacky
Localization	>	Backup for the AccessControl devides - 20200801 Backup for the AccessControl devides 1. Creat >	Description	Backup for the AccessControl devides 1. Creating a building - Done 2. Adding and locating the devices - Done 3. Connecting the devices - Done
Project backups	>	2020-08-01 16:34:37		<ol> <li>Adding users and user groups - Done</li> <li>Assigning the users to the user groups - Done</li> <li>Assigning the permission to users - Done</li> </ol>
Firmware updates	>	Auto backuped, at 2020-07-30 16:35:47. Router firmware ID: 0149, Router firmware ver > 2020-07-30 16:35:48	7. Assigning the permission to user groups - Done 8. Configuring the devices - Done 9. Controlling the devices via 'Smart Access Poin' - Done 10. Controlling the devices via Welcom App - Done	
MyBuildings Account	>	Auto backuped, at 2020-07-30 16:35:07.		
Service	>	Router firmware ID: 0149, Router firmware ver > 2020-07-30 16:35:07		2 Restore project backup
Wi-Fi access point mode settings	>	Auto backuped, at 2020-07-30 16:25:11. Router firmware ID: 0149, Router firmware ver >		The password is used to encrypt the project backup file. You need to enter this password when importing thebackup. Please keep it safe.
Third party authority	>	2020-07-30 16:26:12	Password	
Abnormal devices	>	Auto backuped, at 2020-07-30 16:23:56. Router firmware ID: 0149, Router firmware ver >		Export
Onvif IPC list	>	2020-07-30 16:23:57		Export
Misc settings	>	Auto backuped, at 2020-07-30 16:22:40. Router firmware ID: 0149, Router firmware ver > 2020-07-30 16:22:40		
	Auto backuped, at 2020-07-30 16-22-31.			
		4		<b>h</b>

## 13.5.3 Removing the backup

Please follow the steps below to remove a backup from the current "Smart Access Point":

[1] On the backup screen, click the designated backup.

[2] Click " 🔟 ".

[3] Click " $\sqrt{}$ " to confirm.

	🗘 PRI	FERENCES				
Preferences	Project backups	Backup for the AccessControl devides - 20200801	2 🖻			
System Information	Create new project backup	Date	2020-08-01 16:34:37			
Network settings	> Import project backup		Jacky Backup for the AccessControl devides			
Localization	Backup for the AccessControl devides - 20200801     Backup for the AccessControl devides 1, Creat >	ackup for the AccessControl de ides 1. Creat >				
Project backups	2020-08-01 16:34:37 INFORMATION		<ol> <li>Adding users and user groups - Done</li> <li>Assigning the users to the user groups - Done</li> <li>Assigning the permission to users - Done</li> <li>Assigning the permission to users - Done</li> </ol>			
Firmware updates	Aut Ro.		B. Configuring the devices - Done 9. Controlling the devices via "Smart Access Poin" - Done 10. Controlling the devices via Welcom App - Done			
MyBuildings Account	Autr     Autr     Autr	C? The current project backup will be permanently deleted. Do you want to continue?				
Service	> Rou 2021	2.1	Restore project backup			
Wi-Fi access point mode settings	Auto backuped, at 2020-07-30 16:26:11 Router firmware ID: 0149, Router firmware ver >	3 √	The password is used to encrypt the project backup file. You need to enter this password when importing thebackup. Please keep it safe.			
Third party authority	2020-07-30 16:26:12	Password				
Abnormal devices	Auto backuped, at 2020-07-30 16:23:56     Router firmware ID: 0149, Router firmware ver >     2020-07-30 16:23:57					
Onvit IPC list	2020-07-30 16:23:57     Auto backwood, at 2020-07-30 16:22:40.					
Misc settings	Auto backupad, al 2020-07-30 15/22-40.     Router firmware ID: 0149, Router firmware ver >     2020-07-30 16/22:40					
	Auto backuped, at 2020-07-30 16:22-31.					
			•			

# 13.5.4 Exporting the backup

Please follow the steps below to export a backup from the current "Smart Access Point" to PC:

- [1] On the backup screen, click the designated backup.
- [2] Enter a recovery password according the password rule. The recovery password is used to import the backup from PC.
- [3] Click "Export" to export the backup to PC.
- [4] Right click the backup file.
- [5] Click "Show in folder".
- [6] The backup is displayed in the folder.
- [7] Rename the backup.

	Ö Pi	REFERENCES								
Preferences	Project backups	Backup f	or the AccessControl devic	des - 20200801				-	ī	ĩĩ
System information >	Create new project backup	- Date				2020-08-01 16	34:37			
Network settings >		Author				jacky				
Localization >	Backup for the AccessControl devides - 20200801	Descripti	Description			Backup for the AccessControl devides 1. Creating a building - Done 2. Adding and locating the devices - Done				
Project backups >	Backup for the AccessControl devides 1. Creat > 2020-08-01 16:34:37					<ol> <li>Connecting the devices - Done</li> <li>Adding users and user groups - Done</li> <li>Assigning the users to the user groups - Done</li> <li>Assigning the permission to users - Done</li> </ol>				
Firmware updates >	Auto backuped, at 2020-07-30 16:35:47. Router firmware ID: 0149, Router firmware ver 2020-07-30 16:35:48	> •				8. Configuring the dev 9. Controlling the dev	ission to user groups - Dor vices - Done lices via "Smart Access Poir vices via Welcom App - Do	1" - Done		
MyBuildings Account	Auto backuped, at 2020-07-30 16:35:07.									
Service >	Router firmware ID: 0149, Router firmware ver 2020-07-30 16:35:07	>					estore project back			
Wi-Fi access point mode settings	Auto backuped, at 2020-07-30 16:26:11. Router firmware ID: 0149, Router firmware ver	>				The password is used to encrypt the project backup file. You need to enter this passwor when importing thebackup. Please keep it		ord		
Third party authority >	2020-07-30 16:26:12	Passwor	d		2					٦
Abnormal devices >	Auto backuped, at 2020-07-30 16:23:56. Router firmware ID: 0149, Router firmware ver 2020-07-30 16:23:57	»."			3		Export			1
Onvif IPC list >	Auto backuped, at 2020-07-30 16:22:40.	1								-1
Misc settings Open  Always open files of this type	Router firmware ID: 0149, Router firmware ver 2020-07-30 16:22:40	` <u>L</u>								-1
Show in folder	-				٠					
4 Cancel 5								5	Show all	×
🕹 🛛 🖡 💌 Downloads								-	σ	×
File Home Share View										^ 🕜
Pin to Quick Copy Pasts Access Copbeard Cip		one Hection								
← → ∨ ↑ ♥ > This PC > System (C;) > Users >							✓ Ů Search Down	nloads		P
^ Name	^		Date modified	Туре	Size					
projectba	ackup.bin		2020/8/1 16:36	BIN File		66 KB				
6										
A factor of										
									٥	× ~ 0
🖈 🖻 🗎 🕹 Cut 🛛 💊 🔍 🖷	New item *									
Pin to Quick Copy Paste access Paste shortcut to	folder 👻 🍓 History 🔐 Invert s	election								
Clipboard Organize	New Open Sele	t					a da Canada Dana			0
← → ∨ ↑ ↓ > This PC > System (C) > Users >	> Lownloads		Data sector of		e		✓ Ů Search Down	10.805		٩
			Date modified	Туре	Size	66 MB				
Backup f	for the AccessControl devides - 20200801.bin		2020/8/1 16:36	BIN File		66 KB				
distant and the second se										

# 13.5.5 Importing the backup

Please follow the steps below to import a backup from PC:

- [1] On the backup screen, click "<sup>1</sup>.
- [2] Click "Upload backup", select the backup from your PC.
- [3] Enter the recovery password. see chapter 13.5.4 "Exporting the backup" on page 321.
- [4] Click "√".
- [5] The backup is displayed in the list.

		🌣 PREFE	ERENCES
Preferences		Project backups	Import project backup
System information	>	Create new project backup	Here you can import a project backup.
Network settings	>	Import project backup 1	Input the password when you export the project backup.
Localization	>	Backup for the AccessControl devides - 20200801 Backup for the AccessControl devides 1. Creat >	Password 3
Project backups	>	2020-08-01 16:34:37 5	C:\fakepath\Backup for t
Firmware updates	>	Auto backuped, at 2020-07-30 16:35:47. Router firmware ID: 0149, Router firmware ver > 2020-07-30 16:35:48	
MyBuildings Account	>	Auto backuped, at 2020-07-30 16:35:07.	
Service	>	Router firmware ID: 0149, Router firmware ver > 2020-07-30 16:35:07	
Wi-Fi access point mode settings	>	Auto backuped, at 2020-07-30 16:26:11. Router firmware ID: 0149, Router firmware ver >	
Third party authority	>	2020-07-30 16:26:12	
Abnormal devices	>	Auto backuped, at 2020-07-30 16:23:56. Router firmware ID: 0149, Router firmware ver > 2020-07-30 16:23:57	
Onvif IPC list	>	Auto backuped, at 2020-07-30 16:22:40.	
Misc settings	>	Router firmware ID: 0149, Router firmware ver > 2020-07-30 16:22:40	
		Auto backuped, at 2020-07-30 16:22:31.	× 4 v



## Note

You need to continue the "Resorting a backup" operation for the imported file to take effect. see chapter 13.5.2 "Restoring the backup" on page 319.

# 13.6 Restoring to factory default

## **13.6.1** Restoring the AccessControl devices

You can reset the building If you want to reset all the AccessControl devices.



Attention!

You need to create a backup for the AccessControl devices before reset the building. see chapter 13.5.1 "Creating the backup" on page 318. You need to disconnect all the AccessControl devices before resetting the building. see chapter 10.11 "Disconnecting the devices" on page 250.

Please follow the steps below:

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

BUILDING STRUCTURE	RF WIRELESS CONNECTION	PLACE + LINK	USER MANAGEMENT	KATENE	THE CONTROL	DOOR ENTRY SYSTEM
Design a building by creating floors and rooms	Configure the devices of the access control system e.g. Cylinder, repeater	Locating and linking devices	Add and edit users. Create user groups	Create and edit actions	Create time control	Configurate door entry system devices, e.g. indoor station, outdoor station
🛔 jacky					( Device	configuration

- [2] On the "Preference" screen, click "Service".
- [3] Click "Restore default settings".
- [4] Tick the check box "Reset the project planning to the factory settings".
- [5] Tick the check box "I have stored ...".
- [6] Click " $\sqrt{}$ " to confirm.

Preferences	Service				
System information >	Service 3				
Network settings >	Restore default settings This option resets the device to its factory defaults. All configuration data of this device will be lost.				
Localization >	DELETE PROJECT PLANNING				
Project backups					
Firmware updates >	Reset remote control     Delete user data and settings				
MyBuildings Account	Factory settings				
Service 2	5 ☑ I have stored a current backup on my computer and know that this action will				
Wi-Fi access point mode settings	delete the configuration.				
Third party authority >	× 6 <				
Abnormal devices >					
Onvif IPC list					
Misc settings >					
	*				

## 13.6.2 Accessing "Smart Access Point" remotely

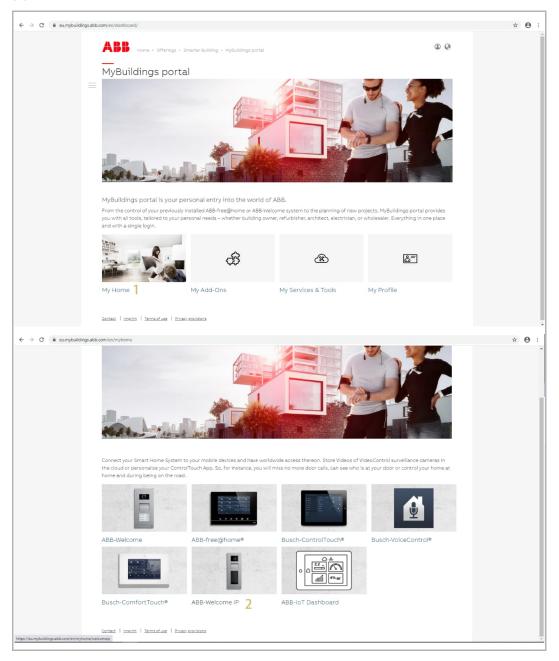
1. Enable the "Remote access" function

- [1] On the "Preference" screen, click "MyBuildings Account".
- [2] Click "Connection".
- [3] Tick the check box "Remote access".

	🌣 PREFE	RENCES			
Preferences	MyBuildings Account	MyBuildings Account			
System information >	Connection 2	Please use your MyBuildings account information to register this device with MyBuildings. If you do not have account yet, you can register here. For more information about MyBuildings, refer to the help.			
Network settings >	License >	At present, the remote functi	ion is temporarily in the trial operation phase.		
Localization >			Pair: 🗸 Connect: 🖌		
Project backups >		User name			
Firmware updates >		Password			
MyBuildings Account 1		Friendly name			
Service >			8663bd77-d5f8-405d-b766-8cd8e32fbab4		
Wi-Fi access point mode settings			Logout		
Third party authority >					
Abnormal devices >					
Onvif IPC list					
Misc settings					
	٠.		♠		

2. Accessing "Smart Access Point" on the MyBuildings Portal

- [1] On the home page of the MyBuildings Portal, click "My Home".
- [2] Click "ABB-Welcome IP".



[3] Scroll down the screen and find your "Smart Access Point", click "Open".

← → X	☆ 🖰 :
Advice: Here you can set up the remote control for your ABB-Welcome® IP System to connect your mobile device with the system. The service is supported by the following devices: IP Touch 7 (H8236.) Smart AccessPoint rp (OP001L.) Simart AccessPoint rp (OP001L.) VideoControl Netzwerk Video Recorder (C820.) VideoControl Netzwerk Video Recorder (C820.) VideoControl Netzwerk Video Recorder (C820.) Note: Using the Welcome App on your home Wi-Fi does not require remote control activation. Registering your mobile device and the IP Touch 7 in Mybuildings portal is sufficient. The use of the Welcome App in your home Wi-Fi requires the following software versions: from IP Touch 7 in Mybuildings portal is sufficient. The use of the Welcome App in your home Wi-Fi requires the following software versions: from IP Touch 7 firmware 1.49 / from IOS app version 3.0.26 / from Android app version 3.0.36. The remote control via MyBuildings Portal ensures you a comfortable and safe Cloud solution with point to point encryption. No adjustments to your Internet router are necessary. After the registration of the first device in MyBuildings Portal, the use of the "Remote Access and Notifications" extension is free of charge until	
Devices     Extensions       Jacky's Pro Edit   Delete   Open 3 available since: Aug 6, 2020 ID: 8663bd77-d5f8-405d-b766-8cd8e32fbab4 Software-Version: V5.21 Description: -	

- [4] If you cannot open the screen, click "Extensions".
- [5] Find the "Remote Access and Notifications" item.
- [6] Click "Subscribe" to purchase the service.

тие тепноте сопто на нуровнотуз то сагелонез учи а сопто саме али заге слока зоколог или ролс со ролс ели урскисти акуазаленся со учи Internet router are necessary.	
After the registration of the first device in MyBuildings Portal, the use of the "Remote Access and Notifications" extension is free of charge until 12/31/20.	
Devices 4 Extensions	
Remote Access and Notifications 5	
$\wedge n$	
\$2.49 per 30 days	
With the extension Remote access and Notifications you will not miss any door calls. You can see who is at your door, even while you on the move and have access to Welcome IP functions, in addition, there are push or e-mail notifications for information on missed door calls. So you always know what's going on at home.	
The following devices support the extension:	
IP Touch 7	
read more 6	
subscribe (\$2.49 per 30 days )	
You already using the "Remote Access and Notifications" extension in 0 of 30 possible mobil devices.	
Contact   Imprint   Terms of use   Privacy provisions	

#### 13.6.3 Restoring the "Remote control" function

"Smart Access Point" can be accessed remotely on the MyBuildings portal. see chapter 13.6.2 "Accessing "Smart Access Point" remotely" on page 325.

If you want to restore the "Remote control" function, please follow the steps below:

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

- [2] On the "Preference" screen, click "Service".
- [3] Click "Restore default settings".
- [4] Tick the check box "Reset remote control".
- [5] Tick the check box "I have stored ...".
- [6] Click " $\sqrt{}$ " to confirm.

	SS PLACE + LINK USER MANAGEMENT KOTOKA INA CONTRACT DOOR ENTRY SYSTEM
Design a building by Configure the d creating floors and the access o rooms system e.g. C repeater	control devices Create user groups system devices, e.g. Cylinder, indoor station, outdoor
🛔 jacky	Configuration 🌣 Preferences
Preferences	Service
System information >	Service Restore default settings This option resets the device to its factory defaults. All configuration data of this device will be lost.
Network settings >	Hestore detaut settings     This upilot resets the device to its factory detauts. An oblinguration data of this device will be lost.
Localization >	
Project backups >	Reset the project planning to the factory settings
Firmware updates >	☑ Reset remote control ☐ Delete user data and settings
MyBuildings Account	
Service 2	Factory settings
Wi-Fi access point mode settings	5 ☑ I have stored a current backup on my computer and know that this action will delete the configuration.
Third party authority	× 6,
Abnormal devices >	
Onvif IPC list	
Misc settings >	
	•
Onvif IPC list	

#### 13.6.4 Restoring all settings to the factory defaults

- [1] On the configuration screen, click "Preference" to access the corresponding screen.
- [2] On the "Preference" screen, click "Service".
- [3] Click "Restore default settings".
- [4] Click "Factory settings".
- [5] All the check boxes are ticked automatically.
- [6] Tick the check box "I have stored ...".
- [7] Click " $\sqrt{}$ " to confirm.

BUILDING STRUCTURE			PLACE + LINK	USER MANAGEMENT	Kan Carlos	TIME CONTROL	DOOR ENTRY SYSTEM
creating floors and	Configure the de the access or system e.g. Cy repeater	ontrol /linder,	Locating and linking devices	Add and edit users. Create user groups	Create and edit actions	Create time control	Configurate door entry system devices, e.g. indoor station, outdoor station
🎍 jacky						Device	configuration 🌣 Preferences
				DREFERENCES			
Proforences		Service					
System information	2	Servic					
Network settings	,		testore default settings		ice to its factory defaults. All confi	guration data of this device	will be lost.
Localization	>	D	ELETE PROJECT PLANNING				
Project backups	>	C L	Reset the project plan	nning to the factory settings			
Firmware updates	,		5 ☑ Reset remote control ☑ Delete user data and				
MyBuildings Account	,						
Service 7	,		2	Factory settings			
Wi-Fi access point mode settings	,	(	5 I have stored a current delete the configuration	backup on my computer and	know that this action will		
Third party authority	,		×		7 🗸		
Abnormal devices	>		^				
Onvif IPC list	,						
Misc settings	,						

#### 13.7 Notification

## Access the "Notification" screen

On the configuration screen, click <sup>1</sup> to access the "Notification" screen.

A maximum of 16,000 notifications are supported on "Smart Access Point".

<b>∨ 0</b> Pa so	os 🕥 🖡		MAIN MENU			
BUILDING STRUCTURE	RF WIRELESS CONNECTION	PLACE + LINK	USER MANAGEMENT	ACTIONS		
Design a building by creating floors and rooms	Configurate the devices of the access control system e.g. cylinders, repeaters	Locating and linking devices	Add and edit users. Create user groups	Create and edit actions	Create time control	Configurate door entry system devices, e.g. indoor station, outdoor station
abb					Device configura	ation 🌣 Preferences

#### 13.7.1 Notification

In the "Notification" view, all notifications that are defined and triggered under "Actions" are documented in the Smart Access Point.

A notification is not always associated with an action by the administrator and is used for information purposes only.

- [1] On the "Notification" screen, click "Notification".
- [2] Enter the key word.
- [3] Press "Search", all results will be displayed on the screen, click a result to view the details and click us to remove this record.
- [4] Press "Delete" to delete all the searching results.
- [6] Click "OK" to confirm the filter.
- [7] Click "Delete" to clear the filter.

				NOTIFIC
Notification		Notification		2 4
Notification(0/0)	>	Key 2d		Search Delete
Alarm(0/0)	>	Filter		<b>5</b> ~
(i) Logs(8/8)	>	Start		
				31
		End		
				31
		Today		
		Cancel	ОК	Delete
			6	7
🛃 Export				
		1		

#### 13.7.2 Alarm record

In the "Alarm" view, alarms that occur in the system are documented in the Smart Access Point.

An alarm is always associated with an action by the administrator. e.g. battery change on the cylinder is necessary.

- [1] On the "Notification" screen, click "Alarm".
- [2] Enter the key word.
- [3] Press "Search", all results will be displayed on the screen, click a result to view the details and click 🔟 to remove this record.
- [4] Press "Delete" to delete all the searching results.
- [6] Click "OK" to confirm the filter.
- [7] Click "Delete" to clear the filter.

			NOTIFIC
Notification		Alarm	2 4
Notification(0/0)	>	Keyword 2	Search Delete
Alarm(0/0) 1	>	Filter	5~
(i) Logs(8/8)	>	Start	
			31
		End	
			31
		Today	
		Alarm state	
		All states	6 7 ·
		Cancel	OK Delete
🛃 Export			

#### Alarm records about AC devices

On the "Preferences" – "Misc settings" screen, tick the checkbox "Alarm when cylinder goes offline".

After this setting, when the AC devices are offline, alarm records about AC devices will be created.

Preferences		Misc settings						
Network settings	>	Time synchronisation for door entry system devices						
Localization	>	Automatically     Manually						
Project backups	>	Synchronize period(hour) 1						
Firmware updates	>	Apply						
MyBuildings Account	>	Door communication devices						
Service	>	Alarm when device goes offline						
Wi-Fi access point mode settings	>	<ul> <li>Enable sound notification</li> <li>Enable popup notification</li> </ul>						
Third party authority	>	Access control devices						
Abnormal devices	>	✓ Alarm when cylinder goes offline						
Onvif IPC list	>	Apply						
Misc settings	>	*						

### 13.7.3 Logs

In the "Log" view, non-critical actions that occur in the system are documented in the Smart Access Point.

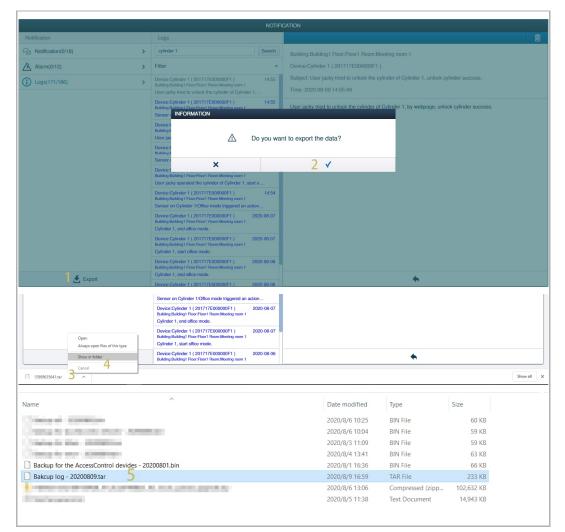
A log entry is not associated with an action by the administrator and is used for information purposes only.

- [1] On the "Notification" screen, click "Logs".
- [2] Enter the key word.
- [3] Press "Search", all results will be displayed on the screen, click a result to view the details and click 🔟 to remove this record.
- [4] Press "Delete" to delete all the searching results.
- [6] Click "OK" to confirm the filter.
- [7] Click "Delete" to clear the filter.

			NOTIFI
Notification		Logs	3 4
Notification(0/0)	>	Keyword 2	Search Delete
Alarm(0/0)	>	Filter	<b>5</b> ~
(i) Logs(8/8)	>	Start	
			31
		End	
			31
		Today	
		Message type	-
		All types 6	<b>/</b> ~
		Cancel OK	Delete
		Device:Smart Access Point ( 105807A7F030734 )	2021-06-25
		jacky 's user info ( password ) has been changed b	oy user jacky.
🛃 Export		Device:Smart Access Point ( 105807A7F030734 )	2021-06-23

#### 13.7.4 Exporting the notifications

- [1] On the "Notification" screen, click "Export".
- [2] Click "√".
- [3] Right click the exported file.
- [4] Click "Show in folder".
- [5] Rename the log file.



#### 13.8 Message center

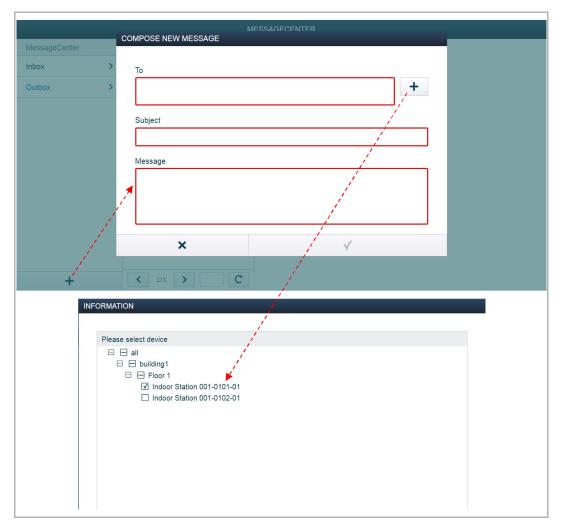
# Accessing the "Message center" screen

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

♥ 🚳 🗟 🛇	ac (1) ac		MAIN MENU			
BUILDING STRUCTURE		PLACE + LINK	USER MANAGEMENT	ACTIONS		DOOR ENTRY SYSTEM
Design a building by creating floors and rooms	Configurate the devices of the access control system e.g. cylinders, repeaters	Locating and linking devices	Add and edit users. Create user groups	Create and edit actions	Create time control	Configurate door entry system devices, e.g. indoor station, outdoor station
abb					Device configura	ation 🌣 Preferences

### 13.8.1 Creating a message

On the "Message center" screen, click "+" to set a recipient, then enter the subject and the message, click " $\sqrt{}$ " to create and send the message.



#### 13.8.2 Replying to a message

On the "Message center" screen, click "Inbox" to view the message received from the indoor stations. You can click on a message and reply to it directly.

A maximum of 1000 messages is supported.

		М	ESSAGECENTER
MessageCenter		Inbox	Test
Inbox	>	Search Search	Indoor Station 001-0101-01
Outbox	>	Filter ~	Test receive time: 2019-03-05 22:53
		Indoor Station 001-0101-01 22:53 Test	Hello! RE:Test Hello!
+		< 1/1 > C	× ×

# 14 Notice

We reserve the right to at all times make technical changes as well as changes to the contents of this document without prior notice.

The detailed specifications agreed to at the time of ordering apply to all orders. ABB accepts no responsibility for possible errors or incompleteness in this document.

We reserve all rights to this document and the topics and illustrations contained therein. The document and its contents, or excerpts thereof, must not be reproduced, transmitted or reused by third parties without prior written consent by ABB.



#### ABB Xiamen Smart Technology Co., Ltd.

No.7, Fangshan South Road, Hi-tech area, Torch park, Xiang An District, Xiamen, China Tel: +86 592 295 9000 Fax: +86 592 562 5072

www.abb.com