2TMD042400D0022 | 18.12.2024

System Manual

Busch-Welcome® IP

BUSCH-JAEGER

1 Overview of IP Technology

1.1 Cabling and Connection

1.1.1 Fundamentals of structured cabling

Structured cabling is a uniform setup plan for a network infrastructure. The network infrastructure is independent of the application and future oriented. Additional designations for the structured cabling are Universal Structured Cabling (UGV) or Universal Communication Cabling (UKV).

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

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

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

Structured cabling includes the following points:

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

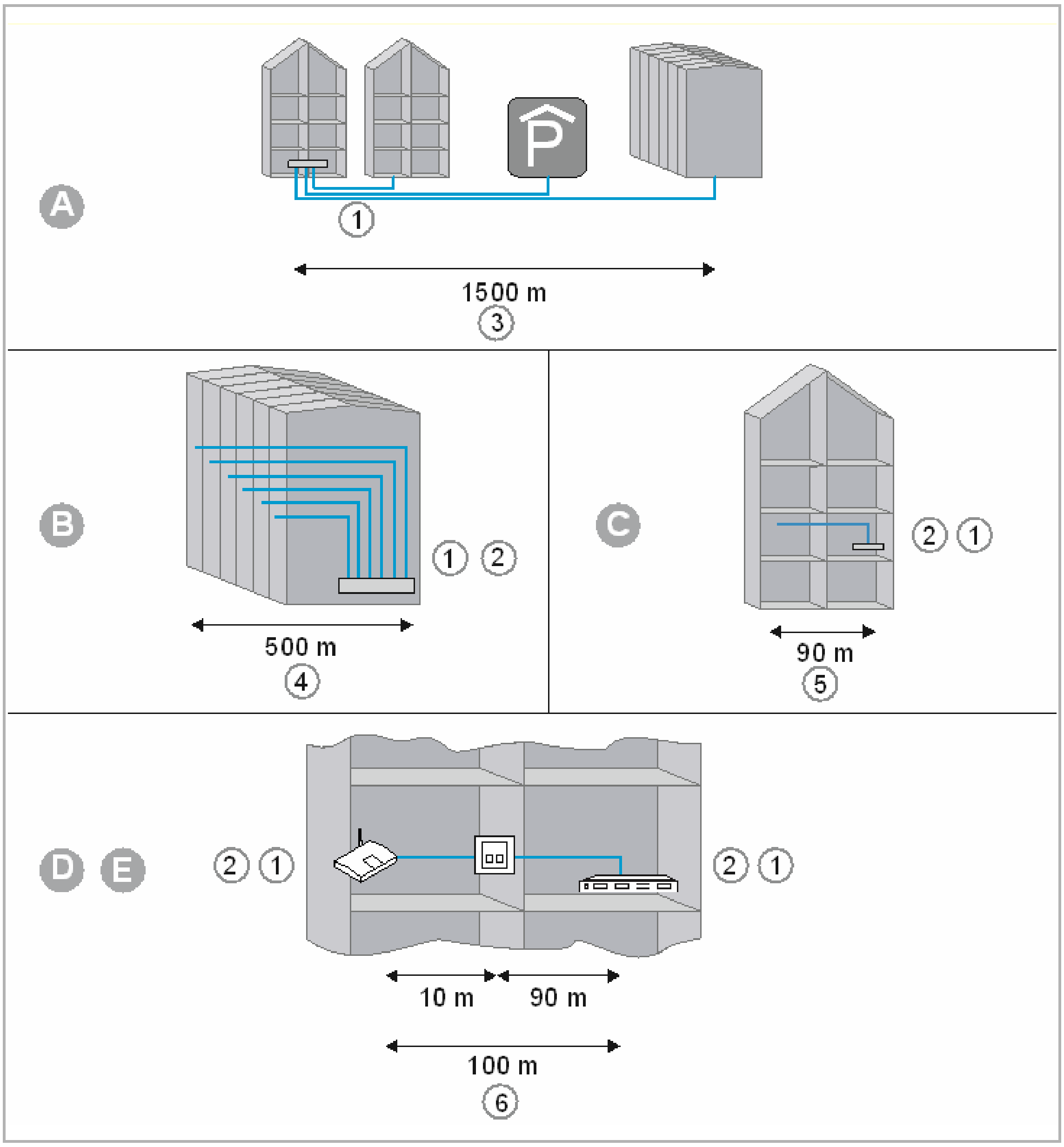
Objectives of structured cabling

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

Standards for structured cabling

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

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



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

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

Cabling is divided into the following areas:

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

The cabling standards are optimised for the following geographic expansion:

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

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

Notice

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

Primary cabling - Site cabling

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

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

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

Secondary cabling - building cabling

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

Tertiary cabling - floor cabling

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

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

Components of structured cabling:

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

1.2 Network types

For a Welcome IP system there is a distinction between networks:

- Building Network
- Private Network

Building Network

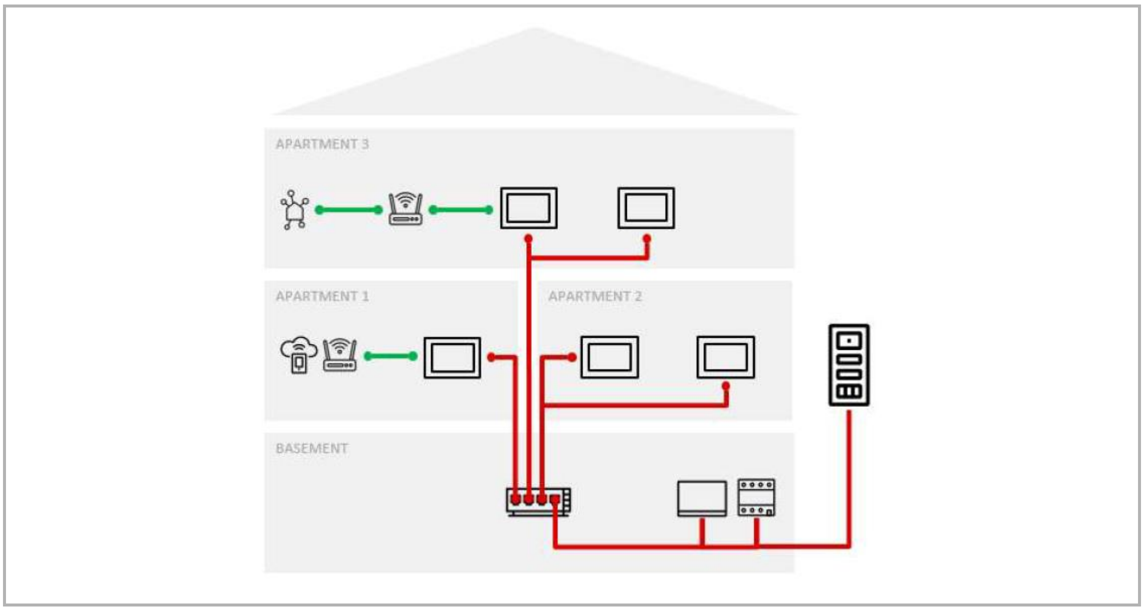
The building network includes all conduits and network components from the outdoor station up to the master indoor station of a unit (apartment or business unit).

Main connection network for Welcome IP. Always necessary, it will be set-up by the installer and represents the core communication way for the Door Entry system devices.

Private Network

The private network includes all components within a unit (apartment or business unit).

It may be used in multi-unit installations to enable private connectivity to smart home and single unit internet. It is usually the end final user’s responsibility, and it could be set up after the main DES System has been commissioned.



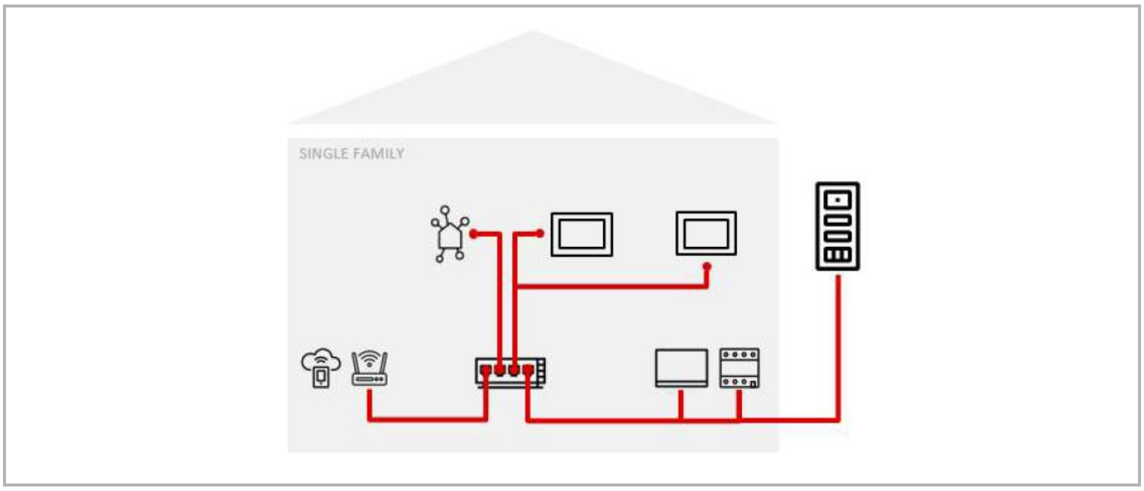
This network differentiation in multi apartment projects, may allow a clear separation between devices belonging to public or private.

- Public devices shared among the tenants of different apartments, (such as main entrance outdoor stations, gate stations, public cameras, elevator controller, guard unit etc.).
- Private devices which are privately managed by the tenants of a single unit (such as private cameras, a second privately confirmed outdoor station, smart home devices, private actuators etc.)

Nevertheless, it is now possible to connect private marked devices directly to the central POE/switch.

The network differentiation is not usually required for Single Family houses, as the entire building is owned and shared, but it is still possible to differentiate if required.

It is still possible to share between Building Network/Private to split the network.



1.3 IP Addressing assignment modes

1.3.1 Precondition

It is required the installation of the following (or later versions) software version:

In case you are not sure which version installed in your components or you face issues during the installation, please use two guides as reference.

- Update Guideline for internet connected systems.
- Update Guideline for off-line systems.

Device name	Software version
SmartAP	V6.59
IP Touch 10 (legacy UI)	V2.48
IP Touch 10 (new UI)	V3.03
IP Touch 7 (legacy UI)	V2.48
IP Touch 7 (new UI)	V3.00
IP Touch Lite 7	V1.10
Outdoor Station	V1.54
Guard Unit	V1.57
IP Actuator	V1.17
IP Elevator Controller	V1.15
Audio IP	V1.22
Mini Video Outdoor Station with IC	V1.16

1.3.2 Automatic (DHCP) / Manual Mode

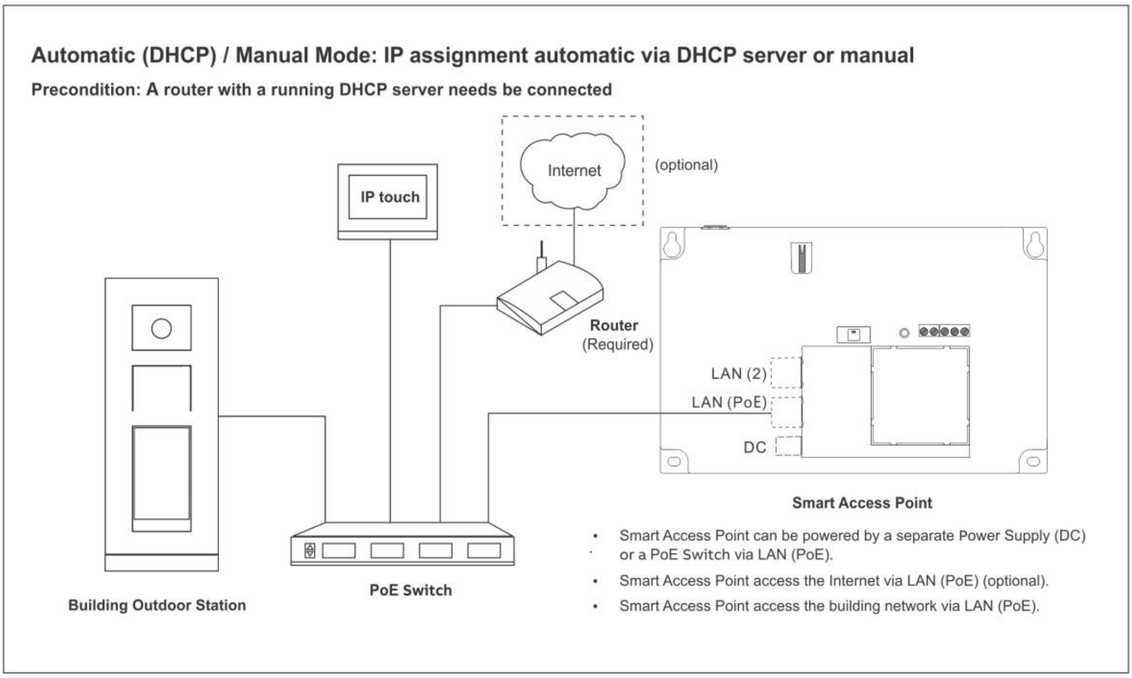
In the Automatic (DHCP) or Manual Mode, the requirement is a router installed and connected to the POE switch which is necessary for the IP address assignation.

The advantages of this mode are:

- The IP address is randomly generated (in DHCP), or manually selected (manual static mode), allowing a multi-function use of the network (no conflict with CCTV, building home automation or others.)
- Option to connect all DES devices* to the same PoE switch, with consequent cabling simplification and speed of installation
- Greater flexibility on multi-unit projects

(* limitations for private used devices per single unit: up to 8 IS, 4 second confirmed OS, 4 IPA)

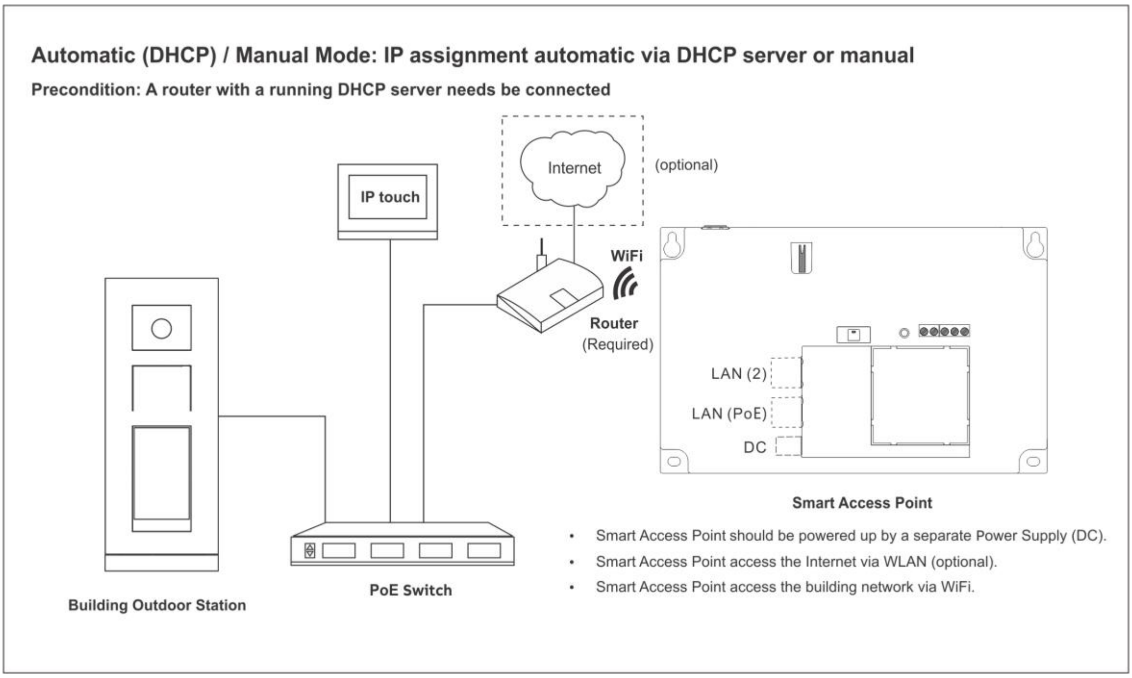
The router is required to be connected via LAN cable to the main PoE switch of the System Network (diagram 1 below), or via WIFI from the SmartAP (diagram 2 below).



Automatic (DHCP) / Manual Mode: IP assignment automatic via DHCP server or manual

Precondition: A router with a running DHCP server needs be connected

- Smart Access Point can be powered by a separate Power Supply (DC) or a PoE Switch via LAN (PoE).
- Smart Access Point access the Internet via LAN (PoE) (optional).
- Smart Access Point access the building network via LAN (PoE).



Automatic (DHCP) / Manual Mode: IP assignment automatic via DHCP server or manual

Precondition: A router with a running DHCP server needs be connected

- Smart Access Point should be powered up by a separate Power Supply (DC).
- Smart Access Point access the Internet via WLAN (optional).
- Smart Access Point access the building network via WiFi.

1.3.3 ABB Legacy Mode

In the ABB Legacy Mode, there is no need for a router to be installed, as it may be used as optional gateway to connect to internet, but it is not required for the IP Addressing assignation.

The IP Addressing is automatically generated by Welcome IP, based on the physical addressing of the devices.

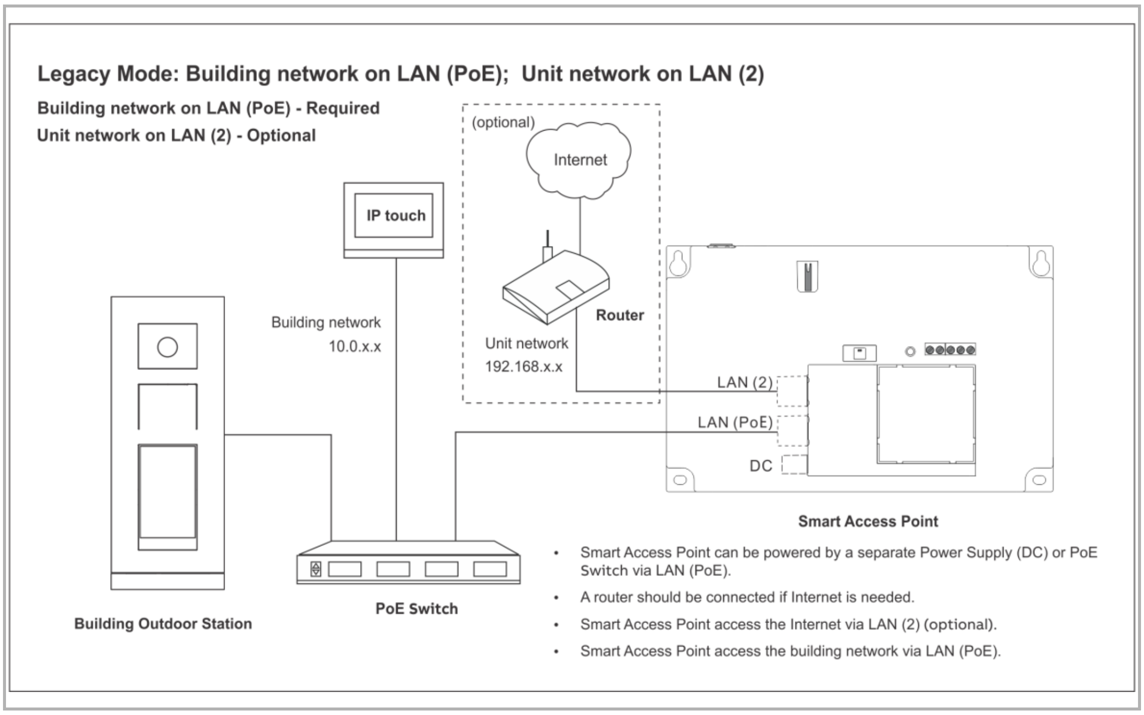
The ABB Legacy Mode requires the separation of the Door Entry Network from other networks that may be used in the project, however, to avoid addressing conflicts.

The advantages of this mode are:

- Simple installation for project with dedicated DES network
- No router requirement
- Option to connect all DES devices* to the same PoE switch, with consequent cabling simplification and speed of installation.

(* limitations for private used devices per single unit: up to 4 IS, 2 second confirmed OS, 2 IPA)

The recommended set up is to connect the Building Network in the LAN (PoE), while dedicating the Private Network to the LAN (2) port in the SmartAP:



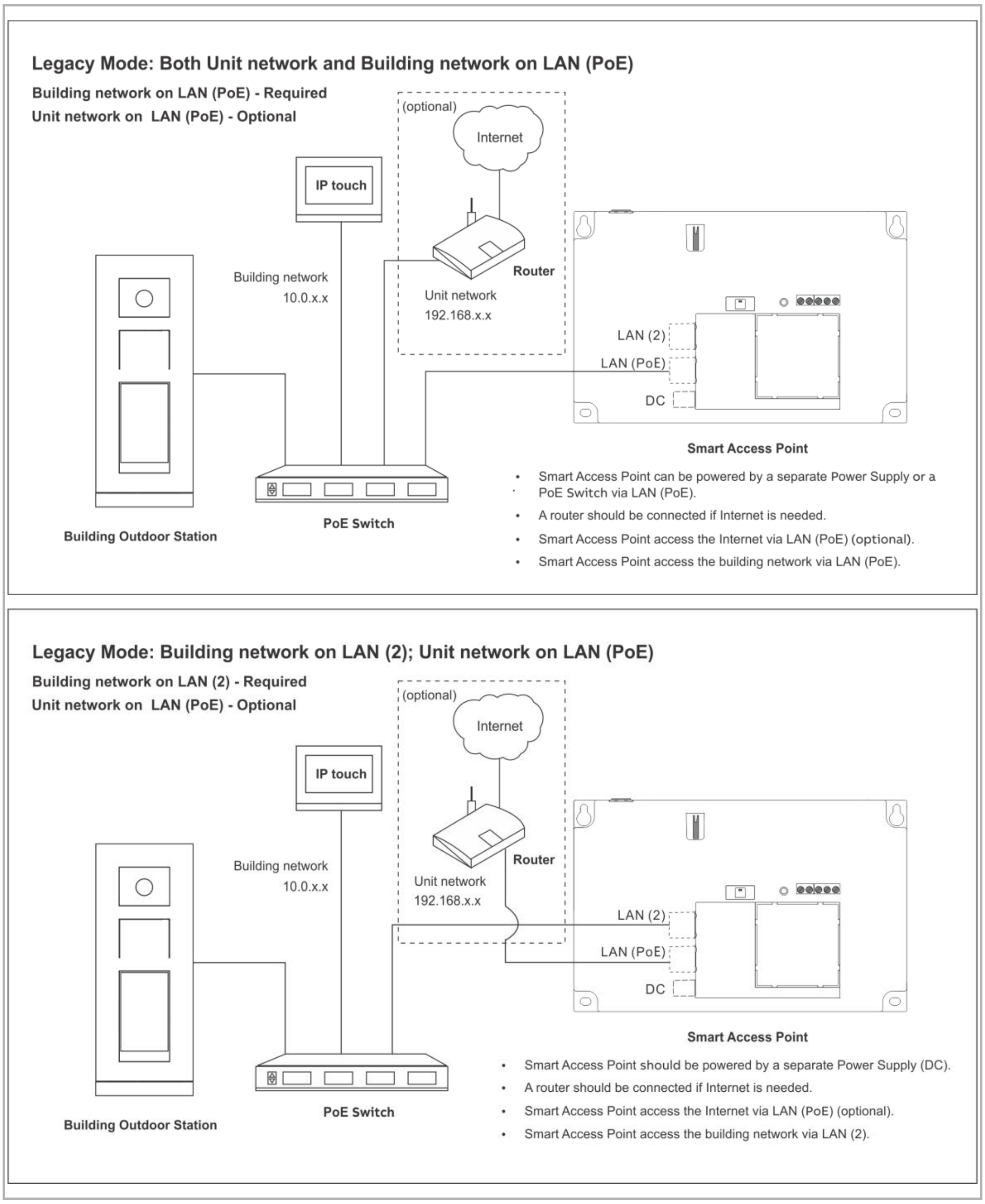
Legacy Mode: Building network on LAN (PoE); Unit network on LAN (2)

Building network on LAN (PoE) - Required

Unit network on LAN (2) - Optional

- Smart Access Point can be powered by a separate Power Supply (DC) or PoE Switch via LAN (PoE).
- A router should be connected if Internet is needed.
- Smart Access Point access the Internet via LAN (2) (optional).
- Smart Access Point access the building network via LAN (PoE).

However, it is also possible to connect the router directly to the PoE, or to the LAN (PoE), or to the WiFi of SmartAP:



Legacy Mode: Both Unit network and Building network on LAN (PoE)

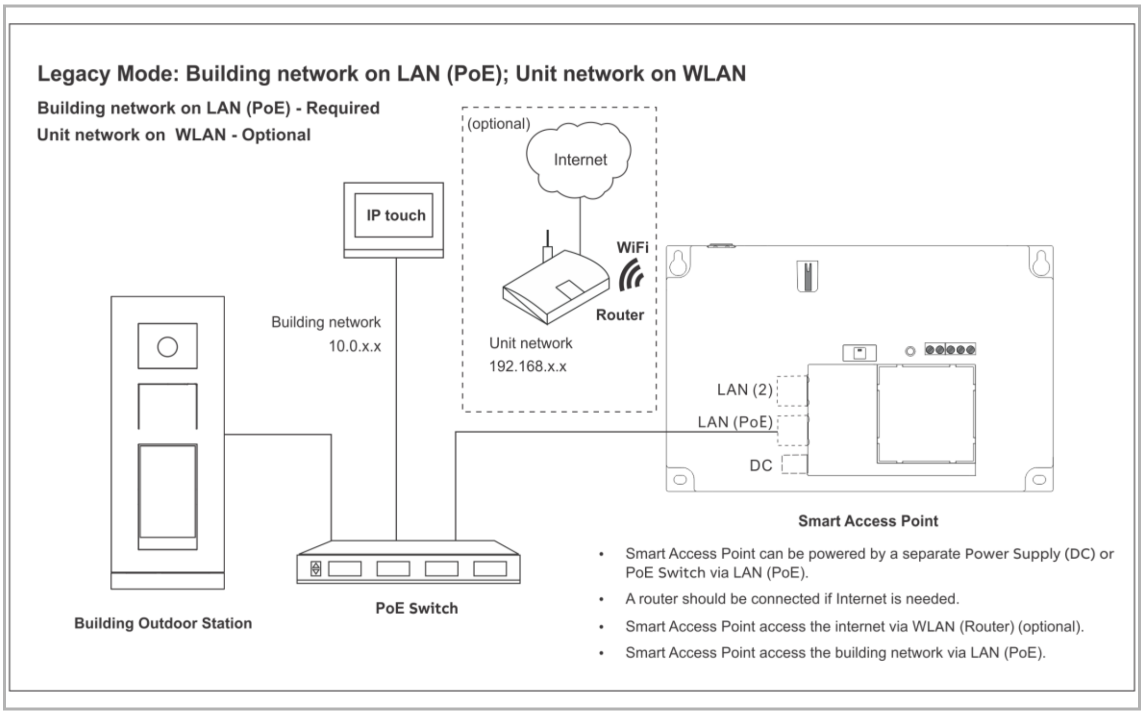
Building network on LAN (PoE) - Required
Unit network on LAN (PoE) - Optional

- Smart Access Point can be powered by a separate Power Supply or a PoE Switch via LAN (PoE).
- A router should be connected if Internet is needed.
- Smart Access Point access the Internet via LAN (PoE) (optional).
- Smart Access Point access the building network via LAN (PoE).

Legacy Mode: Building network on LAN (2); Unit network on LAN (PoE)

Building network on LAN (2) - Required
Unit network on LAN (PoE) - Optional

- Smart Access Point should be powered by a separate Power Supply (DC).
- A router should be connected if Internet is needed.
- Smart Access Point access the Internet via LAN (PoE) (optional).
- Smart Access Point access the building network via LAN (2).



Legacy Mode: Building network on LAN (PoE); Unit network on WLAN

Building network on LAN (PoE) - Required

Unit network on WLAN - Optional

- Smart Access Point can be powered by a separate Power Supply (DC) or PoE Switch via LAN (PoE).
- A router should be connected if Internet is needed.
- Smart Access Point access the internet via WLAN (Router) (optional).
- Smart Access Point access the building network via LAN (PoE).

1.3.4 Ports & services in a Welcome IP system

The following ports & services are used in a Welcome IP system.

Port	Service
5060, 5070	UDP (SIP)
5004 / 5005 / 5006 / 5007	UDP
8016 / 8017	UDP
7777	UDP
7005 / 7006	TCP
7777	TCP
8001	TCP
5061, 5070	TCP (SIPS)
50602	UDP
239.0.0.1:3333	UDP (Multicast)
239.0.0.1:4444	UDP (Multicast)
239.0.0.1:5555	UDP (Multicast)
8887	TCP
10777	TCP (TLS)
11778	TCP (TLS)
12779	TCP (TLS)
5269	TCP
5222	TCP (TLS)
1070, 1071	UDP
8277	TCP

1.4 PoE switch selection

For selecting a PoE switch, please observe the following points:

- All Welcome IP devices meet standard IEEE802.3af
  - Welcome IP devices can be operated with PoE switches that meet standard 802.3af or 802.3at. A power supply via 24 V is also possible as an alternative to the PoE.
- The minimum band width amounts to 100 Mbit/s.

Notice
During selection, observe that the absolute total output on the PoE switch is adequate for all devices to be connected.

- Do not load the PoE switch to its limit.
- Include a power buffer of at least 20% when calculating the total output.

Device	Power supply: PoE switch	Power supply: Local	Consumption	Power consumption (W)
Audio IP	●	-	40 mA / 48 VDC	1.9
IP Touch Lite 7 (LAN+WiFi)	●	●	375 mA / 24 VDC	9.0
IP Touch 7 (LAN+WiFi)	●	●	280 mA / 24 VDC	6.72
IP Touch 7 (LAN+LAN)	●	●	440 mA / 24 VDC	10.6
IP Touch 10 (LAN+WiFi)	●	●	440 mA / 24 VDC	10.6
IP Touch 10 (LAN+LAN)	●	●	500 mA / 24 VDC	12.0
Mini Video Outdoor Station	●	●	350 mA / 24 VDC	8.4
IP Touch 5 Outdoor Station	●	●	450 mA / 24 VDC	10.8
IP Pushbutton Outdoor Station	●	●	450 mA / 24 VDC	10.8
IP Keypad Outdoor Station	●	●	500 mA / 24 VDC	12.0
SmartAP	●	●	375 mA / 24 VDC	9.0
Guard unit	●	●	260 mA / 24 VDC	6.2
IP Actuator	●	●	350 mA / 24 VDC	8.4
P Elevator Controller	●	●	60 mA / 24 VDC	1.4
Lift control relay module	-	●	250 mA / 24 VDC	6.0

Example for the selection of a PoE switch

Count	Device	Power consumption (W)
3	IP Touch 7 Lite (LAN+WiFi)	3*9,0=27.0
1	IP Touch 5 Outdoor Station	10.8
1	IP Actuator	8.4
	Total output	46.2

Result	
Number of occupied ports:	5
Necessary total output:	46.2

Recommendation:

For the calculation of a reserve for the future, a PoE switch with 8 ports and a total output of 70 W is recommended for this example.

The individual consumption per port should not exceed the maximum total consumption of the entire PoE switch.

*

2 Overview of product range

2.1 Outdoor Stations

2.1.1 Overview

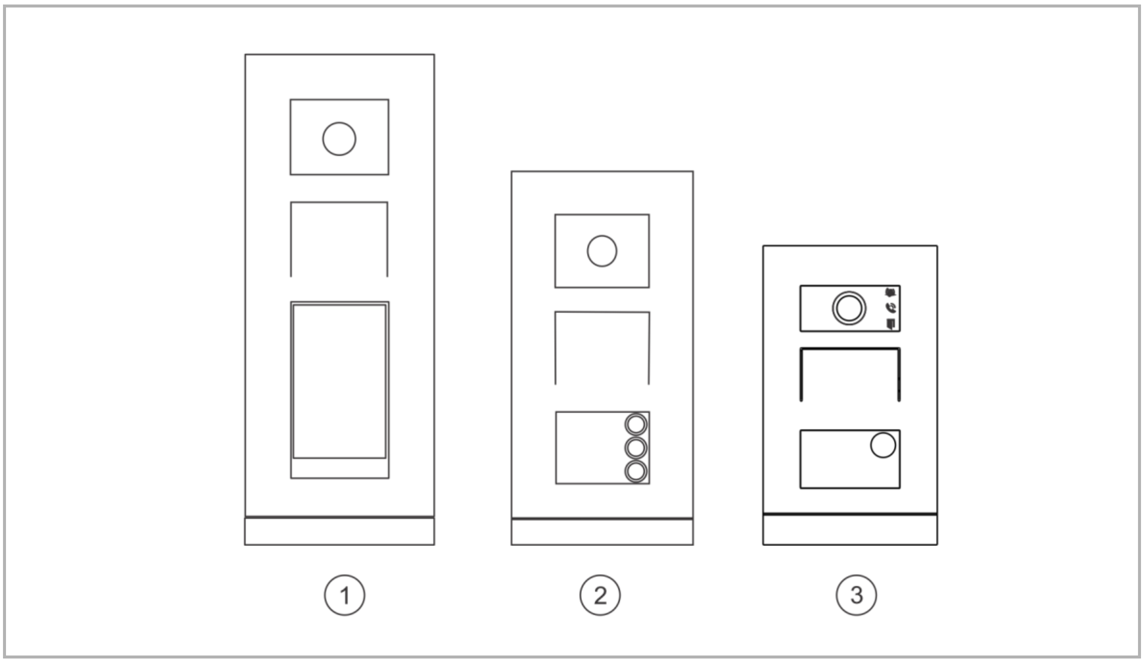
Welcome IP Outdoor Stations are installed in the outdoor areas as follow:

- Building entrances
- Perimeter areas
- Storey areas
- Apartment doors
- Basement garages

For the door call there is also a voice output aside from the classic doorbell buttons. The voice output can be activated as an option.

Outdoor Stations are always equipped with video function.

Outdoor Stations are available in the materials stainless steel and white, and aluminium.



No.	Article number	Product name	Abbreviation
1	H8138.T-.-03	IP Touch 5 Outdoor Station	IP Touch 5 OS
2	H81381P.-.-03	IP Pushbutton Outdoor Station	IP Pushbutton OS
3	H8131.P.-.-03/ H8136.P.-.-03	Mini Video Outdoor Station	Mini OS

*"Outdoor Station" is usually abbreviated to "OS".

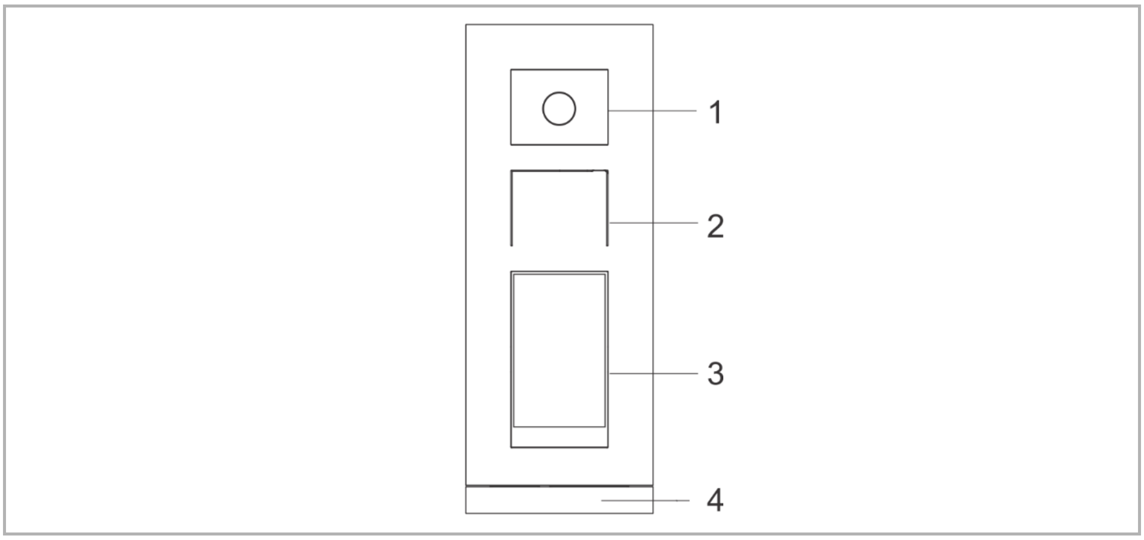
Type	IP Touch 5 OS	IP Pushubtton OS	Mini OS - IC
Video image	720P	720P	VGA
Camera angle diagonal / horizontal / vertical	139° / 111° / 73°	139° / 111° / 73°	139° / 111° / 73°
Anti-mist camera	●	●	●
Automatic day/night switchover	●	●	●
Integrated status display via LED symbols (complies with DIN 18040).	●	●	●
Capacitive touch screen 5 inch	●	-	-
Virtual keypad	●	-	-
Programmable buttons	-	●	●
Detection of door status	●	●	●
Integrated lighting and automatic background illumination	●	●	●
Transfer of all calls to the Guard Unit	●	-	-
Support of lift control	●	●	-
Integrated RFID reader (MIFARE® DESFire® EV1 and EV2)	●	●	●
News and advertising via 5 inch monitor	●	-	-
Induction loop for persons with impaired hearing	●	●	-
Power supply via PoE (802.3af)	●	●	●
Local power supply	●	●	●
Surface-mounted installation	●	●	●
Flush-mounted installation	●	●	●
Cavity wall installation	●	●	●
Protection rating	IP 54	IP 54	IP 54
Safe against vandalism	IK 07	IK 07	IK 07
Remote firmware update	●	●	●

2.1.2 IP Touch 5 OS

Device type

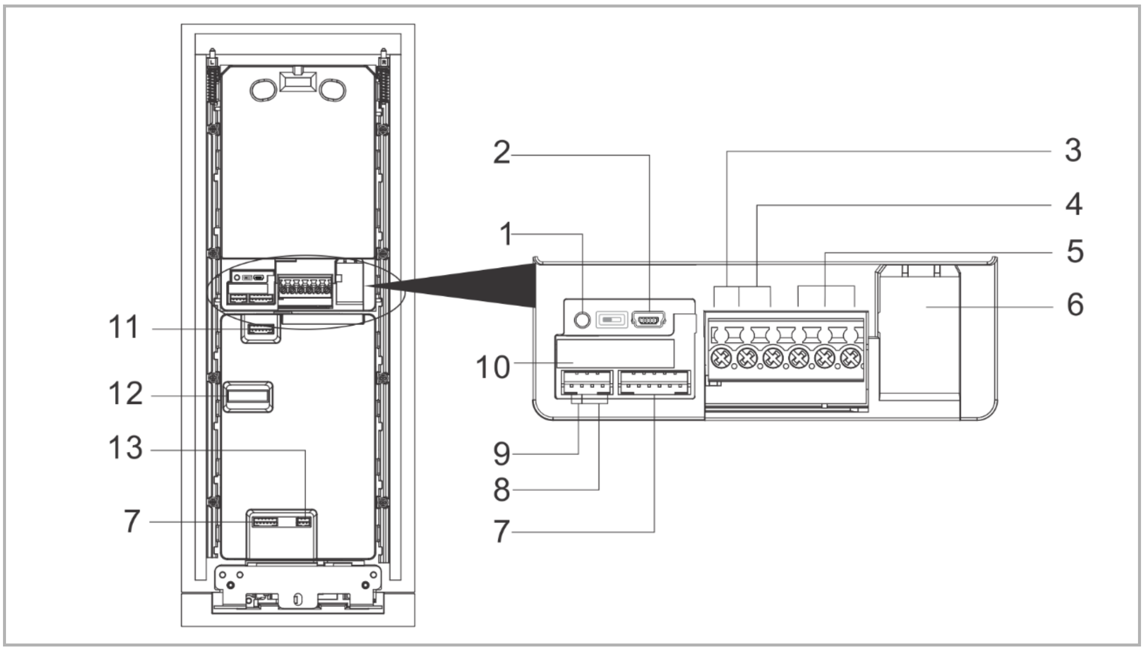
Article number	Product ID	Product name	Colour	Size (WxHxD) Unit: mm
H81381T-S-03	2TMA130010X0027	IP Touch 5 Outdoor Station	Stainless steel	135 x 349 x 29
H81381T-W-03	2TMA130010W0017	IP Touch 5 Outdoor Station	White	135 x 349 x 29

Control elements



No.	Description
1	Camera
2	Speaker and microphone integration
3	5-inch touch display
4	End strip

Terminal description



No.	Description
1	Reset button
2	Micro USB update connector
3	Plug-in clamps (DC+...GND) for standalone power supply
4	Plug-in clamps (LOCK...GND) for door opener
5	Plug-in clamps (COM...NC...NO) for floating output, door opener
6	LAN (PoE)
7	Connector for next module
8	Connector for exit button
9	Connector for the sensor used for door status detection
10	Connector for 5" display module
11	Connector for previous module
12	Connector for A/V module
13	Connector for Wiegand output It supports 26 bits and 34 bits

Technical data

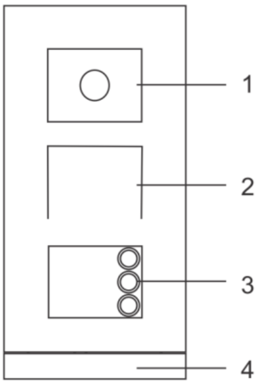
Designation	Value
Rating voltage	24 V ⎓
Operating voltage range	20-27 V ⎓
Rating current	27 V ⎓, 410 mA 24 V ⎓, 450 mA
Operating temperature	-20 °C…+55 °C
Camera type	CMOS
Camera viewing angle	130°
Resolution ratio	HD (1280 x 720 pixel)
Ambient brightness	<50000 Lux
Power supply for door opener	18 V, 4 A impulse, max. 250 mA holding
Floating output for door opener	230 V ~, 3 A 30 V ⎓, 3 A
Video codec	H.264
Audio codec	G.711
IP level	IP 54
IK level	IK 07

2.1.3 IP Pushbutton OS

Device type

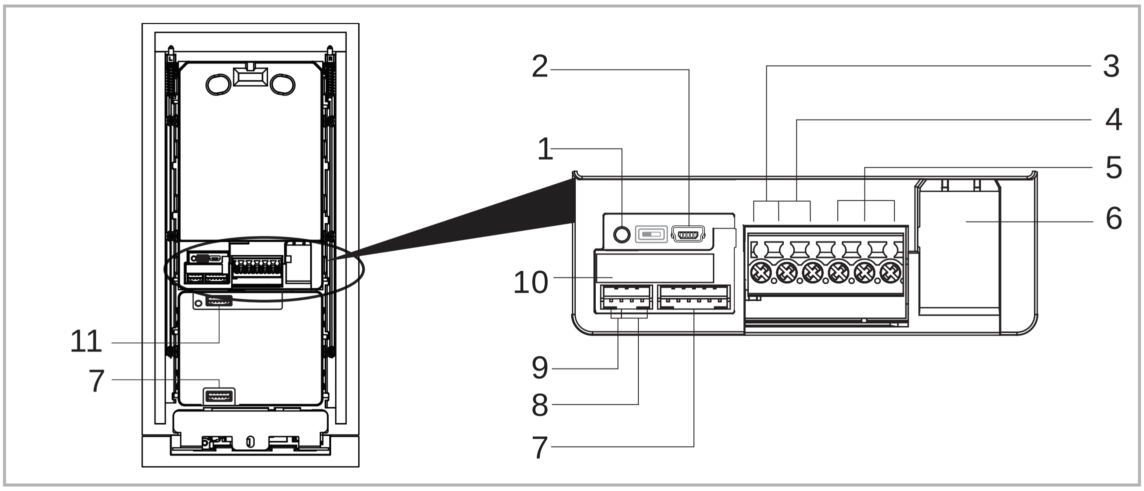
Article number	Product ID	Product name	Colour	Size (WxHxD) Unit: mm
H81381P1-S-03	2TMA130010X0019	OS, IPpush, 1 gang	Stainless steel	135 x 277 x 29
H81381P2-S-03	2TMA130010X0020	OS, IPpush, 2 gang	Stainless steel	135 x 277 x 29
H81381P3-S-03	2TMA130010X0021	OS, IPpush, 3 gang	Stainless steel	135 x 277 x 29
H81381P1-W-03	2TMA130010W0023	OS, IPpush, 1 gang	White	135 x 277 x 29
H81381P2-W-03	2TMA130010W0027	OS, IPpush, 2 gang	White	135 x 277 x 29
H81381P3-W-03	2TMA130010W0031	OS, IPpush, 3 gang	White	135 x 277 x 29

Control elements



No.	Description
1	Camera
2	Speaker and microphone integration
3	Round pushbutton
4	End strip

Terminal description



No.	Description
1	Reset button
2	Micro USB update connector
3	Plug-in clamps (DC+...GND) for standalone power supply
4	Plug-in clamps (LOCK...GND) for door opener
5	Plug-in clamps (COM...NC...NO) for floating output, door opener
6	LAN (PoE)
7	Connector for next module
8	Connector for exit button
9	Connector for the sensor used for door status detection
10	Connector for 5" display module
11	Connector for previous module

Technical data

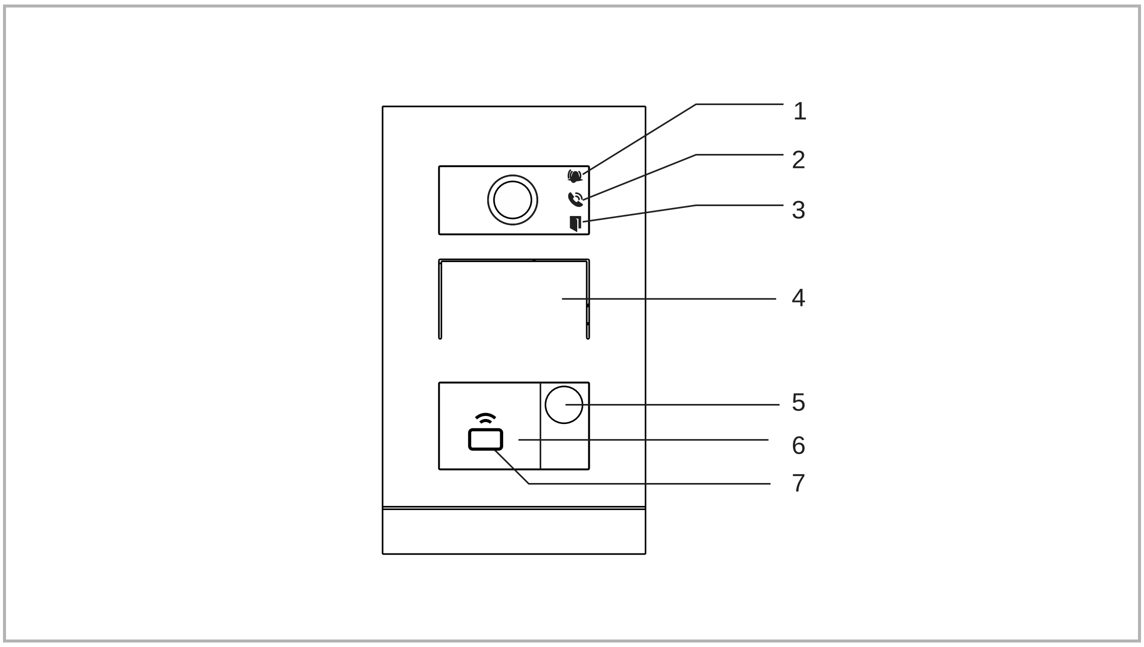
Designation	Value
Rating voltage	24 V DC
Operating voltage range	20-27 V DC
Rating current	27 V DC, 300 mA 24 V DC, 330 mA
Operating temperature	-40 °C…+55 °C
Product dimensions	135mm x 276.9 mm × 17.6 mm
Camera type	CMOS
Camera viewing angle	130°
Resolution ratio	HD (1280 x 720 pixel)
Power supply for door opener	18 V, 4 A impulse, max. 250 mA holding
Floating output for door opener	230 V AC, 3 A 30 V DC, 3 A
Video codec	H.264
Audio codec	G.711
IP level	IP 54
IK level	IK 07

2.1.4 Mini OS

Device type

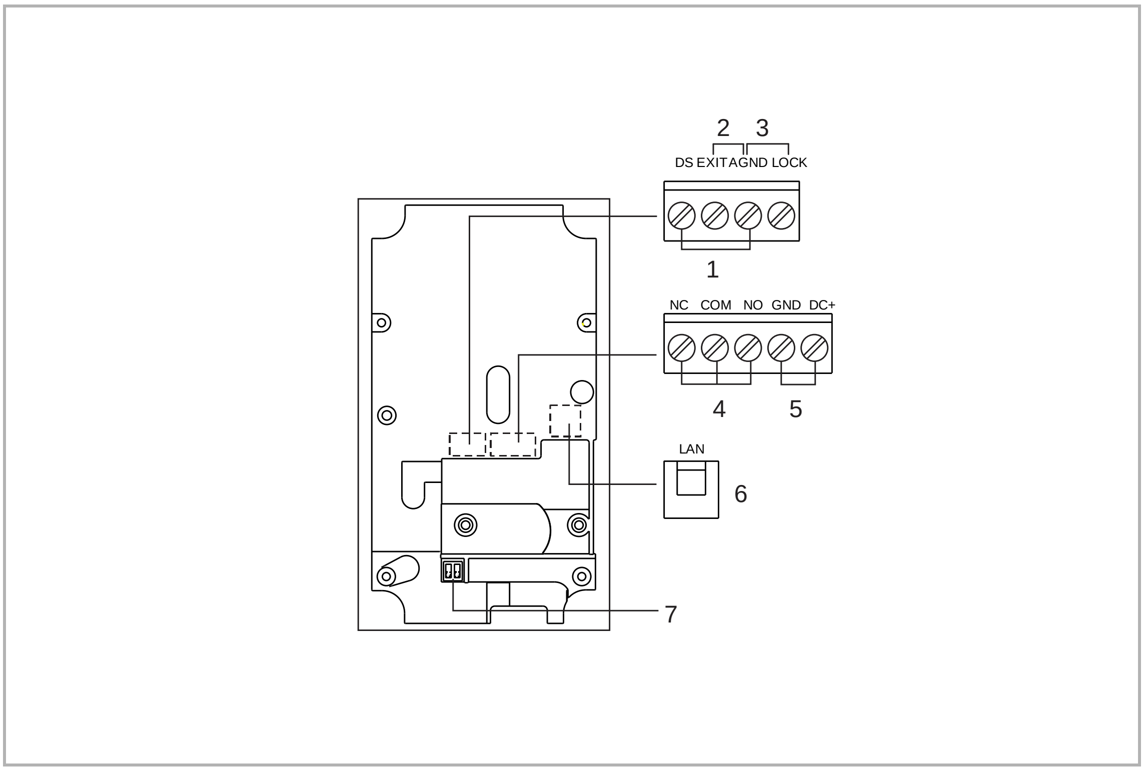
Article number	Product ID	Product name	Colour	Size (WxHxD) Unit: mm
H81313P1-A-03	2TMA130010A0003	Mini video outdoor station, 1 gang, ID, SM	Aluminium alloy	99 x 168 x 26
H81313P2-A-03	2TMA130010A0006	Mini video outdoor station, 2 gang, ID, SM	Aluminium alloy	99 x 168 x 26
H81363P1-A-03	2TMA130010A0009	Mini video outdoor station, 1 gang, ID,FM	Aluminium alloy	105 x 180 x 43
H81363P2-A-03	2TMA130010A0012	Mini video outdoor station, 2 gang, ID, FM	Aluminium alloy	105 x 180 x 43
H81364P1-A-03	2TMA130010A0015	Mini video outdoor station, 1 gang, FM	Aluminium alloy	99 x 168 x 26
H81316P1-A-03	2TMA130010A0016	Mini video outdoor station, 1 gang, IC/DESFire, SM	Aluminium alloy	99 x 168 x 26
H81316P2-A-03	2TMA130010A0017	Mini video outdoor station, 2 gang, IC/DESFire, SM	Aluminium alloy	105 x 180 x 43
H81366P1-A-03	2TMA130010A0018	Mini video outdoor station, 1 gang, IC/DESFire, FM	Aluminium alloy	105 x 180 x 43
H81366P2-A-03	2TMA130010A0019	Mini video outdoor station, 2 gang, IC/DESFire, FM	Aluminium alloy	105 x 180 x 43

Control elements



No.	Description
1	**Ring indicator** Indicator flashes slowly: ringing Indicator flashes quickly: busy line
2	Call indicator
3	Unlock indicator
4	Speaker and microphone integration
5	Call button
6	Label field
7	Integrated ID card reader

Terminal description



No.	Description
1	Connector for the sensor used for door status detection
2	Connector for exit button
3	Plug-in clamps (LOCK...AGND) for door opener
4	Plug-in clamps (COM...NC...NO) for floating output
5	Plug-in clamps (DC+...GND) for standalone power supply
6	LAN (PoE)
7	N/A

Technical data

Designation	Value
Rating voltage	24 V ⎓
Operating voltage range	20-27 V ⎓
Rating current	27 V ⎓, 310 mA 24 V ⎓, 350 mA
Operating temperature	-40 °C…+55 °C
Product dimensions	99 mm x 168 mm × 26 mm (H8131.P.-.) 105 mm x 180 mm × 43 mm (H8136.P.-.)
Camera type	CMOS
Camera viewing angle	104°
Power supply for door opener	15 V ⎓, 4A impulse, max. 250 mA holding
Floating output for door opener	30 V ⎓, 3 A
IP level	IP 54
IK level	IK 07
Network connection standard	IEEE802.3, 10/100 Mbps, auto MDI/MDI-X

2.2 Indoor Stations

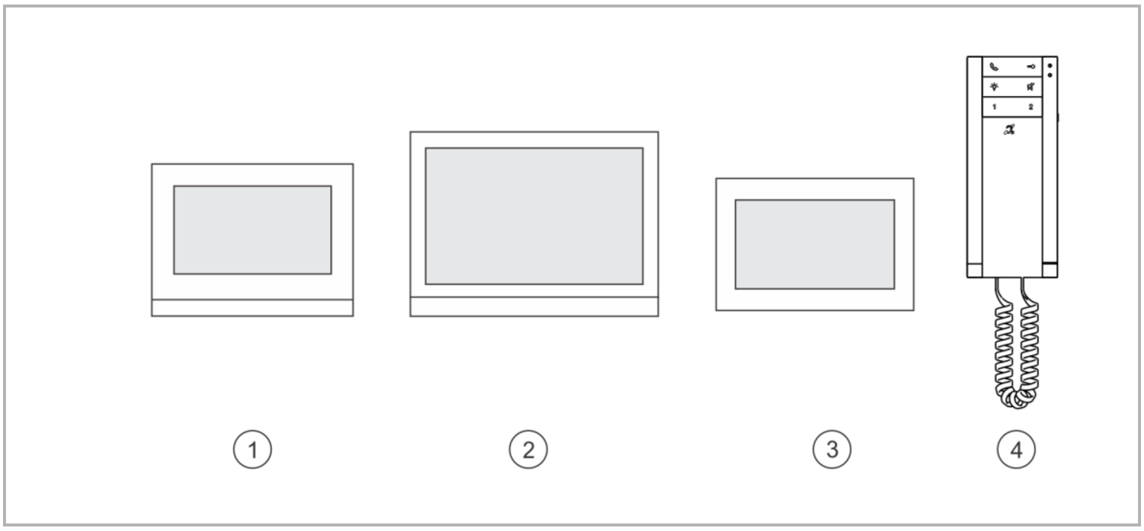
2.2.1 Overview

The door call is signalled on the Indoor Station. Here the call is received and the door is opened when a visitor arrives. The camera image is displayed directly, to ensure that you immediately see who is at the door and you can communicate with the visitor.

As an option, a visitor can leave an audio message, if the function has been enabled on the Indoor Station.

The indoor stations can also be used with the intercom function for communication within and between apartments and buildings.

The integrated blacklist can be used to specify which calls are blocked automatically.



No.	Article number	Product name	Abbreviation
1	H8236-.-03	IP Touch 7	IP Touch 7
2	H8237-.-03	IP Touch 10	IP Touch 10
3	H8249-03	IP Touch Lite 7	IP Touch Lite 7
4	H82001-W-03	Audio IP	Audio IP

*"Indoor Station" is usually abbreviated to "IS"

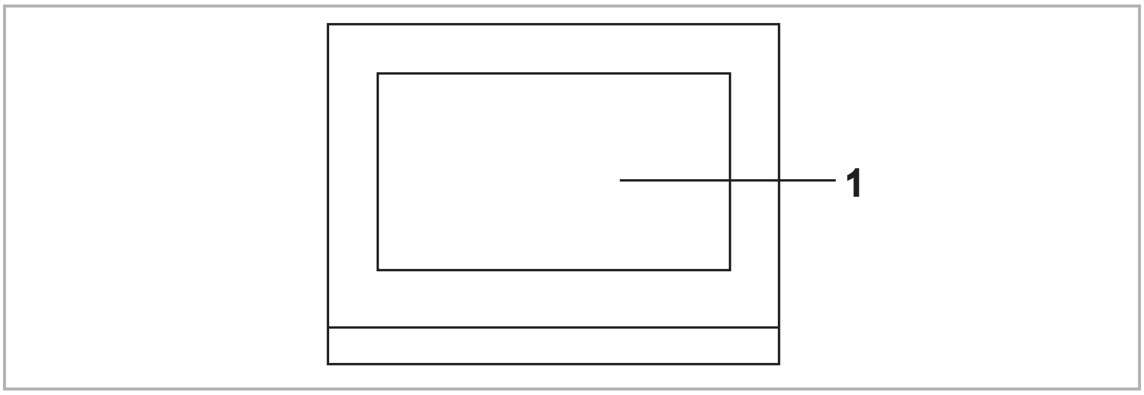
Type	IP Touch 7	IP Touch 10	IP Touch Lite 7	Audio IP
Touchscreen	●	●	●	-
Extension on app without additional system equipment (prerequisite is an Internet connection)	●	●	●	-
Central operating field for DES, CCTV, AC and home automation (KNX & F@H)	●	●	-	-
Video doorbell via IP camera	●	●	●	-
LAN interface	●	●	●	●
Wi-Fi interface	●	●	●	-
Remote firmware update	●	●	●	●
Power supply via PoE (802.3af)	●	●	●	●
Local power supply	●	●	●	●
Surface-mounted installation	●	●	●	●
Flush-mounted installation	●	●	●	-
Cavity wall installation	●	●	●	-
Desktop installation	●	●	●	-
Call lists	●	●	●	-
Send an emergency call (SOS)	●	●	●	●
Support for surveillance of outdoor stations or IP cameras.	●	●	●	-
Support induction loop	●	●	-	-
Leave an audio message	●	●	-	-
Blacklist	●	●	-	-

2.2.2 IP Touch 7

Device type

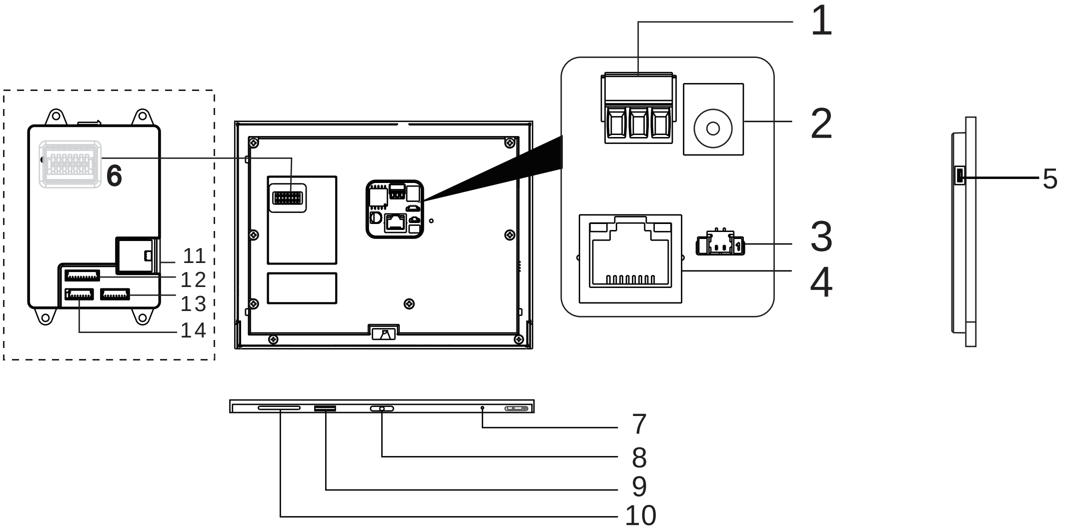
Article number	Order number	Product name	Colour	Size (WxHxD) Unit: mm
H8236-4W-03	2TMA130050W0066	IP Touch 7, DES+KNX+f@h+APP, LAN+WiFi, T-loop	White	199 x 150 x 17
H8236-4B-03	2TMA130050B0066	IP Touch 7, DES+KNX+f@h+APP, LAN+WiFi, T-loop	Black	199 x 150 x 17
H8236-5W-03	2TMA130050W0068	IP Touch 7, DES+KNX+f@h+APP, LAN+LAN, T-loop	White	199 x 150 x 31
H8236-5B-03	2TMA130050B0068	IP Touch 7, DES+KNX+f@h+APP, LAN+LAN, T-loop	Black	199 x 150 x 31

Control elements



No.	Description
1	Touch screen

Terminal description



No.	Description
1	Power input connector
2	Power input connector (DC-JACK input)
3	Doorbell connector
4	LAN1 (PoE)
5	Micro USB Upgrade connector
6	Extension module connector
7	Microphone
8	Dismantling switch
9	Micro SD card connector
10	Speaker
11	[2] LAN2
12	[2] Alarm connector
13	[2] RS485 connector, 12 V output, emergency port (SOS, GAS, fire)
14	[2] Relay output

[2] IP touch 7 (LAN+LAN)

Technical data

Designation	Value
Rating voltage	24 V ⎓
Operating voltage range	20-27 V ⎓
[1] Rating current	27 V ⎓, 250 mA 24 V ⎓, 280 mA
[2] Rating current	27 V ⎓, 390 mA 24 V ⎓, 440 mA
Display size	7"
Resolution	1024 x 600 px
Operating temperature	-10 °C … +55 °C
PoE standard	IEEE802.3 af
[2] Alarm power output	12 V ⎓, 200 mA
[2] Relay output	30 V ⎓, 1 A
[1] Wireless transmission band	802.11b/g/n: 2412...2462MHz (for United States) 2412...2472MHz (for European countries) 802.11a/n: 5150…5250MHz 5250…5350MHz 5470…5725MHz (not used in Russia) 5725…5850MHz (for United States)
[1] Wireless transmission power	Max. 20 dBm@12 Mbps OFDM 2.4 G Max. 20 dBm@12 Mbps OFDM 5.8 G
[1] Wireless transmission standard	IEEE 802.11 a/b/g/n

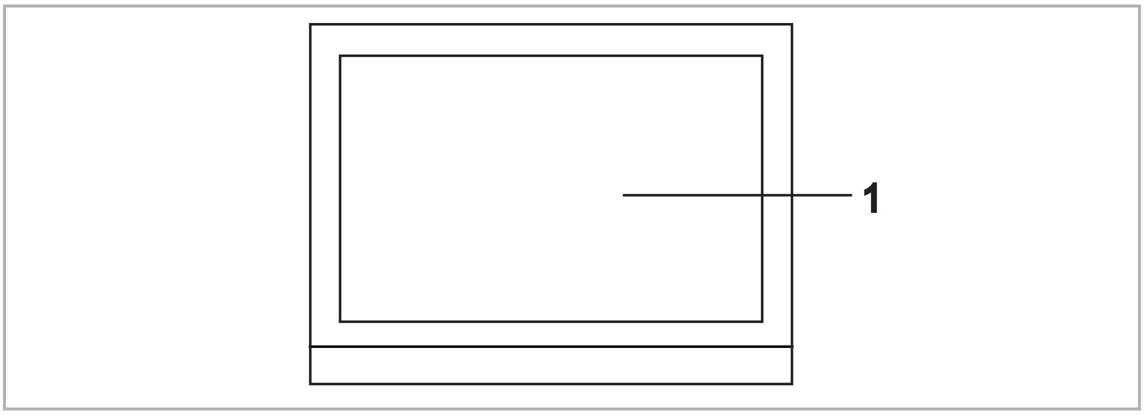
[1] IP touch 7 (LAN+WiFi) [2] IP touch 7 (LAN+LAN)

2.2.3 IP Touch 10

Device type

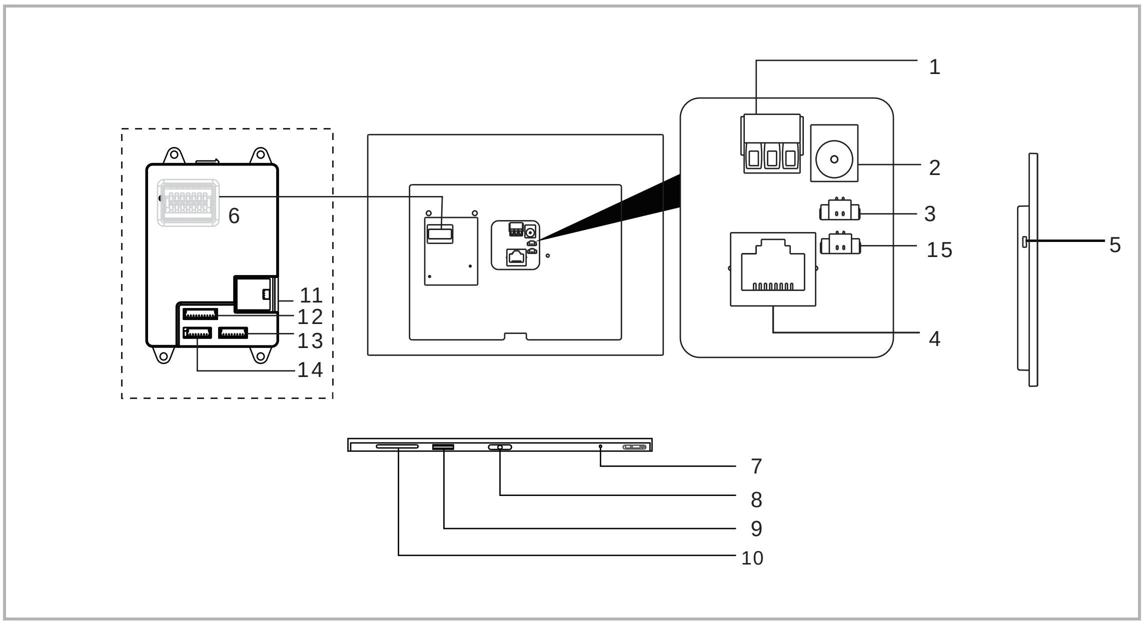
Article number	Order number	Product name	Colour	Size (WxHxD) Unit: mm
H8237-4W-03	2TMA130050W0058	IP Touch 10, DES+KNX+f@h+APP, LAN+WiFi, T-loop	White	251 x 185 x 17
H8237-4B-03	2TMA130050B0058	IP Touch 10, DES+KNX+f@h+APP, LAN+WiFi, T-loop	Black	251 x 185 x 17
H8237-5W-03	2TMA130050W0060	IP Touch 10, DES+KNX+f@h+APP, LAN+LAN, T-loop	White	251 x 185 x 31
H8237-5B-03	2TMA130050B0060	IP Touch 10, DES+KNX+f@h+APP, LAN+LAN, T-loop	Black	251 x 185 x 31

Control elements



No.	Description
1	Touch screen

Terminal description



No.	Description
1	Power input connector
2	Power input connector (DC-JACK input)
3	Doorbell connector
4	LAN1 (PoE)
5	Micro USB Upgrade connector
6	Interface module connector
7	Microphone
8	Dismantling switch
9	Micro SD card connector
10	Speaker
11	[2] LAN2
12	[2] Alarm connector
13	[2] RS485 connector, 12 V output (12 V output is not available when PoE powered)
14	[2] Relay output
15	N/A

[2] IP touch 10 (LAN+LAN)

Technical data

Designation	Value
Rating voltage	24 V ⎓
Operating voltage range	20-27 V ⎓
[1] Rating current	27 V ⎓, 390 mA 24 V ⎓, 440 mA
[2] Rating current	27 V ⎓, 520 mA 24 V ⎓, 600 mA
Display size	10"
Resolution	1280 x 800 px
Operating temperature	-10 °C … +55 °C
PoE standard	IEEE802.3 af
[2] Alarm power output	12 V ⎓, 200 mA (12 V output is not available when PoE powered)
[2] Relay output	30 V ⎓, 1 A
[1] Wireless transmission band	802.11b/g/n: 2412...2462MHz (for United States) 2412...2472MHz (for European countries) 802.11a/n: 5150…5250MHz 5250…5350MHz 5470…5725MHz (not used in Russia) 5725…5850MHz (for United States)
[1] Wireless transmission power	Max. 20 dBm@12 Mbps OFDM 2.4 G Max. 20 dBm@12 Mbps OFDM 5.8 G
[1] Wireless transmission standard	IEEE 802.11 a/b/g/n

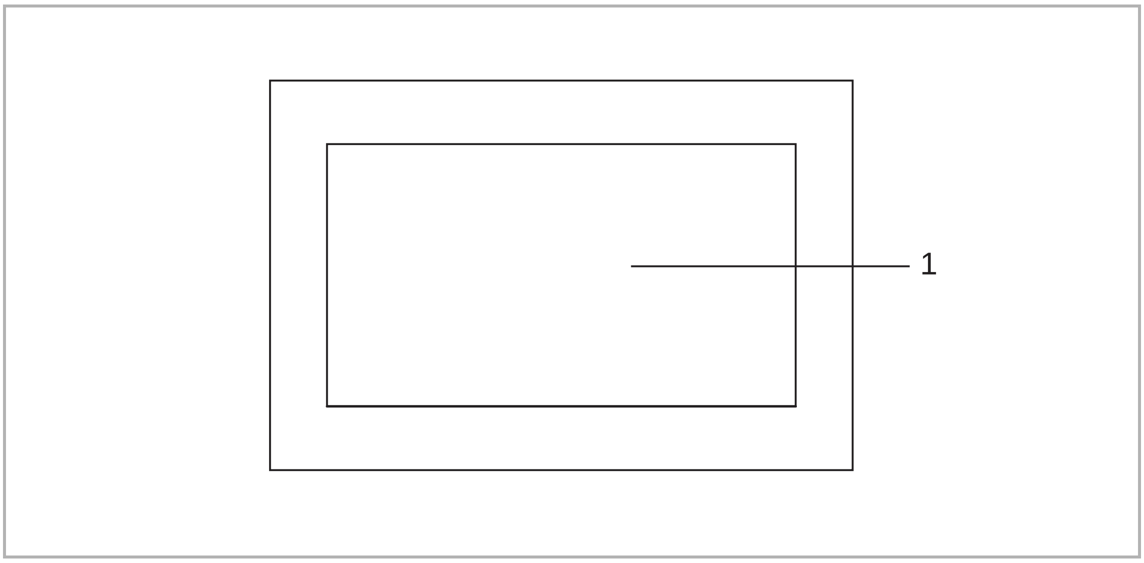
[1] IP touch 10 (LAN+WiFi) [2] IP touch 10 (LAN+LAN)

2.2.4 IP Touch Lite 7

Device type

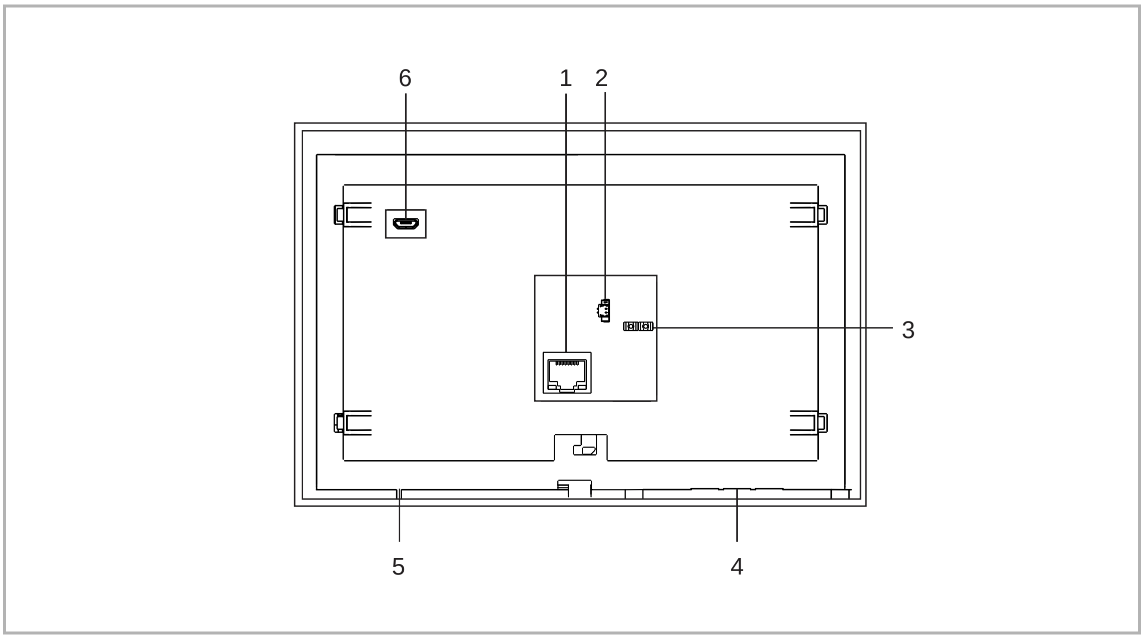
Article number	Order number	Product name	Colour	Size (WxHxD) Unit: mm
H8249-1W-03	2TMA130050W0069	IP Touch Lite 7, DES+APP, LAN+WiFi	White	192 x 128 x 17.2
H8249-1B-03	2TMA130050B0069	IP Touch Lite 7, DES+APP, LAN+WiFi	Black	192 x 128 x 17.2

Control elements



No.	Description
1	Touch screen

Terminal description



No.	Description
1	LAN1 (PoE)
2	Doorbell connector
3	Power input connector
4	Speaker
5	Microphone
6	Micro USB connector emergency engineering access

Technical data

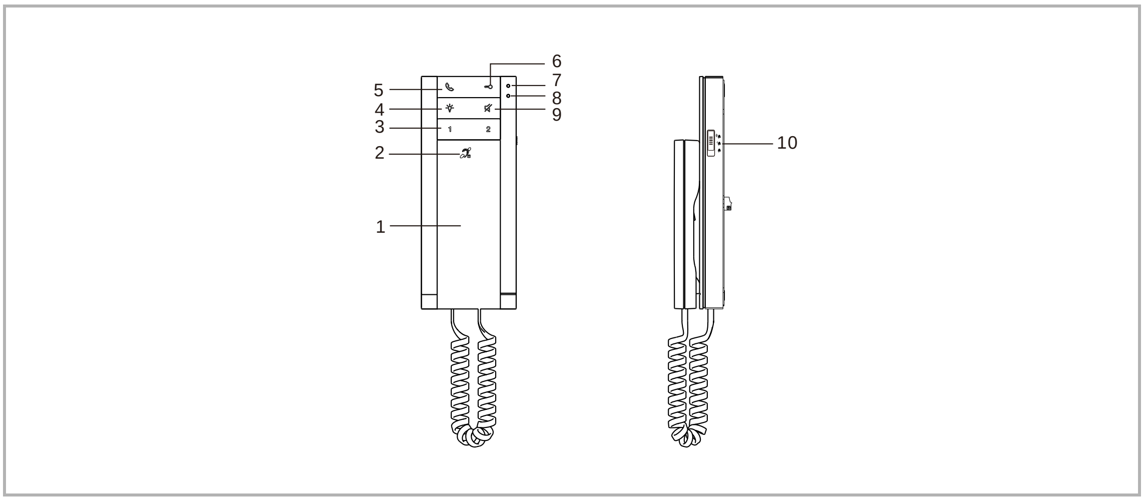
Designation	Value
Rating voltage	24 V ⎓
Operating voltage range	20-27 V ⎓
Rating current	24 V ⎓, 375 mA
Display size	7"
Resolution	1024 x 600 px
Operating temperature	0 °C … +45 °C
Storage temperature	-25 °C … +70 °C
PoE standard	IEEE802.3 af
Wireless transmission band	802.11b/g/n: 2412...2462MHz (for United States) 2412...2472MHz (for European countries) 802.11a/n/ac: 5150…5250MHz 5250…5350MHz 5470…5725MHz 5725…5850MHz (for United States)
Wireless transmission power	Max. 20 dBm
Wireless transmission standard	IEEE 802.11 a/b/g/n/ac
Diameter of the cable thickness (3)	1.0 mm...1.4 mm

2.2.5 Audio IP

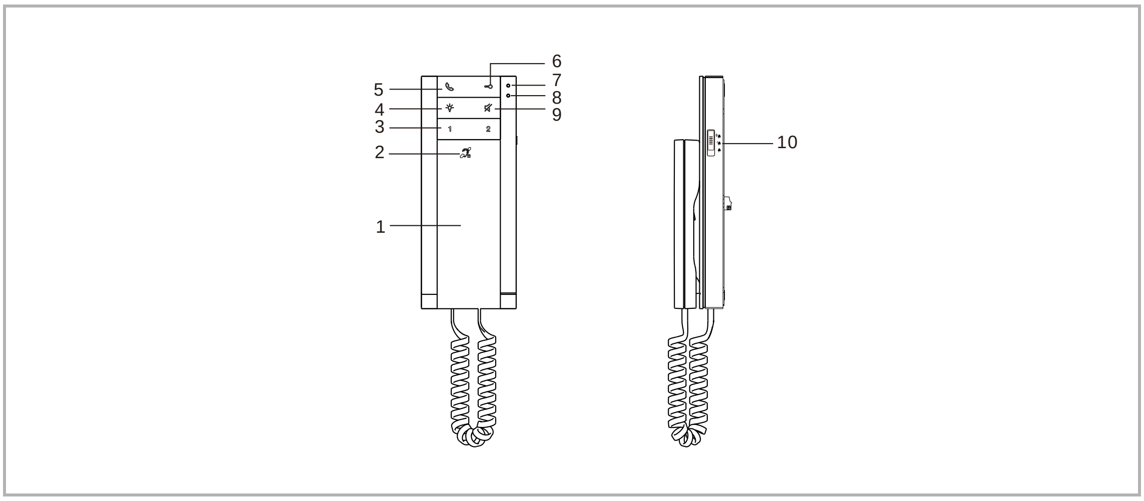
Device type

Article number	Order number	Product name	Colour	Size (WxHxD) Unit: mm
H82001-W-03	2TMA130010W0041	Audio IP, induction loop	White	81 x 198 x 43

Control elements



No.	Description
1	Handset ▪ During a call request, pick up the handset within 30 seconds to accept the call. ▪ During communication, hang up the handset to terminate the call.
2	**Induction Loop symbol** The device is equipped with a hearing loop for coupling the audio signal into hearing aids. ▪ To be able to use these hearing loops, the hearing aid must have what is known as a telephone coil (short: "T-coil") that records the magnetic alternating field of the hearing loop. ▪ The distance to the device should be a maximum of 80 cm for optimal reception.
3	**Programmable button** The button can be programmed on the SmartAP for the functions below: ▪ Intercom to same unit (default) ▪ Intercom to another unit ▪ Call guard unit ▪ Open door with Outdoor Station ▪ Open door with IP Actuator ▪ Turn on the designated light ▪ SOS function
4	**Light button** ▪ In standby status, press the button to turn on the designated light. ▪ In standby status, hold the button for 5 seconds to set the ringtone type. ▪ During communication, hold the button for 5 seconds to set the call volume.



No.	Description
5	**Call button** ▪ Pick up the handset in standby mode and press the button to communicate with other indoor stations within the same apartment (default setting). In doing so, all existing indoor stations within the apartment will be called simultaneously. In this case, the group call is stopped as soon as one of the indoor stations accepts the call. The button can be programmed on the SmartAP to Intercom to another unit or call guard unit.
6	**Unlock button** ▪ *In standby status, press the button to release the default lock of the default outdoor station. (A default outdoor station should be set on the SmartAP before use). ▪ In standby status, hold the button for 10 seconds to enable the "Automatic unlock" function. The LED (red) illuminates to indicate that the "Automatic unlock" function is enabled. The same operation will disable the "Automatic unlock" function and the LED (red) will turn off. * The "Automatic unlock" function means the door will be unlocked automatically during a call request. This function will be disabled automatically after 10 hours.
7	LED (red)
8	LED (blue)
9	**Mute button** ▪ In standby status, press the button to mute the ringtone. ▪ In standby status, hold the button for 3 seconds to mute the ringtone for all the indoor stations in the same apartment. ▪ During a call request, press the button to mute the ringtone. ▪ During communication, press the button to mute the microphone.
10	**Volume button** Adjust the three-level selector (maximum/medium/low) to set the ringtone volume.

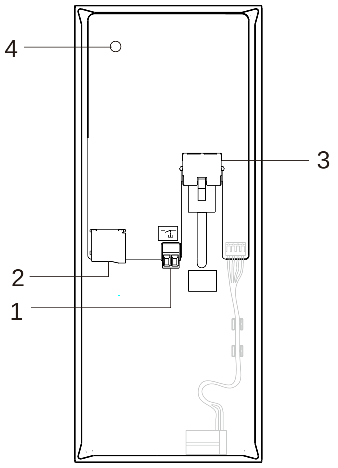
LED Overview

Icon	Description
🔴	Red LED always on
🔵	Blue LED always on
🔴✕	Red LED flashes slowly
🔵✕	Blue LED flashes slowly
🔴✳	Red LED flashes fast
🔵✳	Blue LED flashes fast

LED status

LED status	Description
🔴	"Auto-unlock" function is enabled.
🔵	Mute the speaker or the microphone.
🔴✕ & 🔵✕	Unsigned status or enters the setting mode.
🔵✕	During an incoming call.
🔴✳	Operation failed.
🔵✳	Operation success.
🔴✳ & 🔵✳	IP address conflicts or network connection is not working properly.
🔴✳ / 🔵✳	Two LEDs flash alternative, update the firmware.

Terminal description



No.	Description
1	A potential-free contact, such as a doorbell
2	Micro SD card slot (only for factory use)
3	LAN (PoE), PoE is the only power supply for this device
4	Reset button

Technical data

Designation	Value
Rating voltage	48 V ⎓
Operating voltage	38-57 V ⎓
Rating current	48 V ⎓, 40 mA
Operating temperature	-10 °C…+55 °C
Storage temperature	-25 °C…+70 °C
PoE standard	IEEE802.3 af
IP level	IP 30
Size (DxHxW)	81 x 198 x 43 mm

2.3 System devices

2.3.1 Smart Access Point

*"Smart Access Point" is usually abbreviated to "SmartAP".

The management software is installed on the SmartAP.

The SmartAP offers the access point for commissioning and managing the Welcome IP devices with a PC.

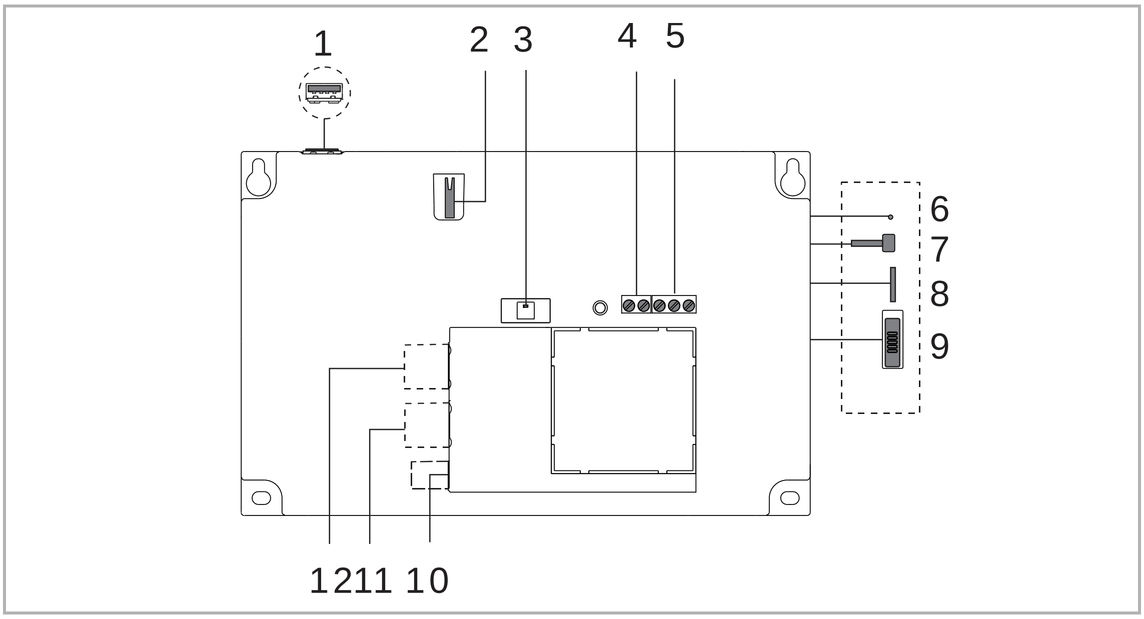
A total of 1200 devices can be supported by the SmartAP.

For opening the Web-based user interface of the SmartAP, you need a computer with a LAN or WLAN network adaptor and an installed Internet browser.

Device type

Article number	Product ID	Product name	Colour	Size (WxHxD) Unit: mm
D04011-03	2TMA400260W0008	SmartAP Pro	White	204 x 32 x 132

Terminal description



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

[1] Status indicator LED

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

Technical data

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

Bluetooth data

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

2.3.2 Guard Unit

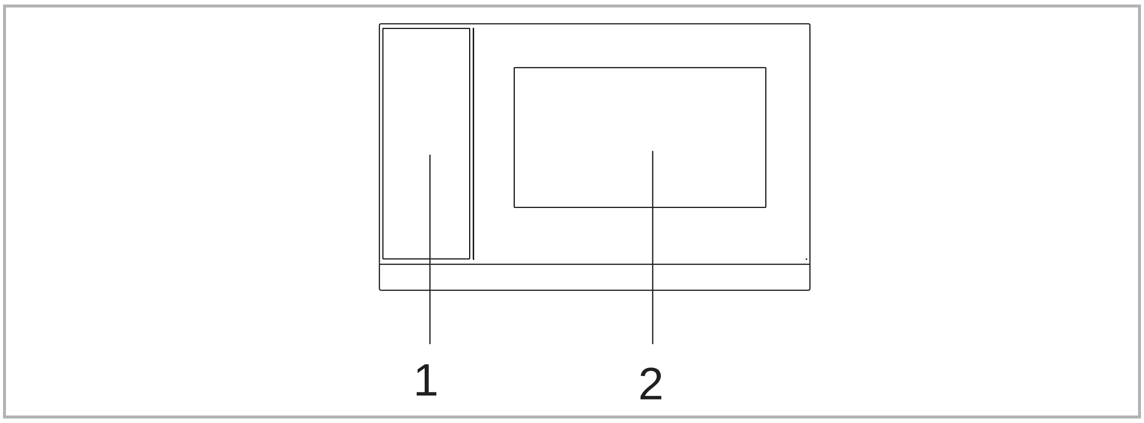
For the Guard Unit a similar range of functions is available as for the Indoor Station. The concierge can transfer the call to an Indoor Station or assign the access authorisation himself. The ABB-Welcome® App function and Smart Home are not possible for the concierge station.

Device type

Article number	Product ID	Product name	Colour	Size (WxHxD) Unit: mm
H8303-03	2TMA130160W0022	Guard Unit	White	265 x 165 x 117

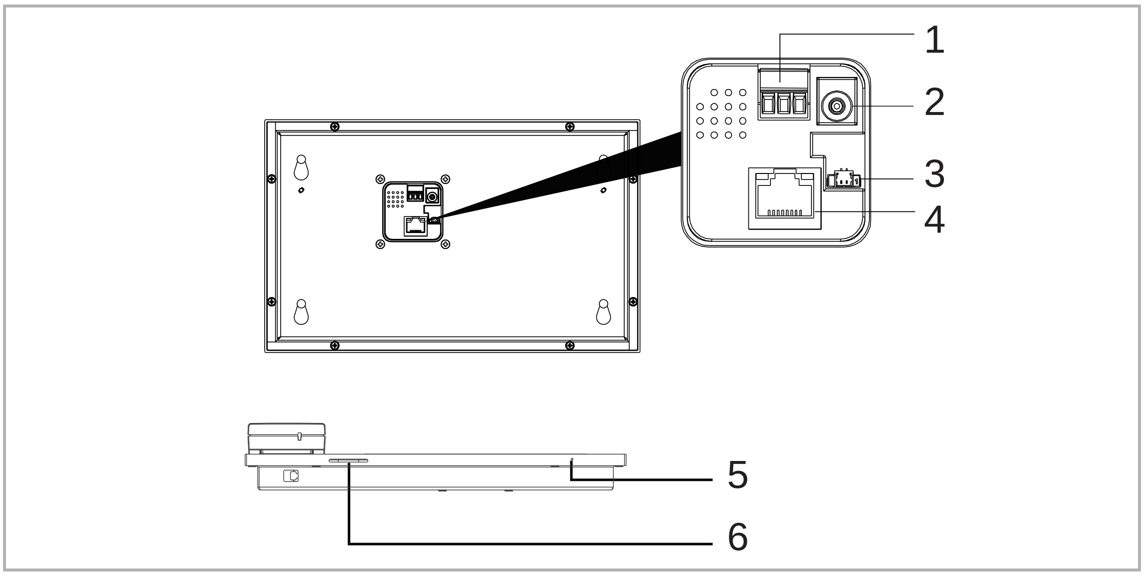
*"Guard Unit" is usually abbreviated to "GU".

Control elements



No.	Description
1	Handset
2	Touch screen

Terminal description



No.	Description
1	Power input connector
2	Power input connector (DC-JACK input)
3	Fire control input (release all the locks in case of emergency)
4	LAN (PoE)
5	Microphone
6	Speaker

Technical data

Designation	Value
Rating voltage	24 V DC
Operating voltage range	20-27 V DC
Rating current	27 V DC, 230 mA 24 V DC, 260 mA
Display size	7"
Resolution	1024 x 600 pixel
Product dimensions	265 mm × 165 mm × 115 mm
Operating temperature	-10 °C…+55 °C
PoE standard	IEEE802.3 af
Network connection standard	IEEE 802.3, 10Base-T/100Base-TX, auto MDI/MDI-X

2.3.3 IP Actuator

The "IP actuator" connects the door openers or the lighting, it carries out the switching commands.

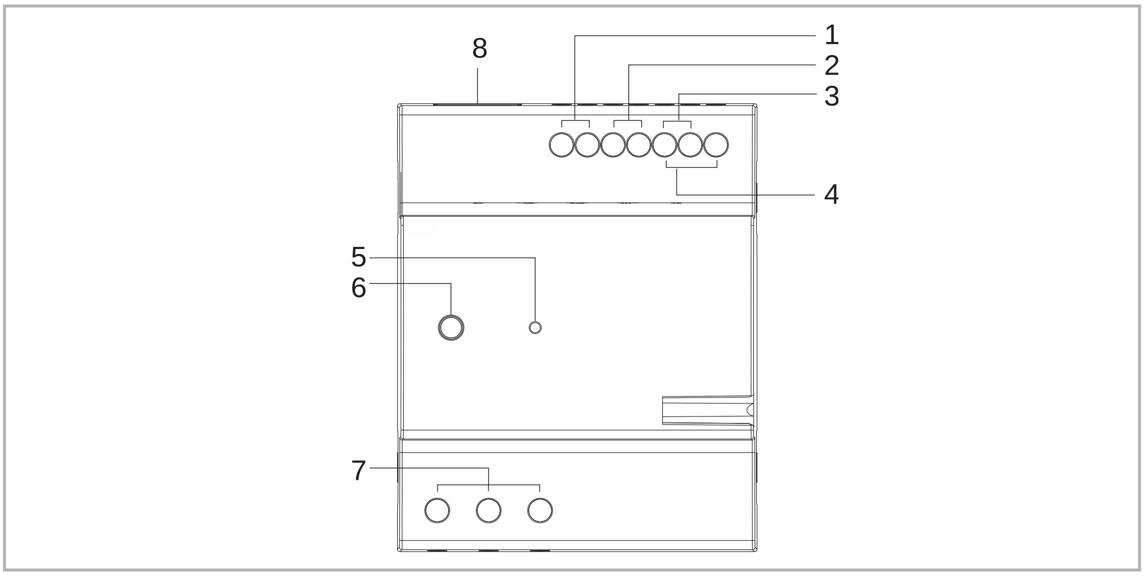
The settings e.g. the switching duration of the lock release or the switching on of the lighting can be made via the "Indoor Station" or the SmartAP.

Device type

Article number	Product ID	Product name	Colour	Size (WxHxD) Unit: mm
H8304-03	2TMA130160H0061	IP Actuator	Grey	65 x 72 x 90

*"IP Actuator" is usually abbreviated to "IPA".

Terminal description



No.	Description
1	System power supply connector
2	Plug-in clamps (LOCK+…LOCK-) for door opener
3	Connector for sensor used for door status detection
4	Connector for exit push-button
5	Reset button
6	Status indicator
7	Plug-in clamps (NC…COM...NO) for floating output, door opener
8	LAN (PoE)

Technical data

Designation	Value
Rating voltage	24 V ⎓
Operating voltage range	20-27 V ⎓
Rating current	27 V ⎓, 310 mA 24 V ⎓, 350 mA
Operating temperature	-25 °C…+55 °C
Power supply for door opener	DC: 12 V ⎓, 4 A impulse, max. 500 mA holding AC: 12 V ~, 50 Hz, max. 500 mA holding
Signal unlocking	230 V ~, 3 A
Network connection standard	IEEE802.3, 10/100 Mbps, auto MDI/MDI-X

2.3.4 IP Elevator Controller & Lift Control Relay Module

The "IP Elevator Controller" & "Lift Control Relay Module" together ensure that elevator only goes to authorised floor(s).

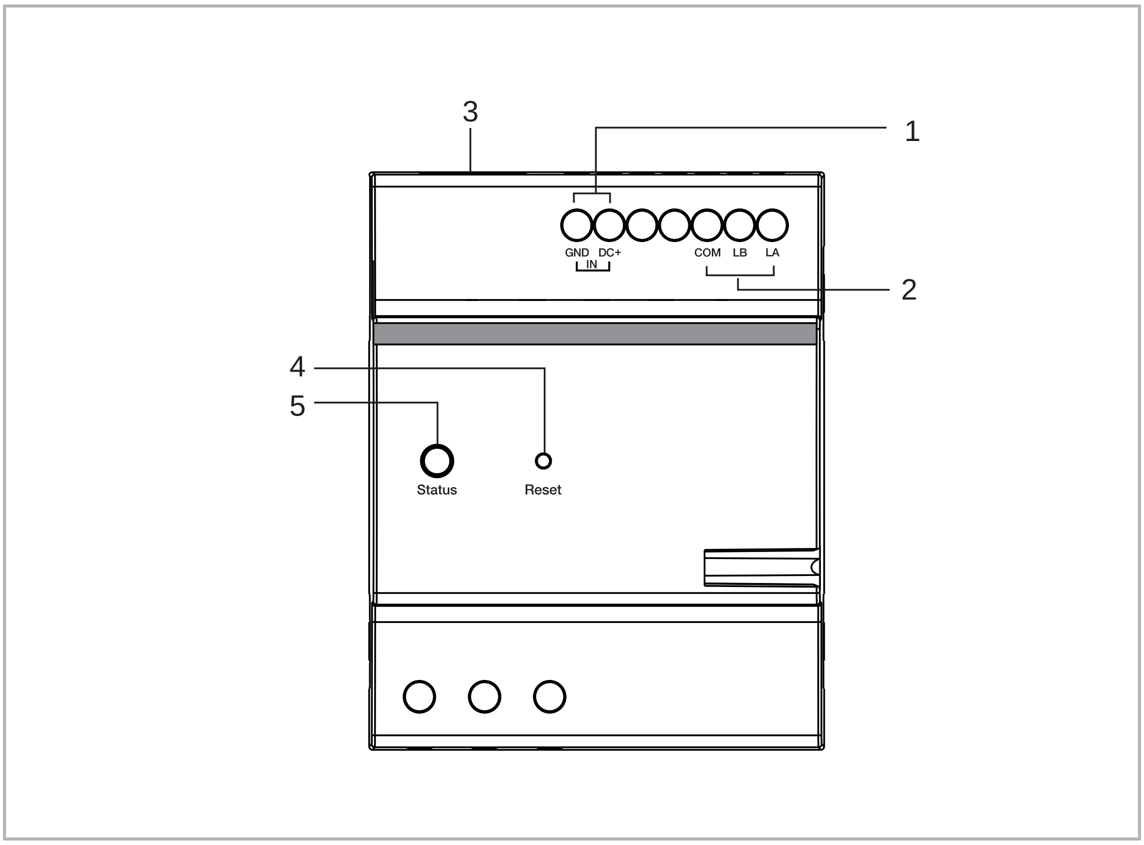
If a resident presses the "unlock" button when receiving a guest's call from the outdoor station, or the authorised user swipes the registered card or enters correct password, the elevator will automatically go down to the floor where the outdoor station is installed. The elevator will then go to the dedicated floor where the resident lives. It cannot go to unauthorised floors, even when other buttons are pressed.

The configuration could be done via the SmartAP.

Device type

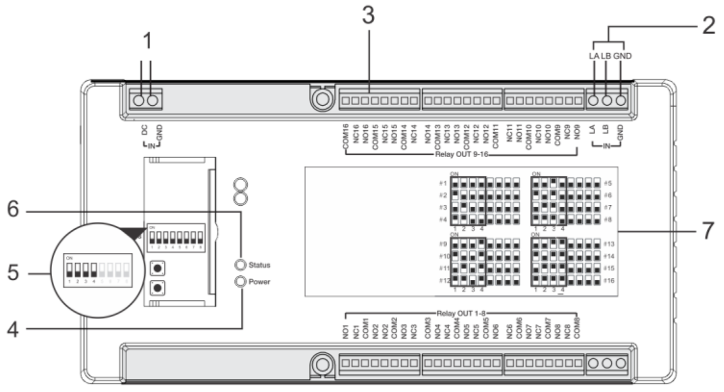
Article number	Product ID	Product name	Colour	Size (WxHxD) Unit: mm
H8308-03	2TMA130160W0042	IP Elevator Controller	Grey	65 x 72 x 90
M2307-03	2TMA130160H0091	Lift Control Relay Module	Grey	216 x 45 x 110

Terminal description - IP Elevator Controller



No.	Description
1	System power supply connector
2	RS485 connector
3	LAN (PoE)
4	**Reset button** Within 2 minutes of powering on the device, press and hold this button for 10 seconds to restore the device to the factory defaults. The status indicator will go off for 3 seconds then start to flash slowly.
5	**Status indicator** ▪ On: the device is working normally ▪ Off: the device is not powered on ▪ Flashing quickly: the device is working abnormally (e.g. IP conflict, no MAC address) ▪ Flashing slowly: the device has not obtained the signature

Terminal description - Lift Control Relay Module


1
2
3
4
5
6
7
LA LB GND
DC
GND
IN
COM16 NC16 NO16 COM15 NC15 NO15 COM14 NC14 NO14 COM13 NC13 NO13 COM12 NC12 NO12 COM11 NC11 NO11 COM10 NC10 NO10 COM9 NC9 NO9
Relay OUT 9-16
LA
LB
GND
IN
ON
Status
Power
#1 #2 #3 #4 #5 #6 #7 #8 #9 #10 #11 #12 #13 #14 #15 #16
Relay OUT 1-8
NO1 NC1 COM1 NO2 NC2 COM2 NO3 NC3 COM3 NO4 NC4 COM4 NO5 NC5 COM5 NO6 NC6 COM6 NO7 NC7 COM7 NO8 NC8 COM8

No.	Description
1	Power supply connector
2	Elevator control module connector
3	**Relay output** Connect to the elevator keyboard
4	Power LED
5	**Module address** The module address can be set to 1-16 (only the left 4 bits are used).
6	**Status LED** Blinks when working normally
7	**Product label** All 16 module address settings are displayed on the label.

Technical data - IP Elevator Controller

Designation	Value
Rating voltage	24 V ⎓
Operating voltage range	20-27 V ⎓
Rating current	24 V ⎓, 60 mA
Operating temperature	-20 °C…+55 °C
Storage temperature	-20 °C…+70 °C
PoE standard	IEEE802.3 af

Technical data - Lift Control Relay Module

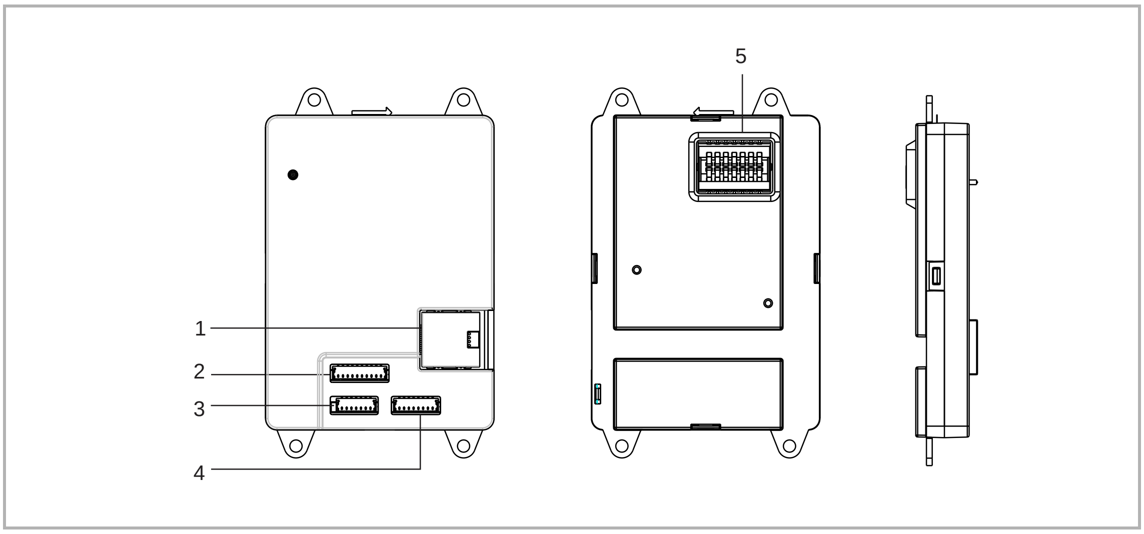
Designation	Value
Rating voltage	24 V ⎓
Operating voltage range	20-27 V ⎓
Rating current	24 V ⎓, 250 mA
Operating temperature	-20 °C…+55 °C
Storage temperature	-20 °C…+70 °C

2.3.5 Interface module

Device type

Article number	Order number	Product name	Colour	Size (WxHxD) Unit: mm
52361EX-03	2TMA130160B0138	Interface Module	-	16.5 x 60 x 82

Terminal description



No.	Description
1	LAN2
2	Alarm input
3	Relay out *2
4	RS485 connector, 12 V output, emergency port (SOS, GAS, FIRE)
5	Connector for IP touch

Technical data

Designation	Value
Rating voltage	24 V ⎓
Operating voltage range	20-27 V ⎓
Rating current	27 V ⎓, 150 mA 24 V ⎓, 170 mA
Operating temperature	-10 °C…+55 °C
Power supply output	12 V ⎓, 200 mA
Relay output	24 V ⎓, 1 A

2.3.6 Power Supply

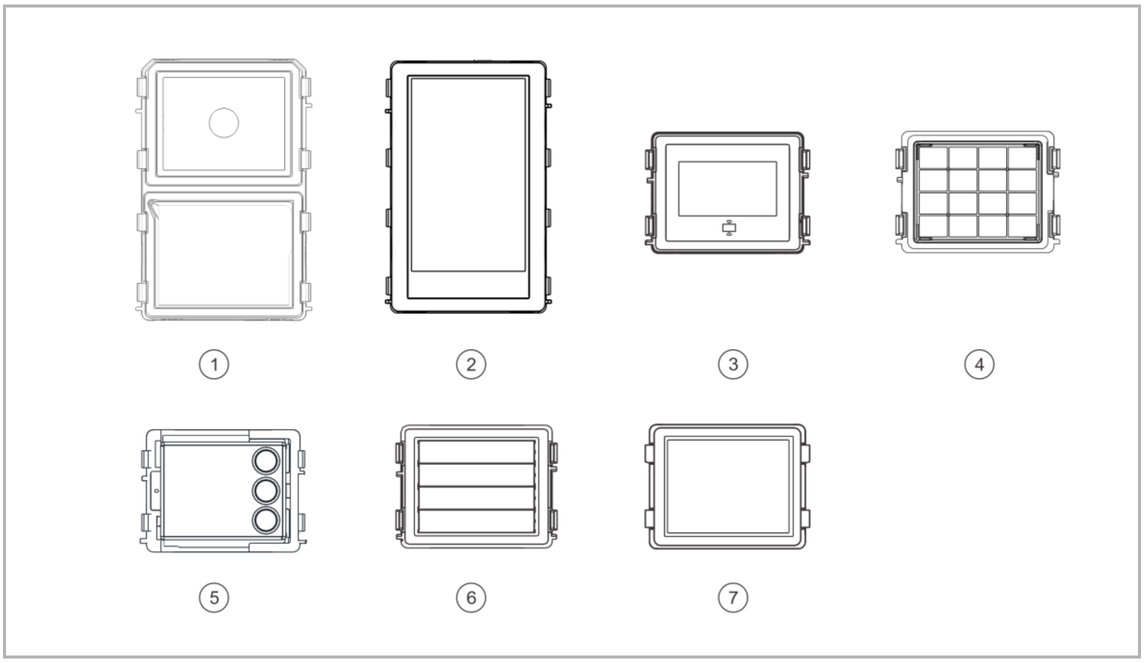
Power supply supplies the power for the devices on the system.

Device type

Article number	Product ID	Product name	Colour	Size (WxHxD) Unit: mm
53011PS-03	2TMA130160W0029	Power Adaptor 24VDC		43.8 x 85 x 79

2.4 Outdoor Station Modules

2.4.1 Overview



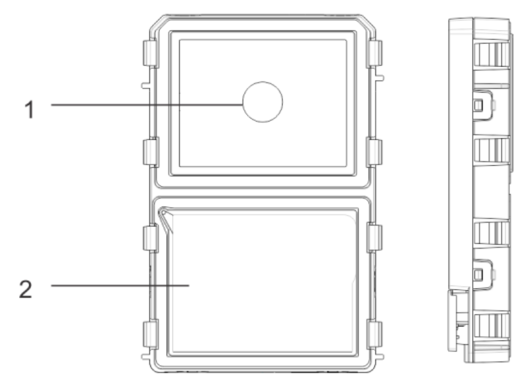
No.	Article number	Product name
1	H85138.M-S-03	A/V Module
2	H85138.DP-03	Touch 5" Module
3	5138.CR-03	Display Module
4	5138.K-.-03	Keypad Module
5	5138.RP. -03	Round Pushbutton Module
6	5138.SP. -03	Bar Pushbutton Module
7	51381DN-03	Info Module

2.4.2 A/V Module

Device type

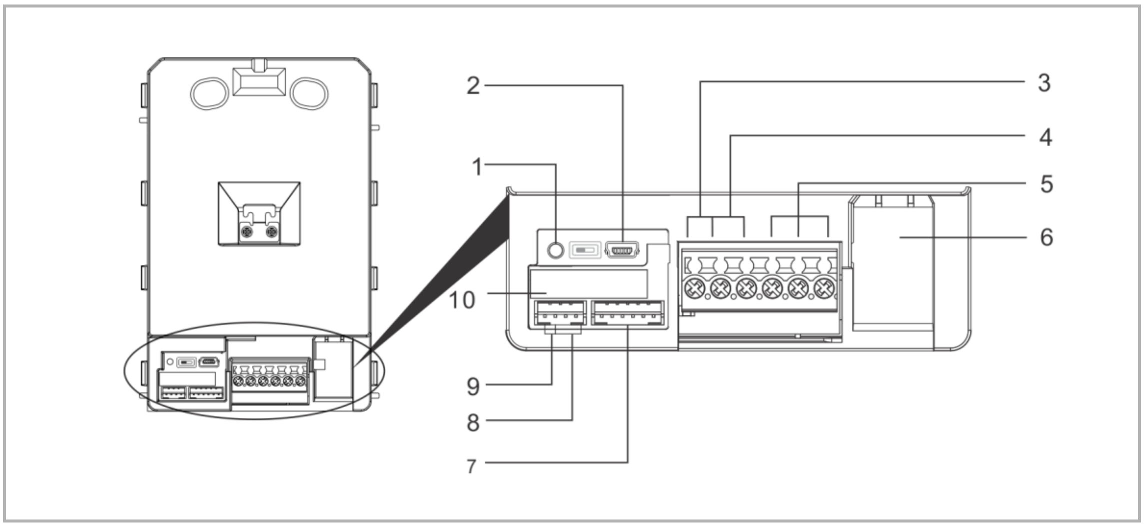
Article number	Order number	Product name	Colour	Size (WxHxD) Unit: mm
H851381M-S-03	2TMA130160B0090	A/V Module	-	96 x 143 x 28

Control elements



No.	Description
1	Camera
2	Speaker and microphone

Terminal description



No.	Description
1	Reset button
2	Micro USB update connector
3	Plug-in clamps (DC+...GND) for standalone power supply
4	Plug-in clamps (LOCK...GND) for door opener
5	Plug-in clamps (COM...NC...NO) for floating output
6	Network connector (PoE)
7	Connector for next module
8	Connector for exit button
9	Connector for the sensor used for door status detection
10	Connector for big display module

Technical data

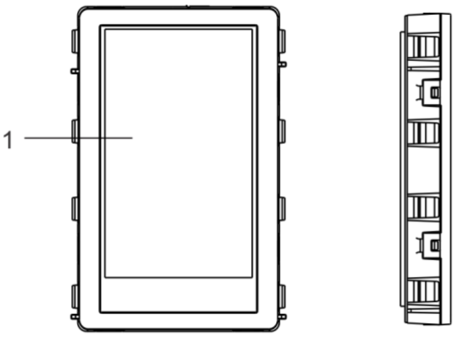
Designation	Value
Rating voltage	24 V ⎓
Operating voltage range	20-27 V ⎓
Rating current	27 V ⎓, 290 mA 24 V ⎓, 320 mA
Operating temperature	-40 °C…+55 °C
Camera type	CMOS
Camera viewing angle	130°
Resolution	HD (1280 x 720 pixel)
Power supply for door opener	18 V ⎓, 4 A impulse, max. 250 mA holding
Floating output for door opener	230 V ~, 3 A 30 V ⎓, 3 A
Video codec	H.264
Audio codec	G.711

2.4.3 Touch 5" Module

Device type

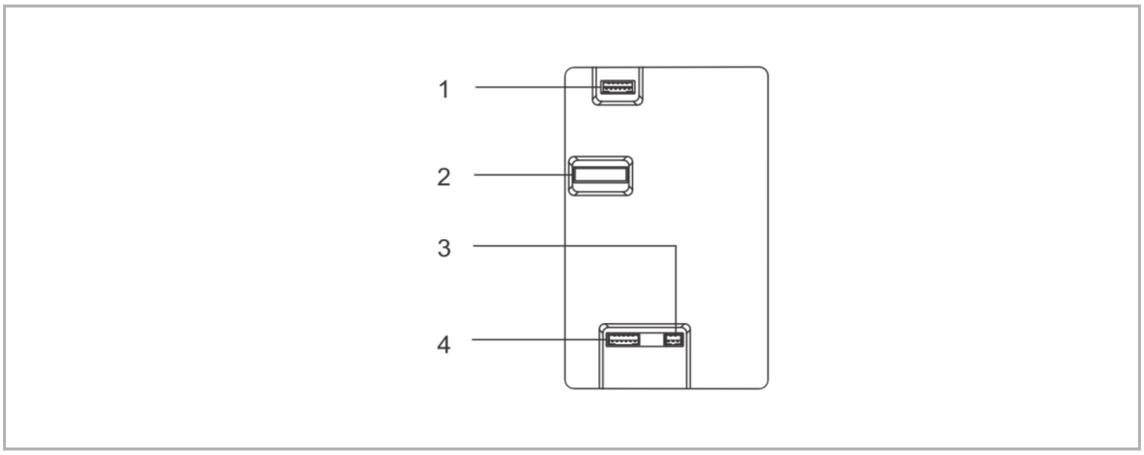
Article number	Order number	Product name	Colour	Size (WxHxD) Unit: mm
H851381DP-03	2TMA130160B0091	Touch 5" Module	-	96 x 143 x 23

Control elements



No.	Description
1	Touch screen

Terminal description



No.	Description
1	Connector for previous module
2	Connector for A/V module
3	Connector for Wiegand output It supports 26 bits and 34 bits
4	Connector for next module

Technical data

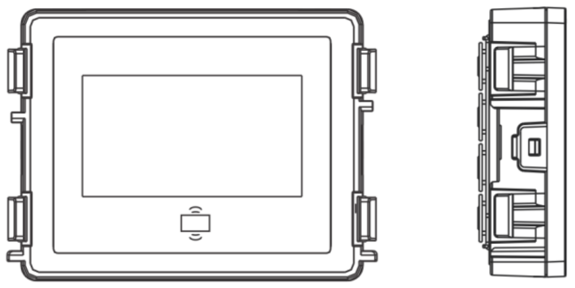
Designation	Value
Rating voltage	24 V ⎓
Operating voltage range	20-27 V ⎓
Rating current	27 V ⎓, 120 mA 24 V ⎓, 130 mA
Operating temperature	-20 °C…+55 °C
Ambient brightness	<50000 Lux
Frequency range	13.56MHz
Maximum power	≤-0.2 dBμA/m @ 3m

2.4.4 Display Module

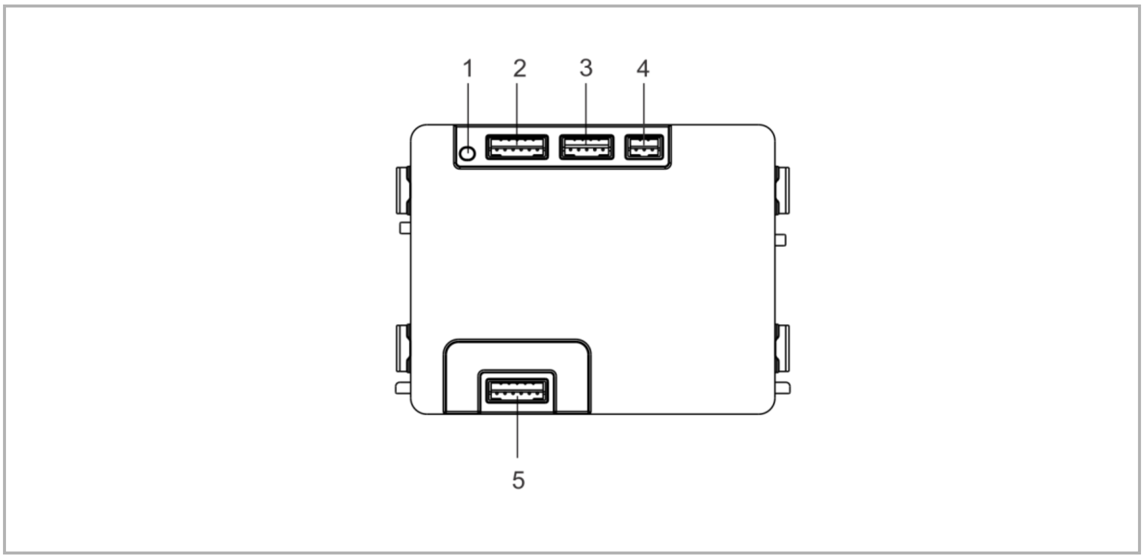
Device type

Article number	Order number	Product name	Colour	Size (WxHxD) Unit: mm
51381CR-03	2TMA130160N0030	Display Module, ID	-	97 x 72 x 25
51382CR-03	2TMA130160N0029	Display Module, Desfire/IC	-	97 x 72 x 25

Control elements



Terminal description



No.	Description
1	Program button
2	Connector for previous module
3	Connector for device software update
4	Connector for Wiegand output It supports 26 bits and 34 bits
5	Connector for next module

Technical data

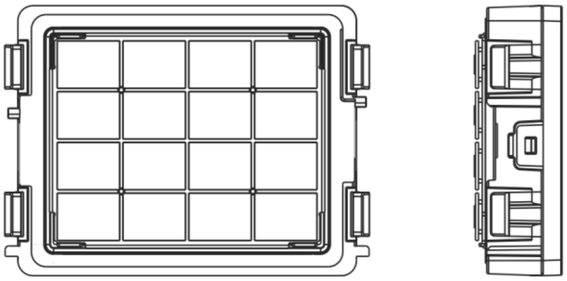
Designation	Value
Rating voltage	24 V ⎓
Operating voltage range	20-27 V ⎓
Rating current	27 V ⎓, 145 mA 24 V ⎓, 160 mA
Operating temperature	-40 °C…+55 °C
Frequency range (ID)	125KHz
Maximum power (ID)	≤-3.19 dBµA/m @ 3m
Frequency range (IC)	13.56MHz
Maximum power (IC)	≤-4.75 dBµA/m @ 3m

2.4.5 Keypad Module

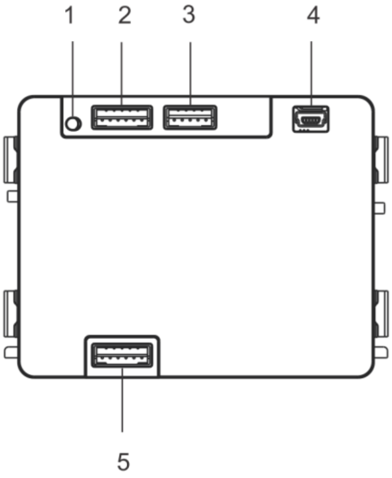
Device type

Article number	Order number	Product name	Colour	Size (WxHxD) Unit: mm
51381K-S-03	2TMA130160X0023	Keypad Module	Stainless steel	97 x 72 x 25
51381K-W-03	2TMA130010W0018	Keypad Module	White	97 x 72 x 25

Control elements



Terminal description



No.	Description
1	Program button
2	Connector for previous module
3	Connector for device software update (can only be done at the factory)
4	Micro USB update connector
5	Connector for next module

Technical data

Designation	Value
Rating voltage	24 V ⎓
Operating voltage range	20-27 V ⎓
Rating current	27 V ⎓, 20 mA 24 V ⎓, 20 mA
Operating temperature	-40 °C…+55 °C

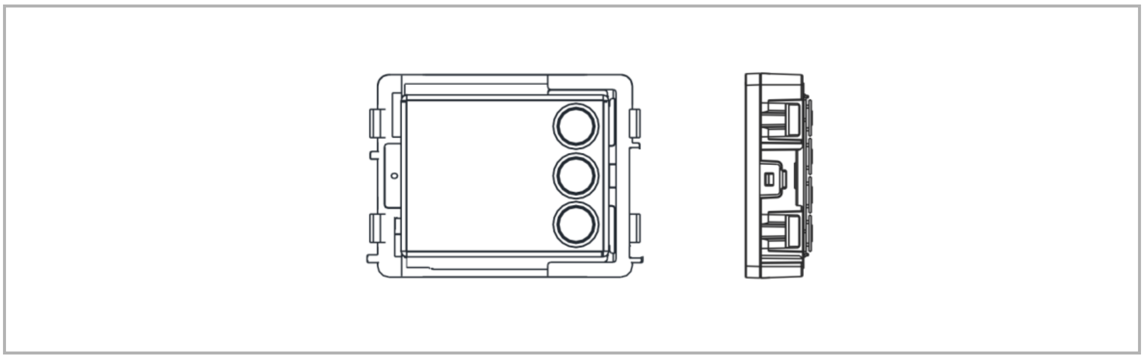
2.4.6 Round Pushbutton Module

Device type

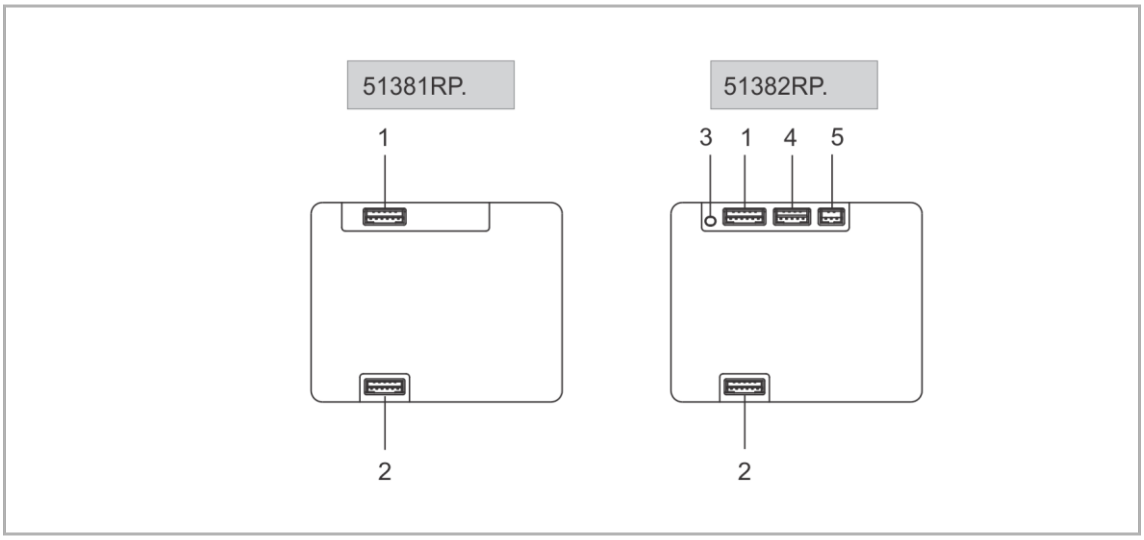
Article number	Order number	Product name	Colour	Size (WxHxD) Unit: mm
51381RP1-03	2TMA130160N0023	Round Pushbutton Module, 1 button	-	97 x 72 x 25
51381RP2-03	2TMA130160N0024	Round Pushbutton Module, 2 button	-	97 x 72 x 25
51381RP3-03	2TMA130160N0025	Round Pushbutton Module, 3 button	-	97 x 72 x 25

Article number	Order number	Product name	Colour	Size (WxHxD) Unit: mm
51382RP1-03	2TMA130160N0026	Round Pushbutton Module, 1 button, Desfire/IC	-	97 x 72 x 25
51382RP2-03	2TMA130160N0027	Round Pushbutton Module, 2 button, Desfire/IC	-	97 x 72 x 25
51382RP3-03	2TMA130160N0028	Round Pushbutton Module, 3 button, Desfire/IC	-	97 x 72 x 25

Control elements



Terminal description



No.	Description
1	Connector for previous module
2	Connector for next module
3	Program button
4	Connector for device software update
5	[2] Connector for Wiegand output It supports 26 bits and 34 bits

[2] 51382RP

Technical data

Designation	Value
Rating voltage	24 V ⎓
Operating voltage range	20-27 V ⎓
1 Rating current	27 V ⎓, 10 mA 24 V ⎓, 10 mA
2 Rating current	27 V ⎓, 35 mA 24 V ⎓, 40 mA
Operating temperature	-40 °C…+55 °C
2 Frequency range	13.56MHz
2 Maximum power	≤0 dBμA/m @ 3m

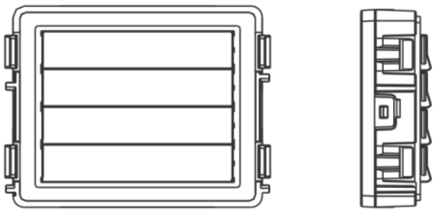
[1] 51381RP. [2] 51382RP.

2.4.7 Bar Pushbutton Module

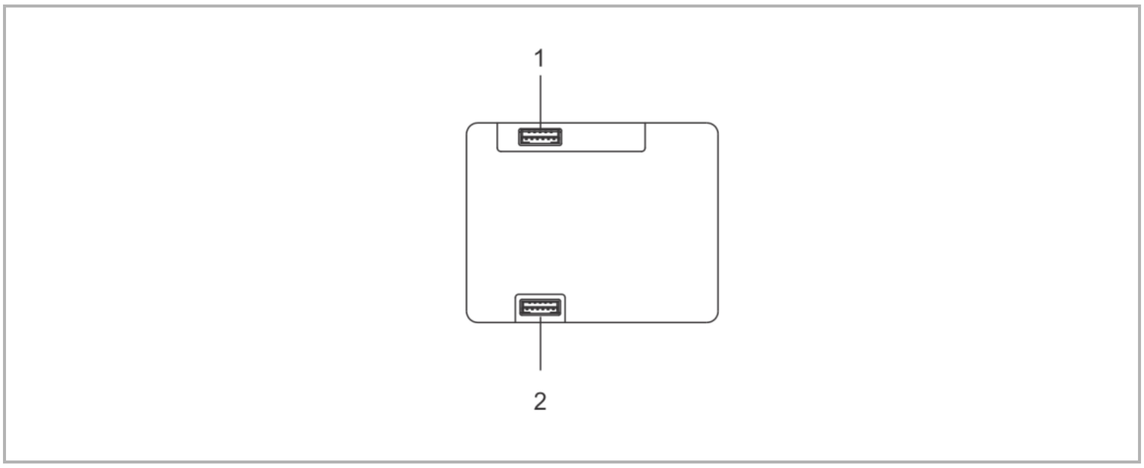
Device type

Article number	Order number	Product name	Colour	Size (WxHxD) Unit: mm
51381SP3-03	2TMA130160N0021	Bar Pushbutton Module, 3/6 buttons	-	97 x 72 x 25
51381SP4-03	2TMA130160N0022	Bar Pushbutton Module, 4/8 buttons	-	97 x 72 x 25

Control elements



Terminal description



No.	Description
1	Connector for previous module
2	Connector for next module

Technical data

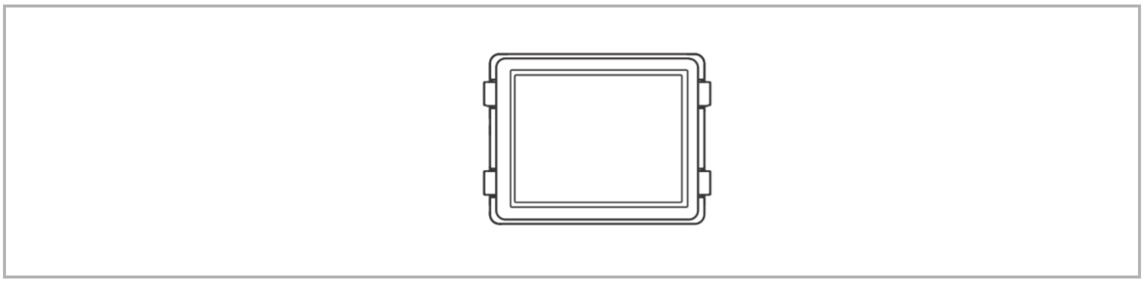
Designation	Value
Rating voltage	24 V ⎓
Operating voltage range	20-27 V ⎓
Rating current	27 V ⎓, 8 mA 24 V ⎓, 8 mA
Operating temperature	-40 °C…+55 °C

2.4.8 Info Module

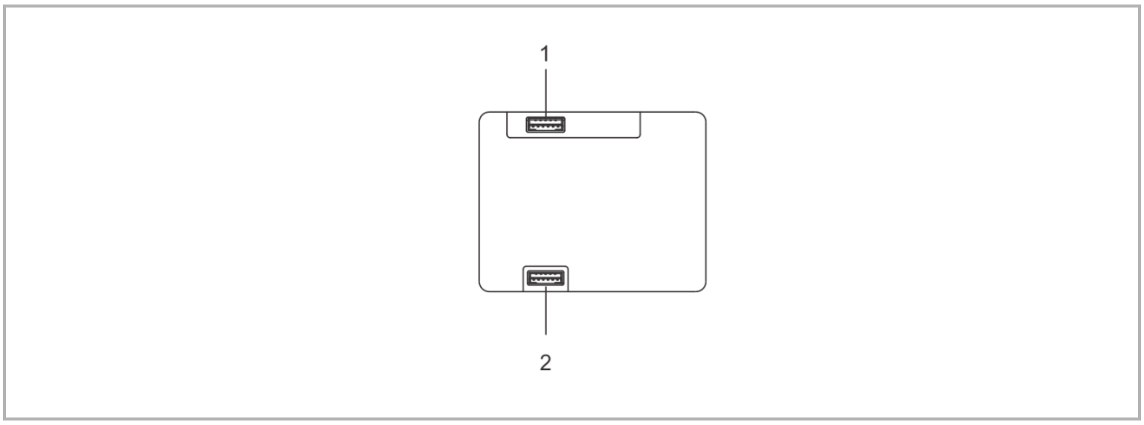
Device type

Article number	Order number	Product name	Colour	Size (WxHxD) Unit: mm
51381DN-03	2TMA200160N0038	Info Module	-	97 x 72 x 25

Control elements



Terminal description



No.	Description
1	Connector for previous module
2	Connector for next module

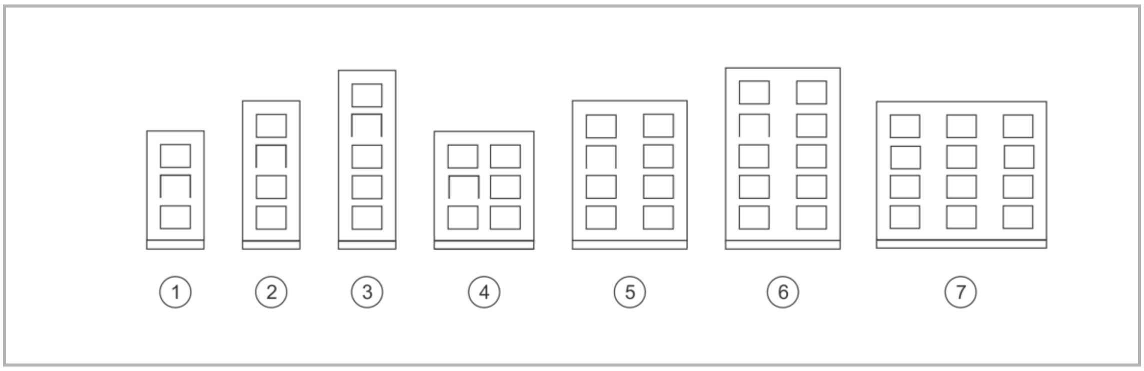
Technical data

Designation	Value
Rating voltage	24 V ⎓
Operating voltage range	20-27 V ⎓
Rating current	27 V ⎓, 8 mA 24 V ⎓, 8 mA
Operating temperature	-40 °C…+55 °C

2.5 Installation materials

2.5.1 Video Outdoor Station frame

Overview



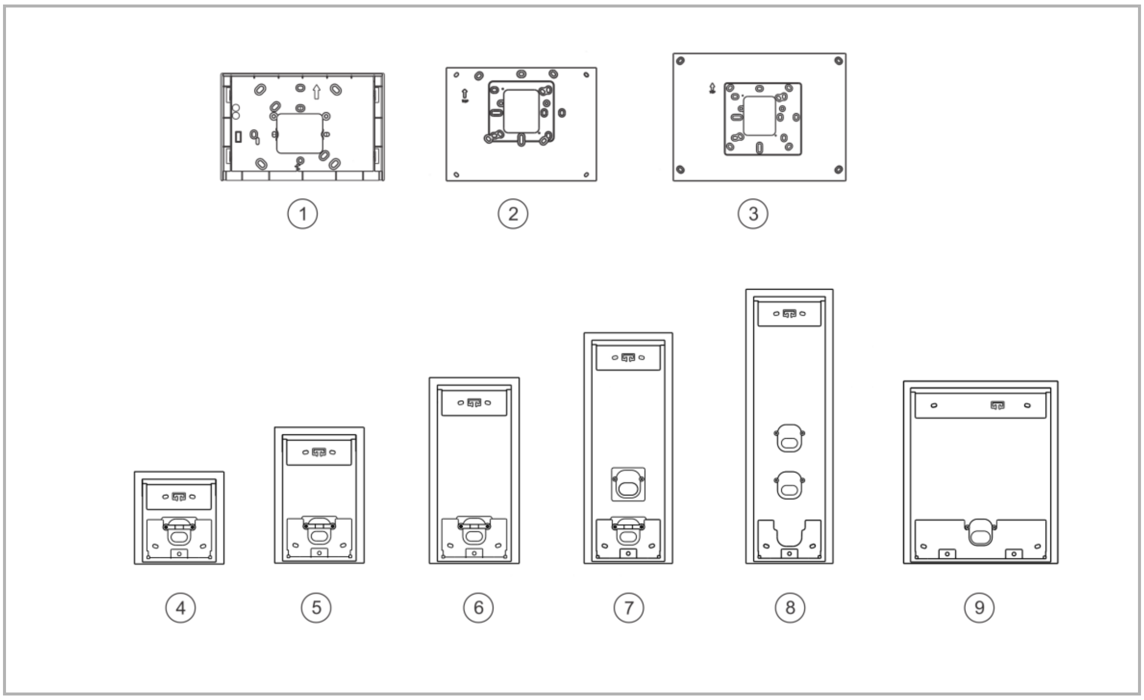
No.	Article number	Product name
1	41383CF-.-03	Video OS frame, size 1/3
2	41384CF-.-03	Video OS frame, size 1/4
3	41385CF-.-03	Video OS frame, size 1/5
4	41386CF-.-03	Video OS frame, size 2/3
5	41388CF-.-03	Video OS frame, size 2/4
6	413810CF-.-03	Video OS frame, size 2/5
7	413812CF-.-03	Video OS frame, size 3/4

Device type

Article number	Order number	Product name	Colour	Size (WxHxD) Unit: mm
41383CF-A-03	2TMA200160A0003	Video OS frame, size 1/3	Aluminium	135 x 277 x 20.5
41384CF-A-03	2TMA200160A0005	Video OS frame, size 1/4	Aluminium	135 x 349 x 20.5
41385CF-A-03	2TMA200160A0007	Video OS frame, size 1/5	Aluminium	135 x 421 x 20.5
41386CF-A-03	2TMA200160A0009	Video OS frame, size 2/3	Aluminium	235 x 277 x 20.5
41388CF-A-03	2TMA220161A0010	Video OS frame, size 2/4	Aluminium	235 x 349 x 20.5
413810CF-A-03	2TMA220161A0011	Video OS frame, size 2/5	Aluminium	235 x 421 x 20.5
413812CF-A-03	2TMA220160A0010	Video OS frame, size 3/4	Aluminium	407 x 349 x 20.5
41383CF-B-03	2TMA220160B1004	Video OS frame, size 1/3	Anthracite	135 x 277 x 20.5
41384CF-B-03	2TMA220160B1005	Video OS frame, size 1/4	Anthracite	135 x 349 x 20.5
41385CF-B-03	2TMA220160B1006	Video OS frame, size 1/5	Anthracite	135 x 421 x 20.5
41383CF-S-03	2TMA130160X0026	Video OS frame, size 1/3	Stainless steel	135 x 277 x 20.5
41384CF-S-03	2TMA130160X0027	Video OS frame, size 1/4	Stainless steel	135 x 349 x 20.5
41385CF-S-03	2TMA130160X0028	Video OS frame, size 1/5	Stainless steel	135 x 421 x 20.5
41386CF-S-03	2TMA130160X0029	Video OS frame, size 2/3	Stainless steel	235 x 277 x 20.5
41383CF-W-03	2TMA130160W0002	Video OS frame, size 1/3	2TMA130160W0010	135 x 277 x 20.5
41384CF-W-03	2TMA130160W0003	Video OS frame, size 1/4	2TMA130160W0011	135 x 349 x 20.5
41385CF-W-03	2TMA130160W0004	Video OS frame, size 1/5	2TMA130160W0012	135 x 421 x 20.5

2.5.2 Surface-mounted box

Overview



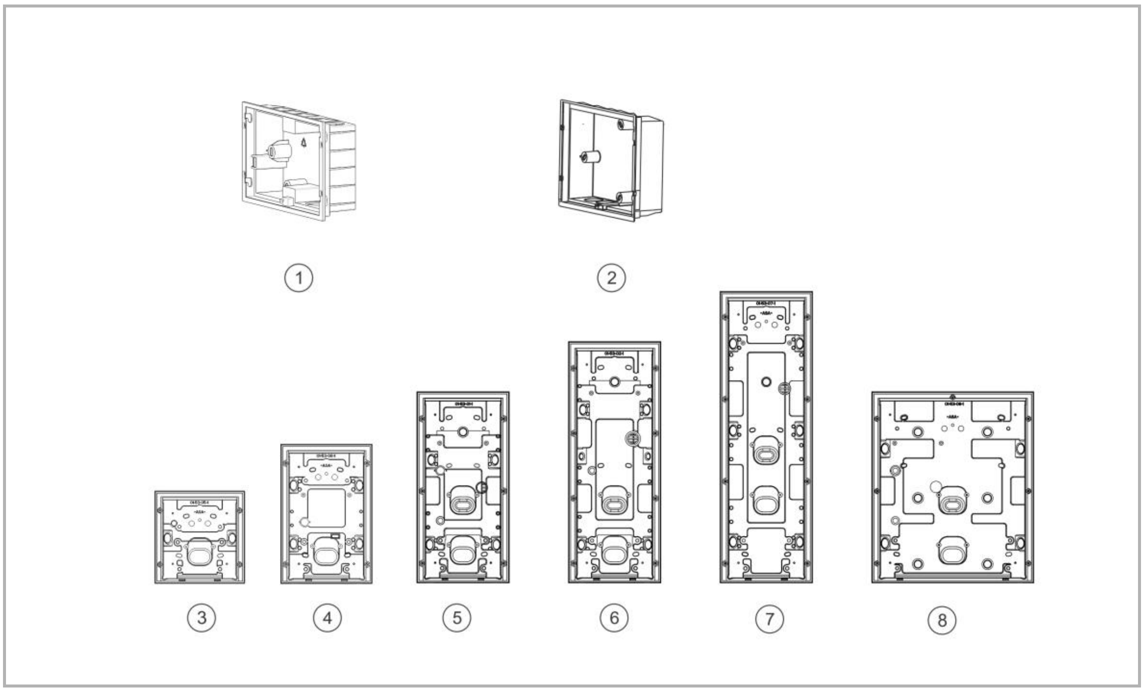
No.	Article number	Product name
1	42491S-.-03	Surface-mounted box for IP Touch Lite 7
2	42361S-.-03	Surface-mounted box for IP Touch 7
3	42371S-.-03	Surface-mounted box for IP Touch 10
4	41381S-.-03	Surface-mounted box for OS, size 1/1
5	41382S-.-03	Surface-mounted box for OS, size 1/2
6	41383S-.-03	Surface-mounted box for OS, size 1/3
7	41384S-.-03	Surface-mounted box for OS, size 1/4
8	41385S-.-03	Surface-mounted box for OS, size 1/5
9	41386S-.-03	Surface-mounted box for OS, size 2/3

Device type

Article number	Order number	Product name	Colour	Size (WxHxD) Unit: mm
42491S-W-03	2TMA320160W0001	Surface-mounted box for IP Touch Lite 7	White	188 x 123 x 14
42491S-B-03	2TMA320160B0001	Surface-mounted box for IP Touch Lite 7	Black	188 x 123 x 14
42361S-W-03	2TMA130160W0021	Surface-mounted box for IP Touch 7	White	197 x 148 x 12.7
42361S-B-03	2TMA130160B0089	Surface-mounted box for IP Touch 7	Black	197 x 148 x 12.7
42371S-W-03	2TMA130160W0041	Surface-mounted box for IP Touch 10	White	221 x 251 x 13.5
42371S-B-03	2TMA130160B0141	Surface-mounted box for IP Touch 10	Black	221 x 251 x 13.5
41381S-B-03	2TMA130160B0059	Surface-mounted box for OS, size 1/1	Anthracite	133 x 137 x 32
41382S-B-03	2TMA130160B0060	Surface-mounted box for OS, size 1/2	Anthracite	133 x 203 x 32
41383S-B-03	2TMA130160B0061	Surface-mounted box for OS, size 1/3	Anthracite	133 x 275 x 32
41384S-B-03	2TMA130160B0062	Surface-mounted box for OS, size 1/4	Anthracite	133 x 347 x 32
41385S-B-03	2TMA130160B0063	Surface-mounted box for OS, size 1/5	Anthracite	133 x 419 x 32
41386S-B-03	2TMA130160B0064	Surface-mounted box for OS, size 2/3	Anthracite	233 x 275 x 32
41381S-H-03	2TMA130160H0041	Surface-mounted box for OS, size 1/1	Grey	133 x 137 x 32
41382S-H-03	2TMA130160H0042	Surface-mounted box for OS, size 1/2	Grey	133 x 203 x 32
41383S-H-03	2TMA130160H0043	Surface-mounted box for OS, size 1/3	Grey	133 x 275 x 32
41384S-H-03	2TMA130160H0044	Surface-mounted box for OS, size 1/4	Grey	133 x 347 x 32
41385S-H-03	2TMA130160H0045	Surface-mounted box for OS, size 1/5	Grey	133 x 419 x 32
41386S-H-03	2TMA130160H0046	Surface-mounted box for OS, size 2/3	Grey	233 x 275 x 32

2.5.3 Flush-mounted box

Overview



No.	Article number	Product name
1	42491F-.-03	Flush-mounted box for IP Touch Lite 7
2	42361F-.-03	Flush-mounted box for IP Touch 7/10
3	41381F-.-03	Flush-mounted box for OS, size 1/1
4	41382F-.-03	Flush-mounted box for OS, size 1/2
5	41383F-.-03	Flush-mounted box for OS, size 1/3
6	41384F-.-03	Flush-mounted box for OS, size 1/4
7	41385F-.-03	Flush-mounted box for OS, size 1/5
8	41386F-.-03	Flush-mounted box for OS, size 2/3

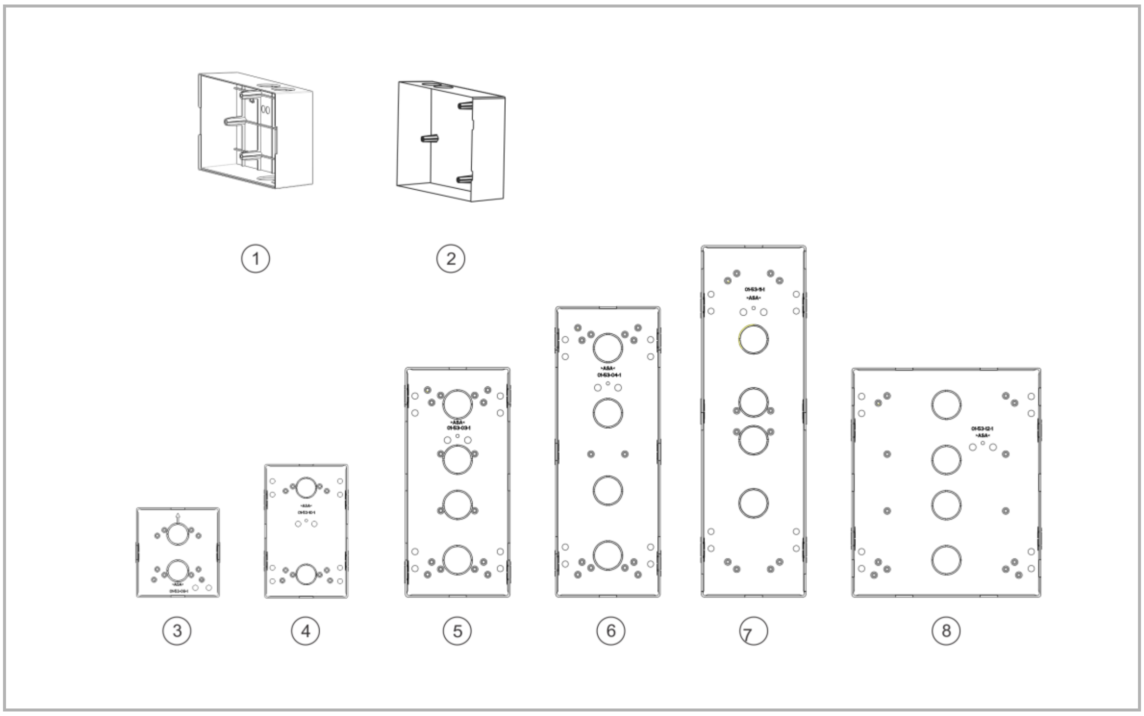
Device type

Article number	Order number	Product name	Colour	Size (WxHxD) Unit: mm
42491F-03	2TMA320160B0002	*Flush-mounted box for IP Touch Lite 7	Black	178 x 108 x 52
42361F-03	2TMA130160B0134	*Flush-mounted box for IP Touch 7/10	-	194 x 145 x 55
41381F-B-03	2TMA130160B0051	Flush-mounted box for OS, size 1/1	Anthracite	133 x 137 x 52
41382F-B-03	2TMA130160B0052	Flush-mounted box for OS, size 1/2	Anthracite	133 x 203 x 52
41383F-B-03	2TMA130160B0053	Flush-mounted box for OS, size 1/3	Anthracite	133 x 275 x 52
41384F-B-03	2TMA130160B0054	Flush-mounted box for OS, size 1/4	Anthracite	133 x 347 x 52
41385F-B-03	2TMA130160B0055	Flush-mounted box for OS, size 1/5	Anthracite	133 x 419 x 52
41386F-B-03	2TMA130160B0056	Flush-mounted box for OS, size 2/3	Anthracite	233 x 275 x 52
41381F-H-03	2TMA130160H0033	Flush-mounted box for OS, size 1/2	Grey	133 x 137 x 52
41382F-H-03	2TMA130160H0034	Flush-mounted box for OS, size 1/3	Grey	133 x 203 x 52
41383F-H-03	2TMA130160H0035	Flush-mounted box for OS, size 1/3	Grey	133 x 275 x 52
41384F-H-03	2TMA130160H0036	Flush-mounted box for OS, size 1/4	Grey	133 x 347 x 52
41385F-H-03	2TMA130160H0037	Flush-mounted box for OS, size 1/5	Grey	133 x 419 x 52
41386F-H-03	2TMA130160H0038	Flush-mounted box for OS, size 2/3	Grey	233 x 275 x 52

*IP Touch Lite 7, IP Touch 7 & IP Touch 10 integrated the flush-mounted box with the pre-installation box in the package.

2.5.4 Pre-mounting box

Overview



No.	Article number	Product name
1	42491F-.-03	Pre-installation box for IP Touch Lite 7
2	42361F-.-03	Pre-installation box for IP Touch 7/10
3	41381F-.-03	Pre-installation box for OS, size 1/1
4	41382F-.-03	Pre-installation box for OS, size 1/2
5	41383F-.-03	Pre-installation box for OS, size 1/3
6	41384F-.-03	Pre-installation box for OS, size 1/4
7	41385F-.-03	Pre-installation box for OS, size 1/5
8	41386F-.-03	Pre-installation box for OS, size 2/3

Device type

Article number	Order number	Product name	Colour	Size (WxHxD) Unit: mm
42491F-03	2TMA320160B0002	Pre-installation box for IP Touch Lite 7	Black	178 x 108 x 52
42361F-03	2TMA130160B0134	Pre-installation box for IP Touch 7/10	-	194 x 145 x 55
41381PB-03	2TMA130160B0067	Pre-installation box for OS, size 1/1	-	124 x 133 x 64.5
41382PB-03	2TMA130160B0068	Pre-installation box for OS, size 1/2	-	124 x 199 x 64.5
41383PB-03	2TMA130160B0069	Pre-installation box for OS, size 1/3	-	124 x 271 x 64.5
41384PB-03	2TMA130160B0070	Pre-installation box for OS, size 1/4	-	124 x 343 x 64.5
41385PB-03	2TMA130160B0071	Pre-installation box for OS, size 1/5	-	124 x 415 x 64.5
41386PB-03	2TMA130160B0072	Pre-installation box for OS, size 2/3	-	224 x 271 x 64.5

*IP Touch Lite 7, IP Touch 7 & IP Touch 10 integrated the flush-mounted box with the pre-installation box in the package.

2.6 Accessories

2.7 Outdoor Stations

Device type

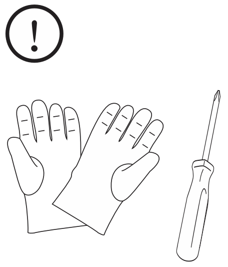
Article number	Order number	Product name	Colour	Size (WxHxD) Unit: mm
51381EP-A-03	2TMA200160A0037	End-strip, size 1/x	Stainless steel	135 x 19 x 16
51382EP-A-03	2TMA200160A0038	End-strip, size 2/x	Stainless steel	235 x 19 x 16
51381MT-03	2TMA130160B0075	Mounting tool, 135mm	Aluminium alloy	165 x 26 x 4

3 Installation guidelines

3.1 Outdoor Stations

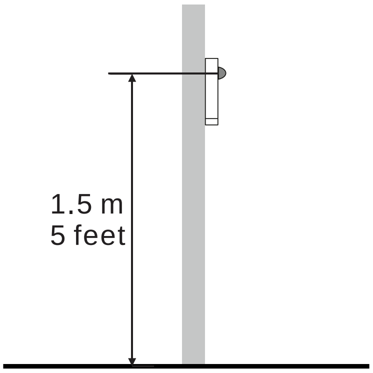
3.1.1 Preparation

Please use gloves to protect yourself against cuts.



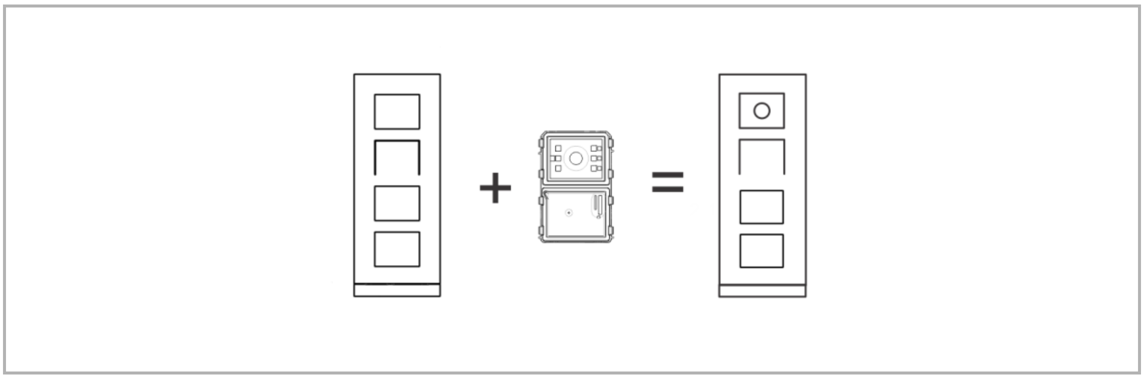
3.1.2 Installation height

(unit: mm)

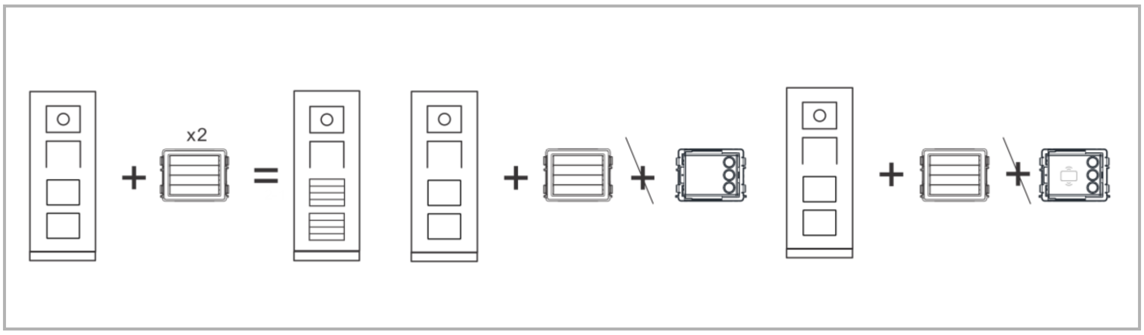


3.1.3 The rule of assembled modules

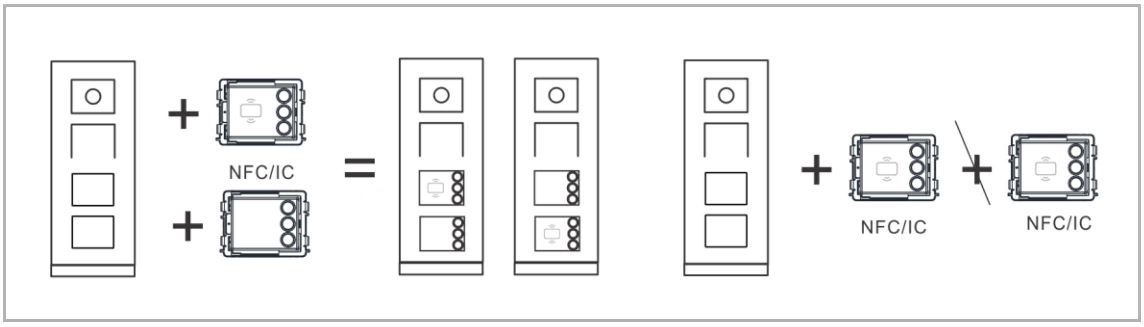
Rule 1: A/V module should be placed on the top.



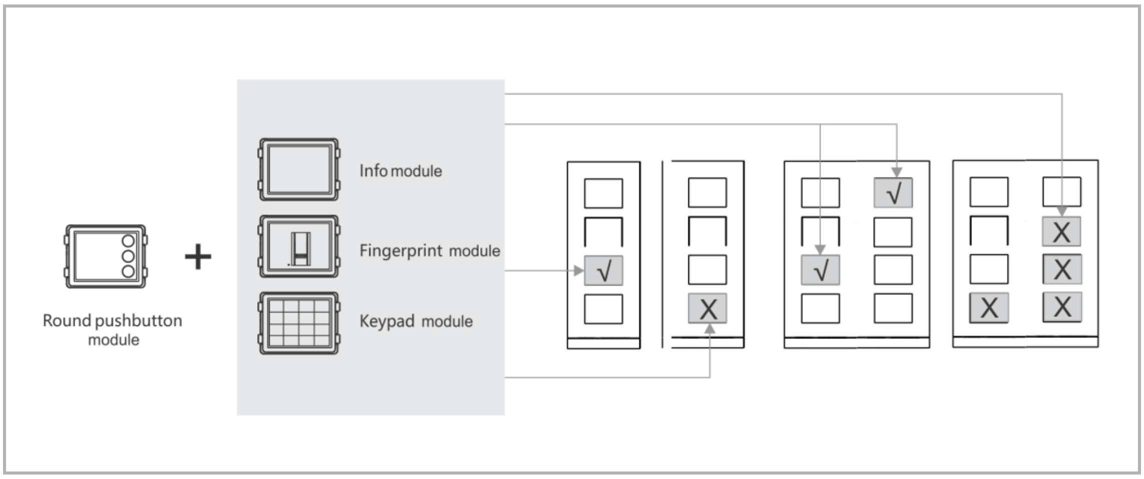
Rule 2: Bar pushbutton module cannot work with round pushbutton module



Rule 3: Only supports 1 Round pushbutton module with NFC



Rule 4: When other module works with Round pushbutton module



3.1.4 Installation overview

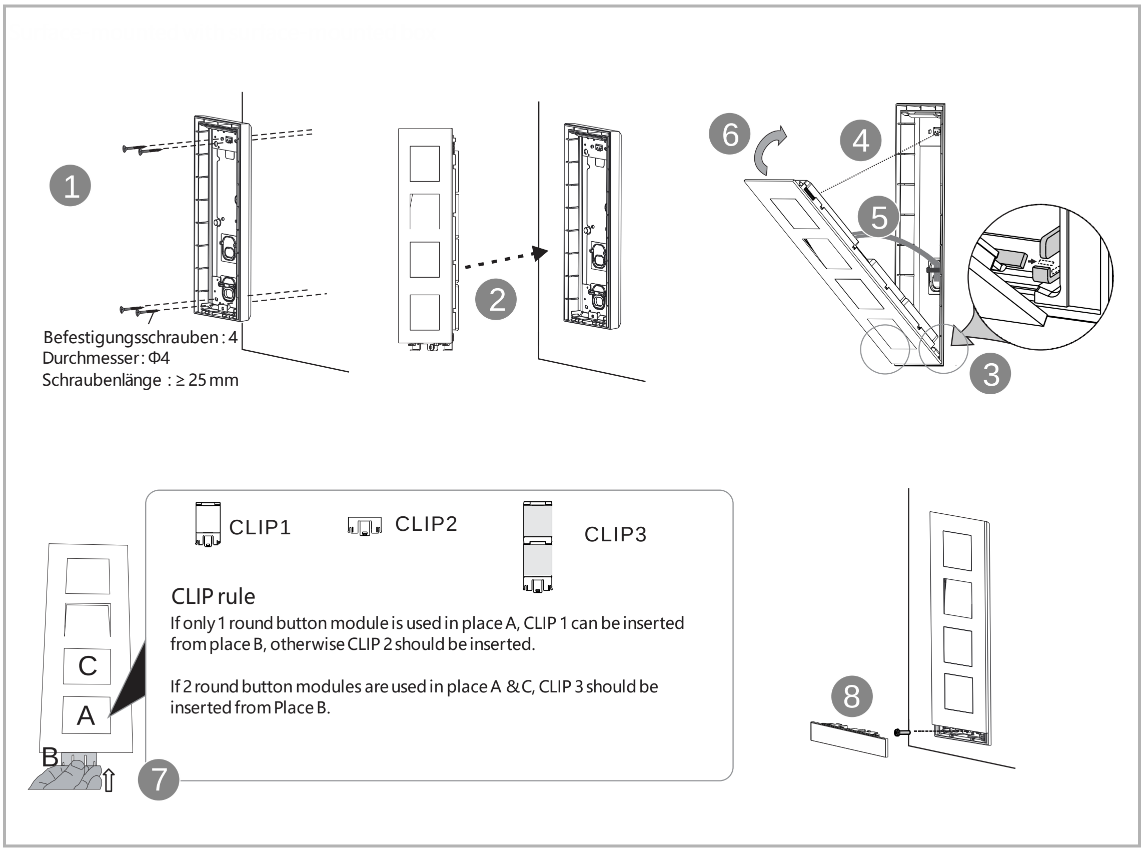
Outdoor Station type	Installation type
[1] Single column OS	Surface-mounted installation
	Flush-mounted installation in solid walls
	Flush-mounted installation in hollow walls
[2] Multiple columns OS	Flush-mounted installation in solid walls
Mini OS	Surface-mounted installation
	Flush-mounted installation in solid walls
	Flush-mounted installation in hollow walls

[1] Single column OS contains IP Touch 5 OS, IP pushbutton OS , IP keypad OS and other Outdoor Stations assembled with customised modules.

[2] Multiple columns OS contains the Outdoor Stations assembled with customised modules.

3.1.5 Single column OS

Surface-mounted installation with surface-mounted box



Befestigungsschrauben : 4
Durchmesser : Φ4
Schraubenlänge : ≥ 25 mm

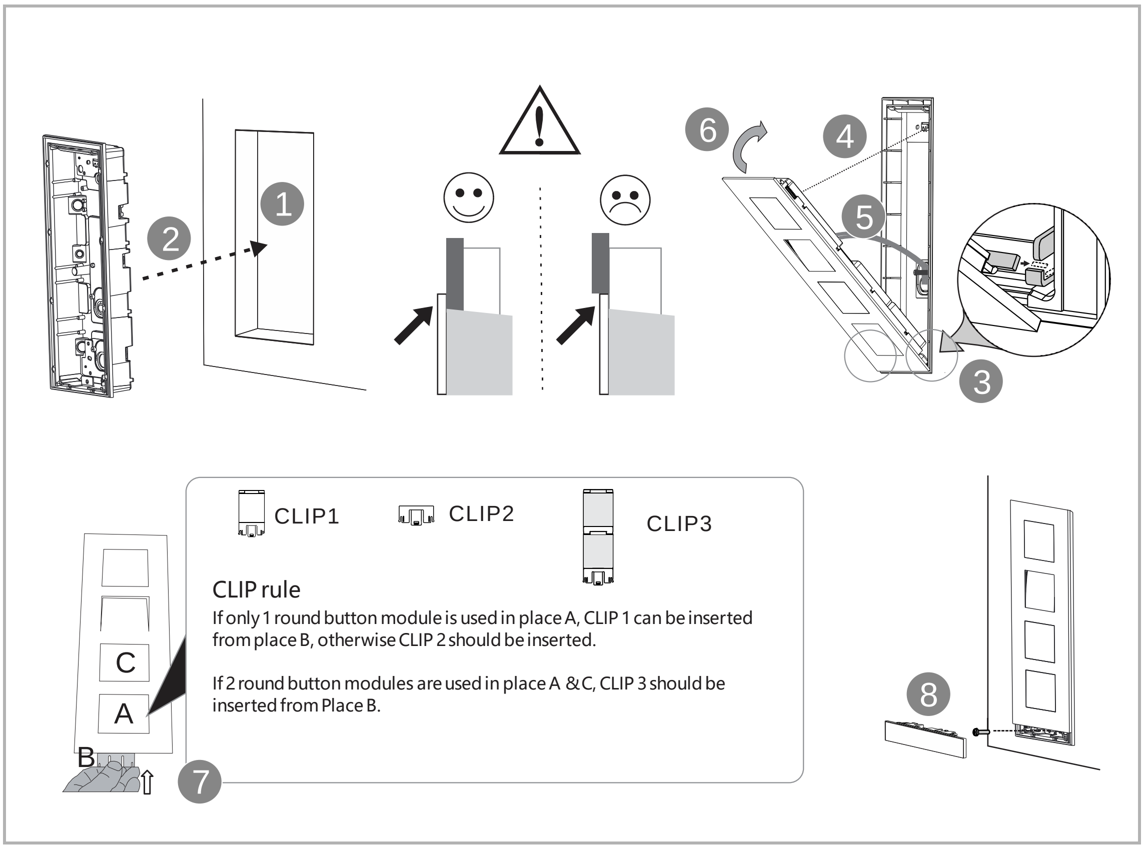
CLIP rule

If only 1 round button module is used in place A, CLIP 1 can be inserted from place B, otherwise CLIP 2 should be inserted.

If 2 round button modules are used in place A &C, CLIP 3 should be inserted from Place B.

Flush-mounted installation in solid walls

1. Without pre-mounted box

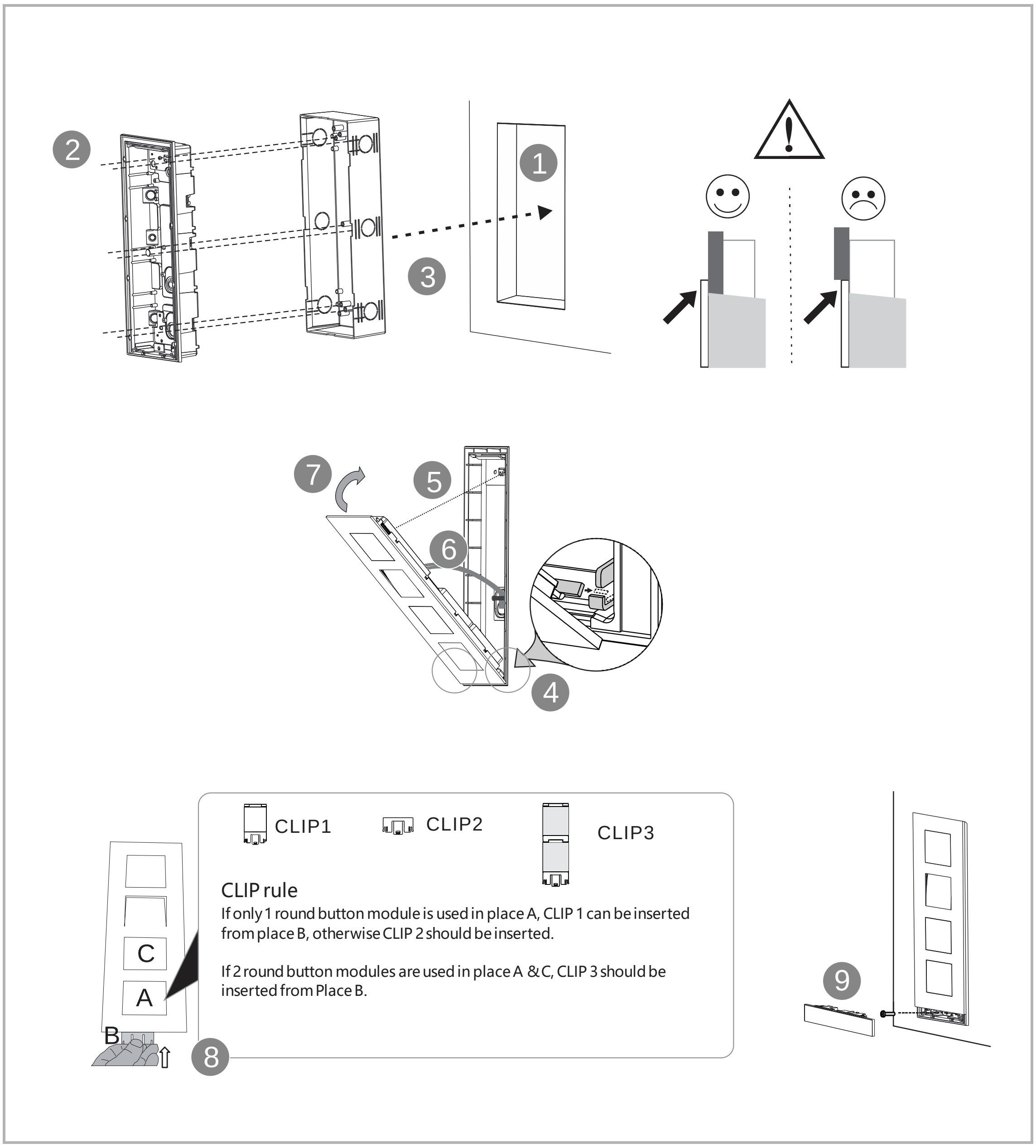


CLIP rule

If only 1 round button module is used in place A, CLIP 1 can be inserted from place B, otherwise CLIP 2 should be inserted.

If 2 round button modules are used in place A &C, CLIP 3 should be inserted from Place B.

2. With pre-mounted box

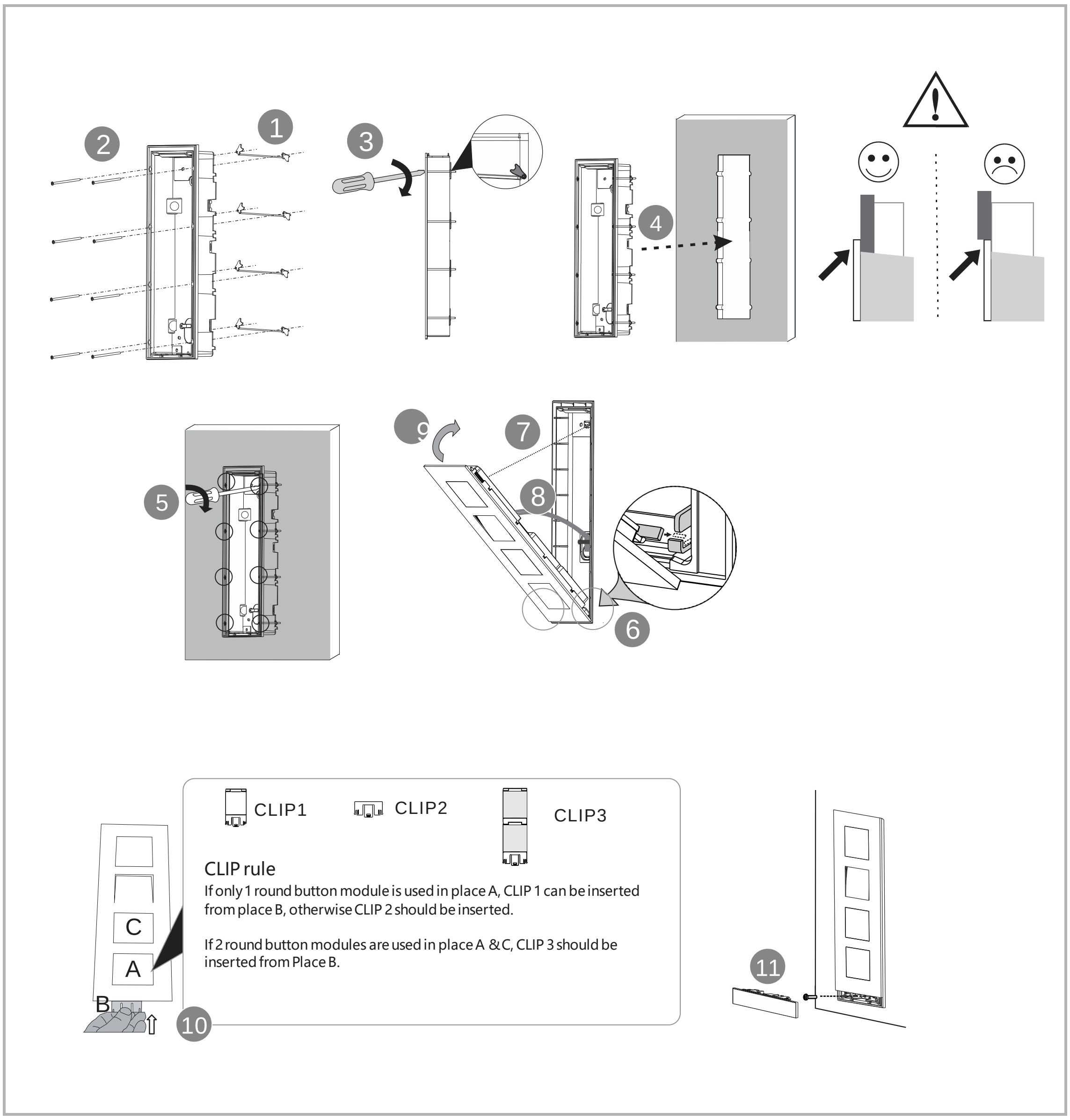


CLIP rule

If only 1 round button module is used in place A, CLIP 1 can be inserted from place B, otherwise CLIP 2 should be inserted.

If 2 round button modules are used in place A &C, CLIP 3 should be inserted from Place B.

Flush-mounted installation in hollow walls

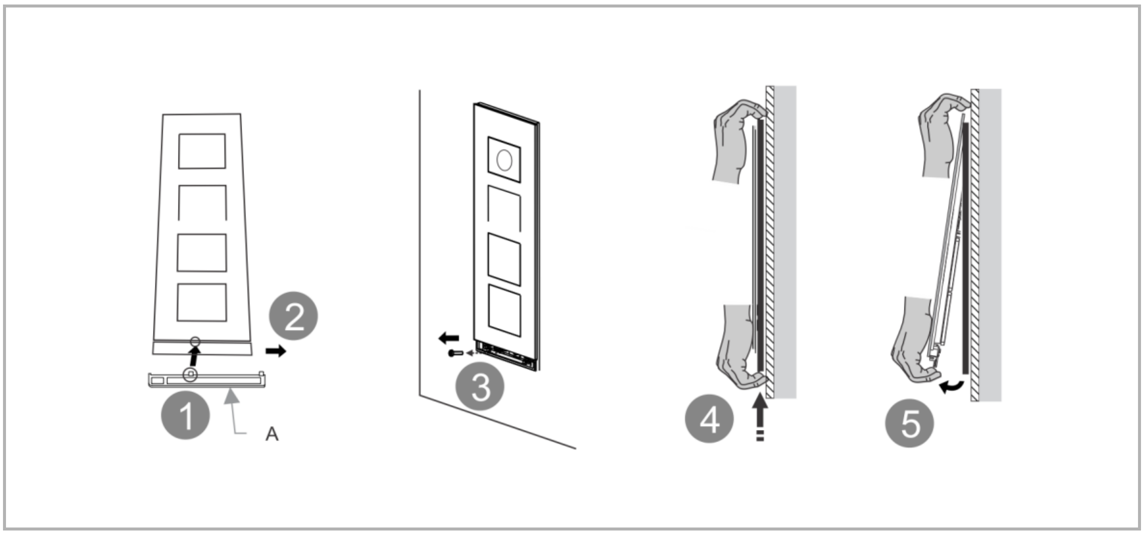


CLIP rule

If only 1 round button module is used in place A, CLIP 1 can be inserted from place B, otherwise CLIP 2 should be inserted.

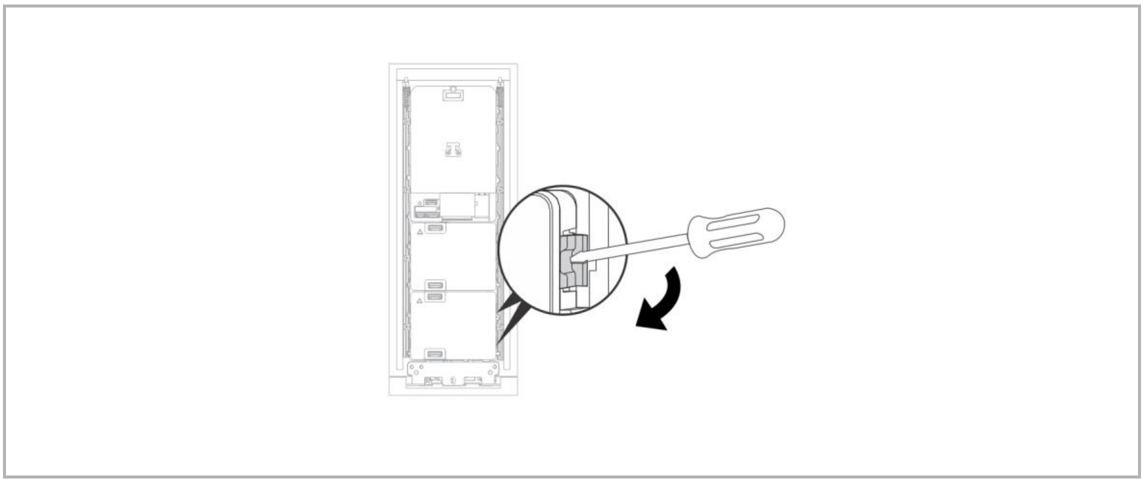
If 2 round button modules are used in place A &C, CLIP 3 should be inserted from Place B.

Dismantling single column OS

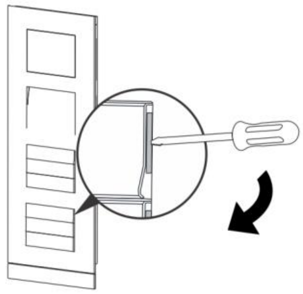


A	Mounting tool

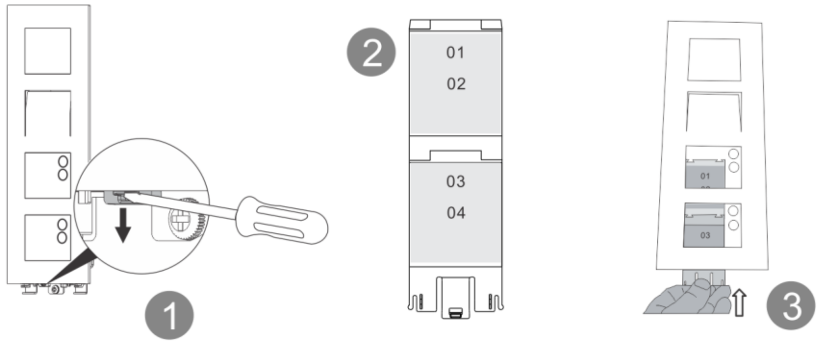
Dismantling the modules



Dismantling the name label

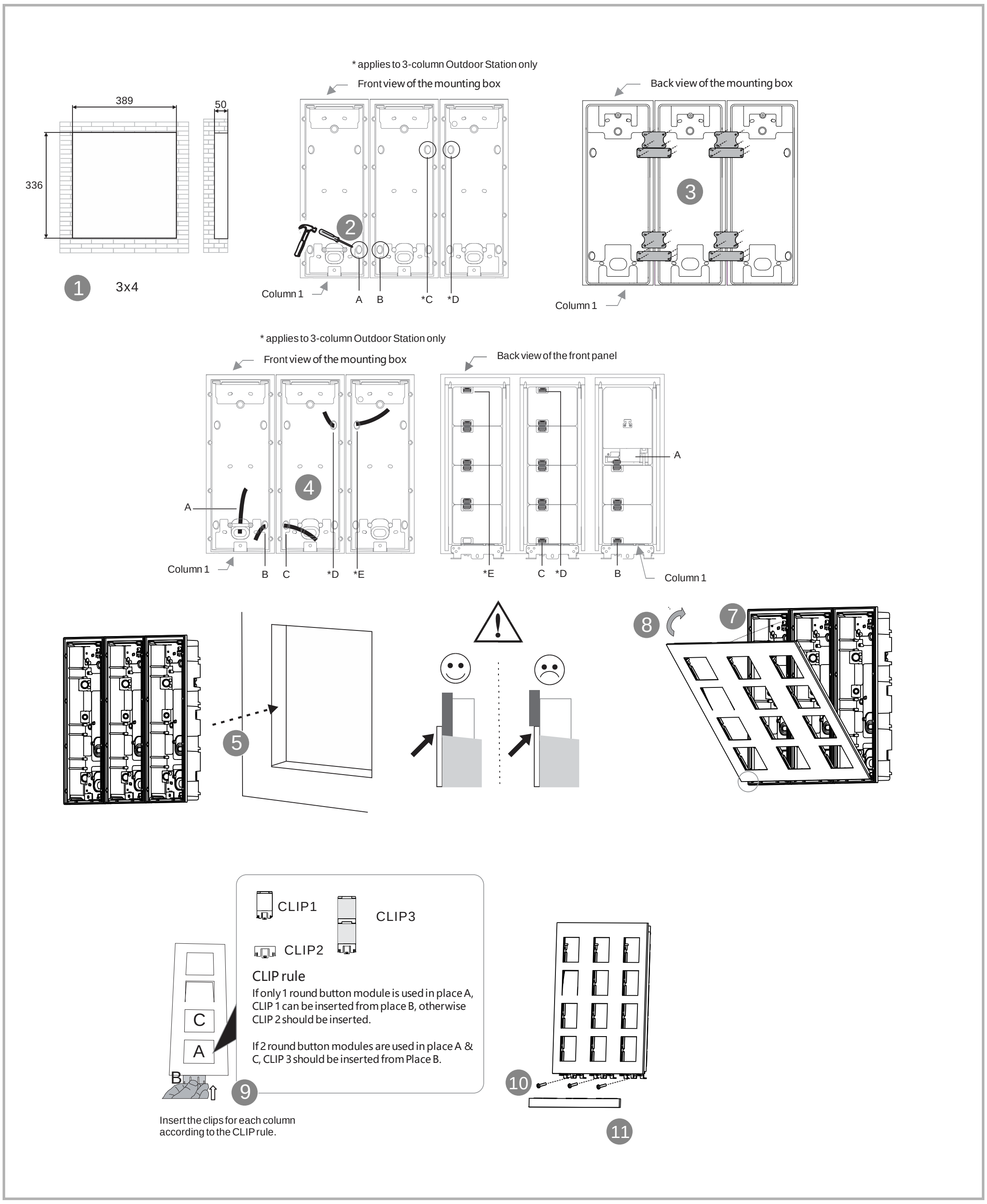


Replacing the name plate



3.1.6 Multiple columns OS

Flush-mounted installation in solid wall without pre-mounted boxes


389
50
336
1
3x4
* applies to 3-column Outdoor Station only
Front view of the mounting box
2
Column 1
A
B
*C
*D
Back view of the mounting box
3
Column 1
* applies to 3-column Outdoor Station only
Front view of the mounting box
4
A
Column 1
B
C
*D
*E
Back view of the front panel
A
*E
C
*D
B
Column 1
5
8
7
CLIP1
CLIP3
CLIP2
C
A
B
9
10
11

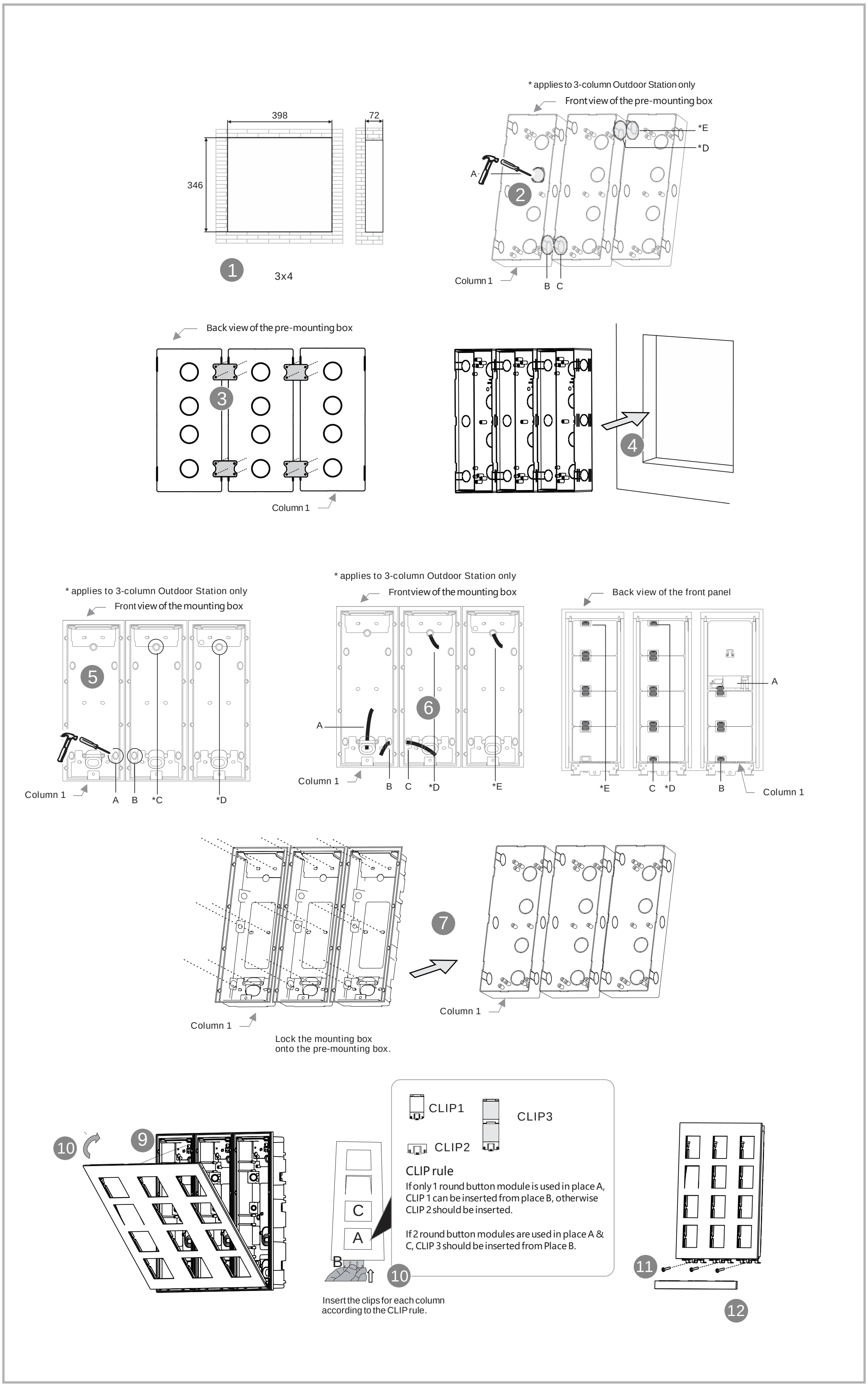
CLIP rule

If only 1 round button module is used in place A, CLIP 1 can be inserted from place B, otherwise CLIP 2 should be inserted.

If 2 round button modules are used in place A & C, CLIP 3 should be inserted from Place B.

Insert the clips for each column according to the CLIP rule.

Flush-mounted installation in solid wall with pre-mounted boxes


* applies to 3-column Outdoor Station only
Front view of the pre-mounting box
398
72
346
1
3x4
*E
*D
A
2
Column 1
B C
Back view of the pre-mounting box
3
Column 1
4
* applies to 3-column Outdoor Station only
Front view of the mounting box
5
Column 1
A B *C *D
* applies to 3-column Outdoor Station only
Front view of the mounting box
A
6
Column 1
B C *D *E
Back view of the front panel
A
*E C *D B
Column 1
7
Column 1
Column 1
CLIP1
CLIP3
CLIP2
10
9
C
A
B
10
11
12

Lock the mounting box onto the pre-mounting box.

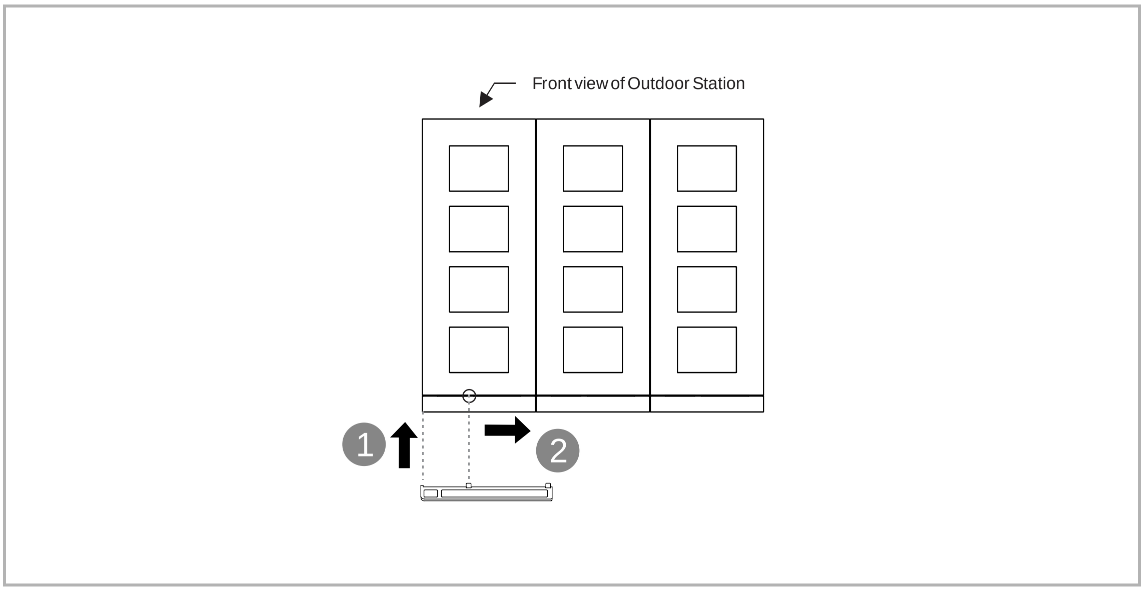
CLIP rule

If only 1 round button module is used in place A, CLIP 1 can be inserted from place B, otherwise CLIP 2 should be inserted.

If 2 round button modules are used in place A & C, CLIP 3 should be inserted from Place B.

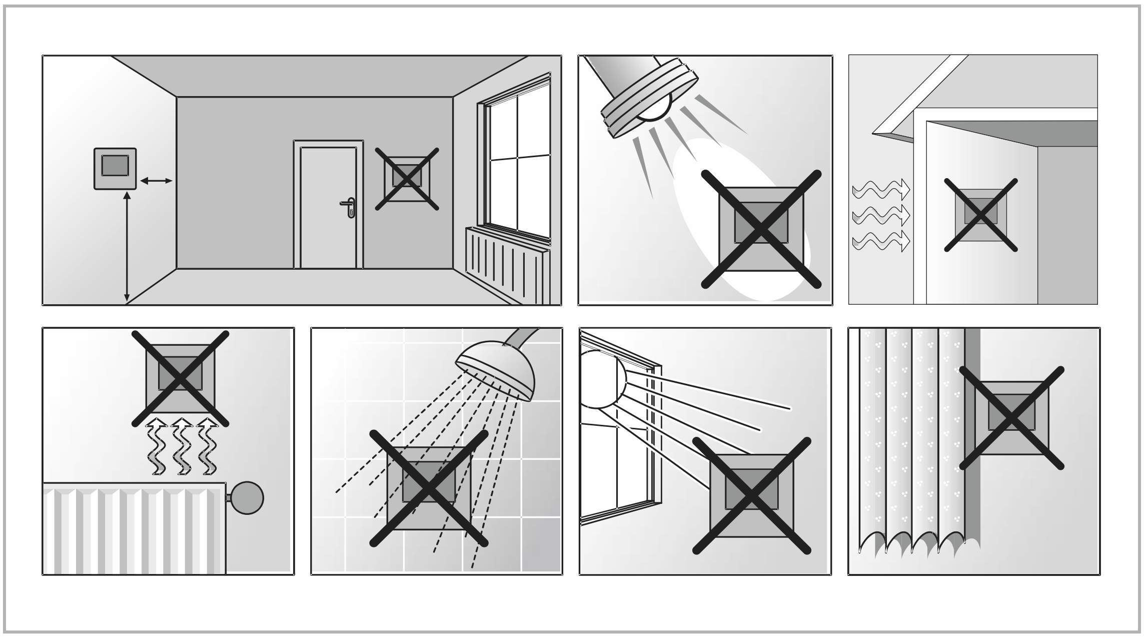
Insert the clips for each column according to the CLIP rule.

Dismantling the multiple columns OS



3.2 Indoor Stations

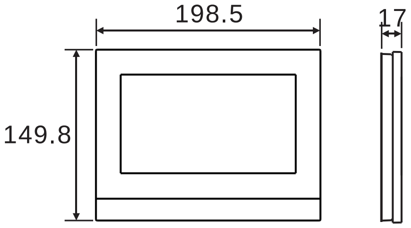
3.2.1 Location



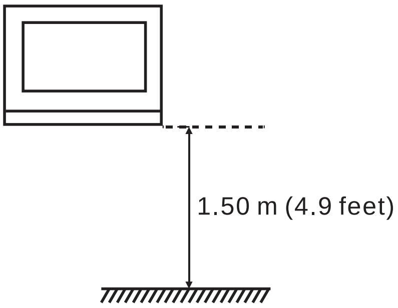
3.2.2 IP Touch 7

Product dimension

(unit: mm)

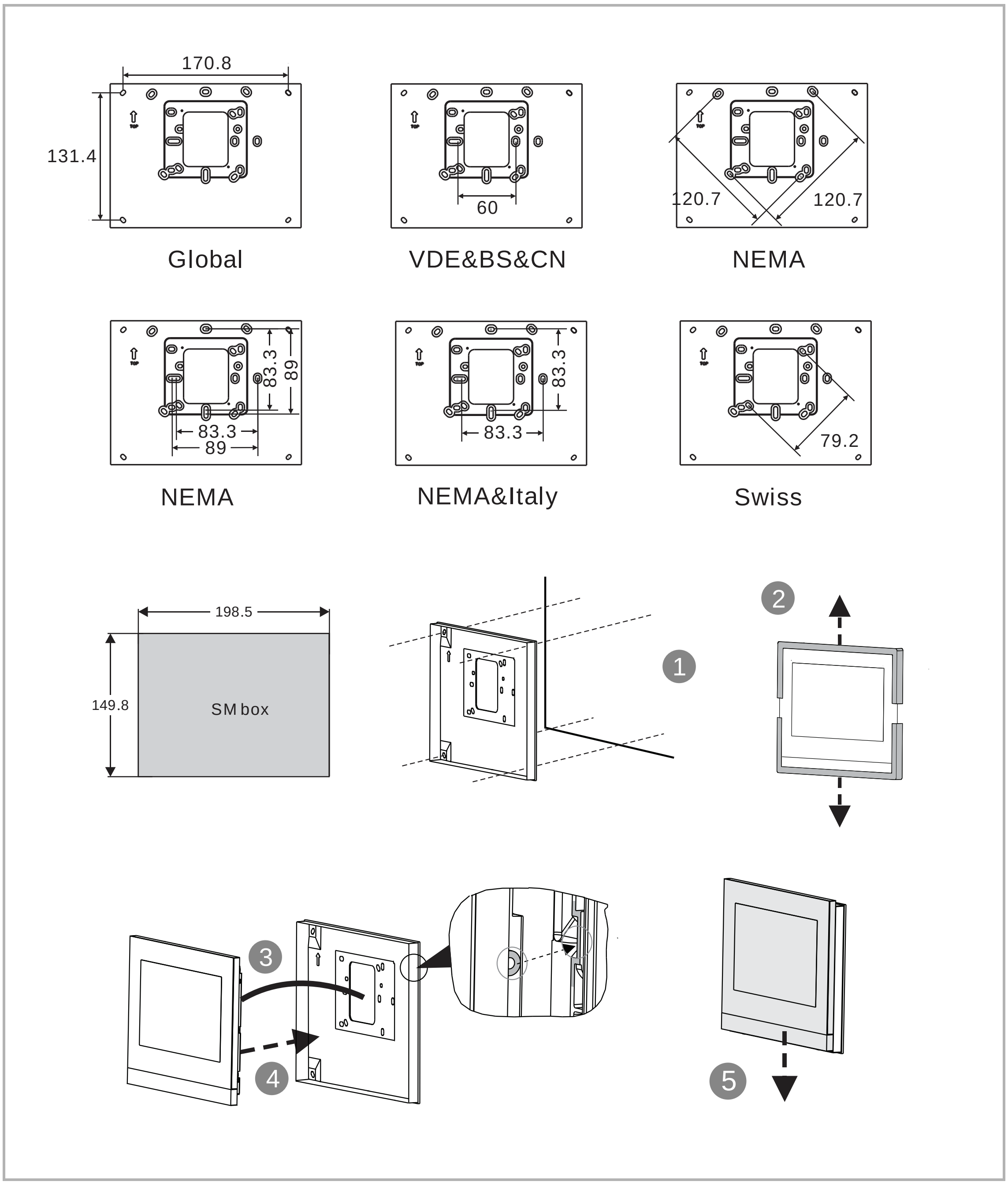


Installation height

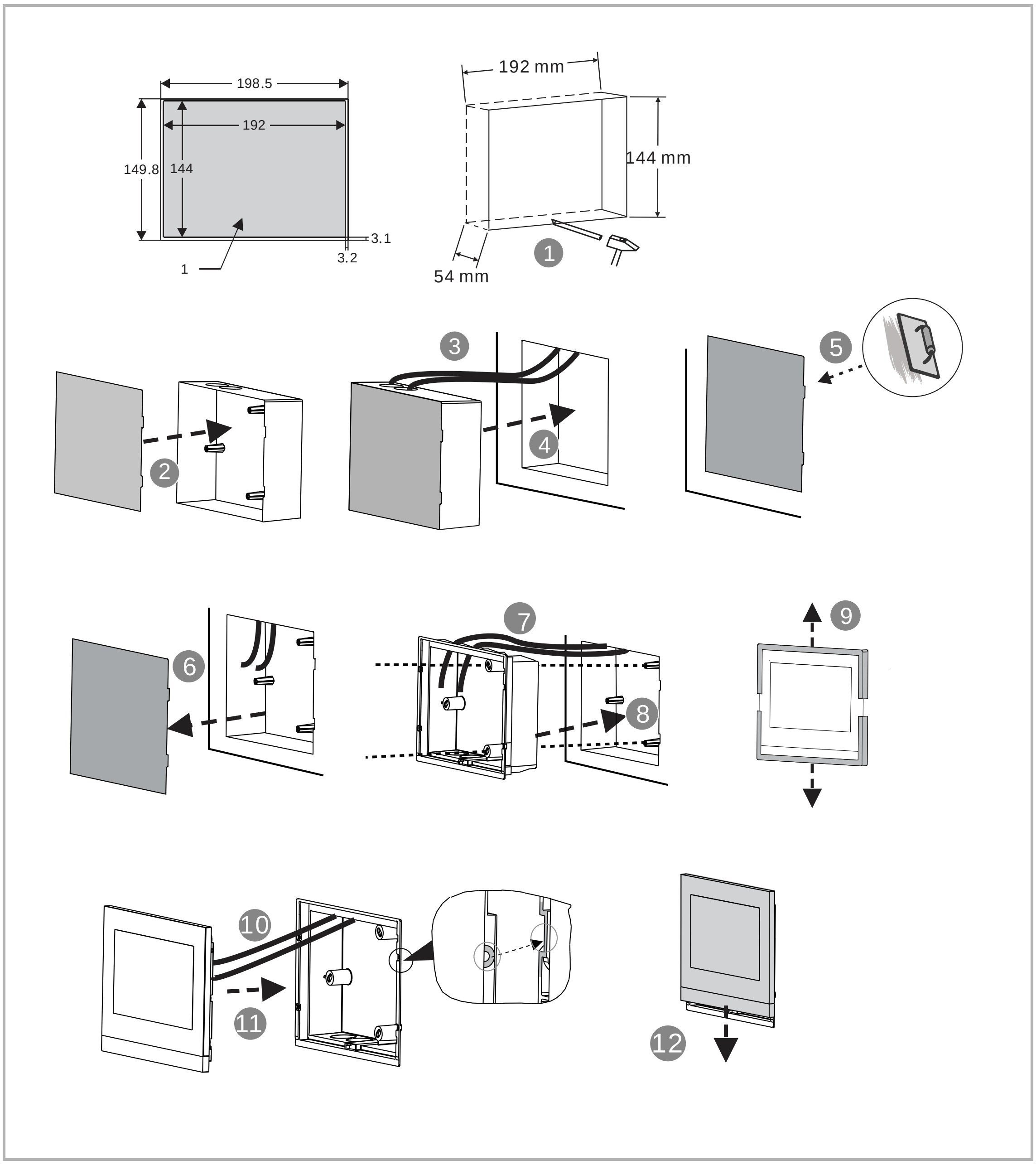


Surface-mounted installation

This chapter is not suitable for IP Touch 7 (LAN+LAN).

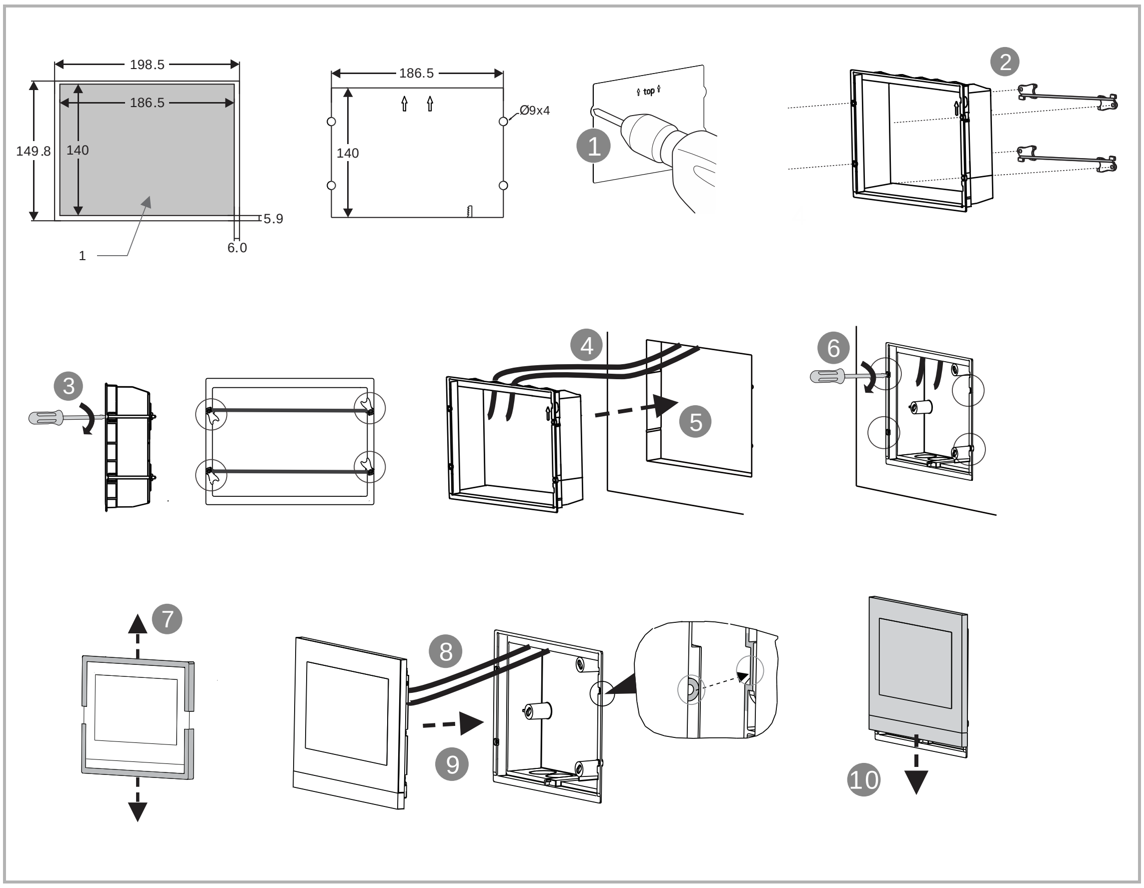


Flush-mounted installation in the solid wall with pre-installation box



1	Hole size of the pre-installation box

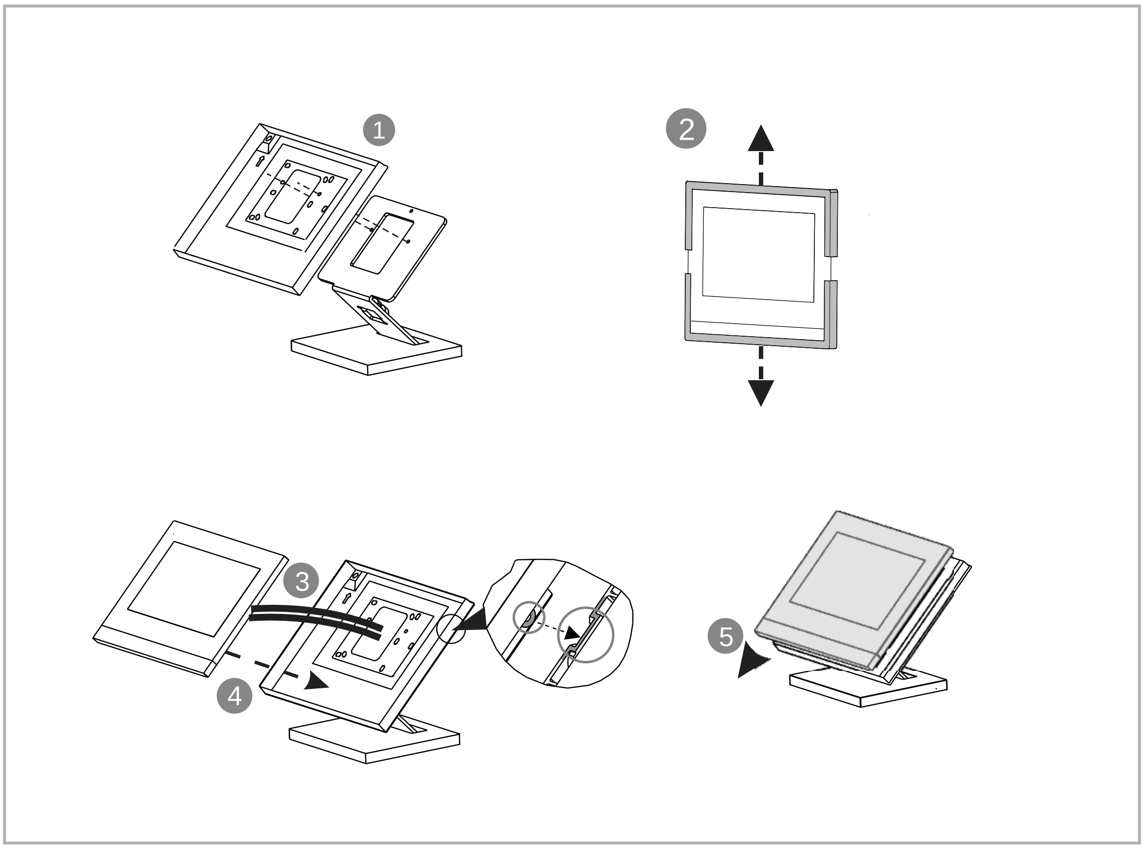
Flush-mounted installation in the hollow wall



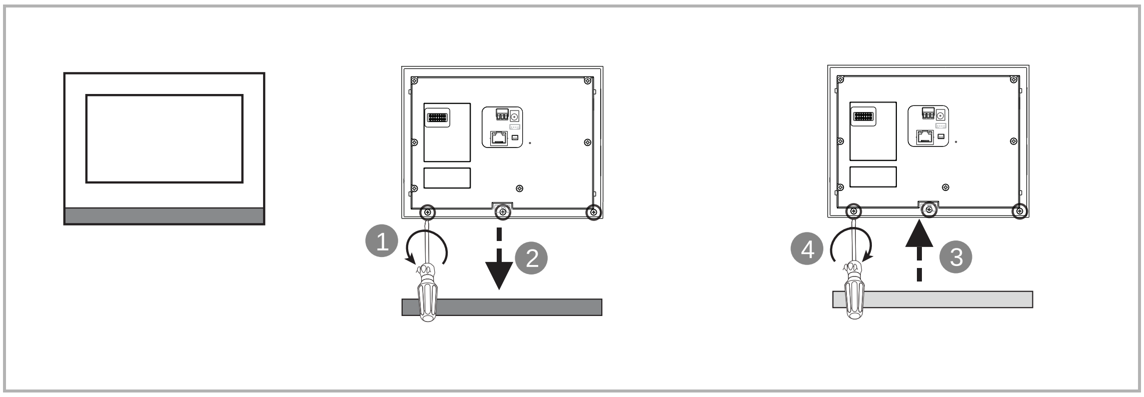
1	Hole size of flush-mounted box

Desktop installation

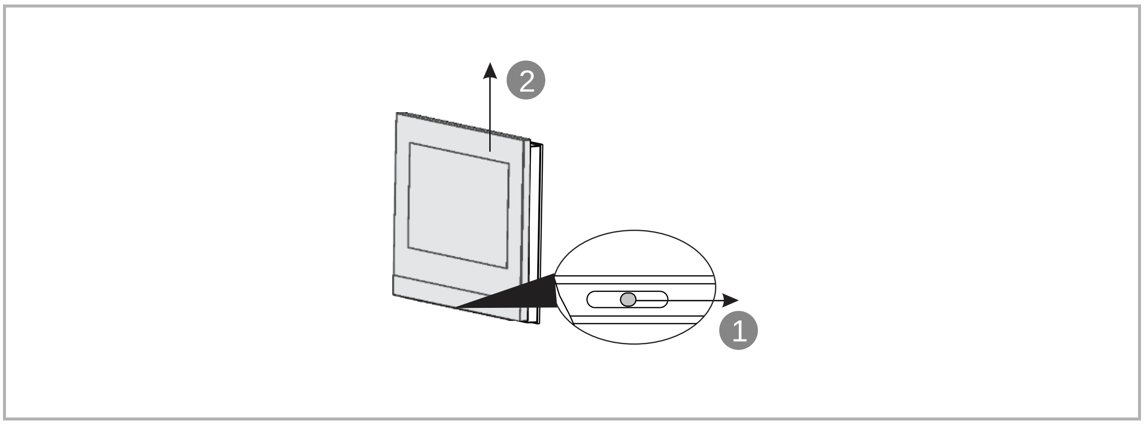
This chapter is not suitable for IP Touch 7 (LAN+LAN).



Replacing the end strip



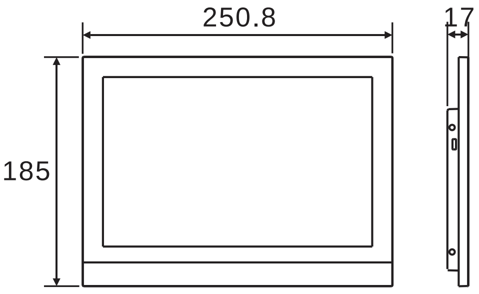
Dismantling



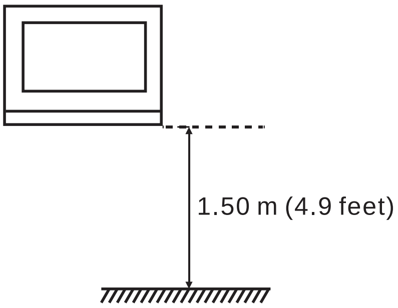
3.2.3 IP Touch 10

Product dimension

(unit: mm)



Installation height

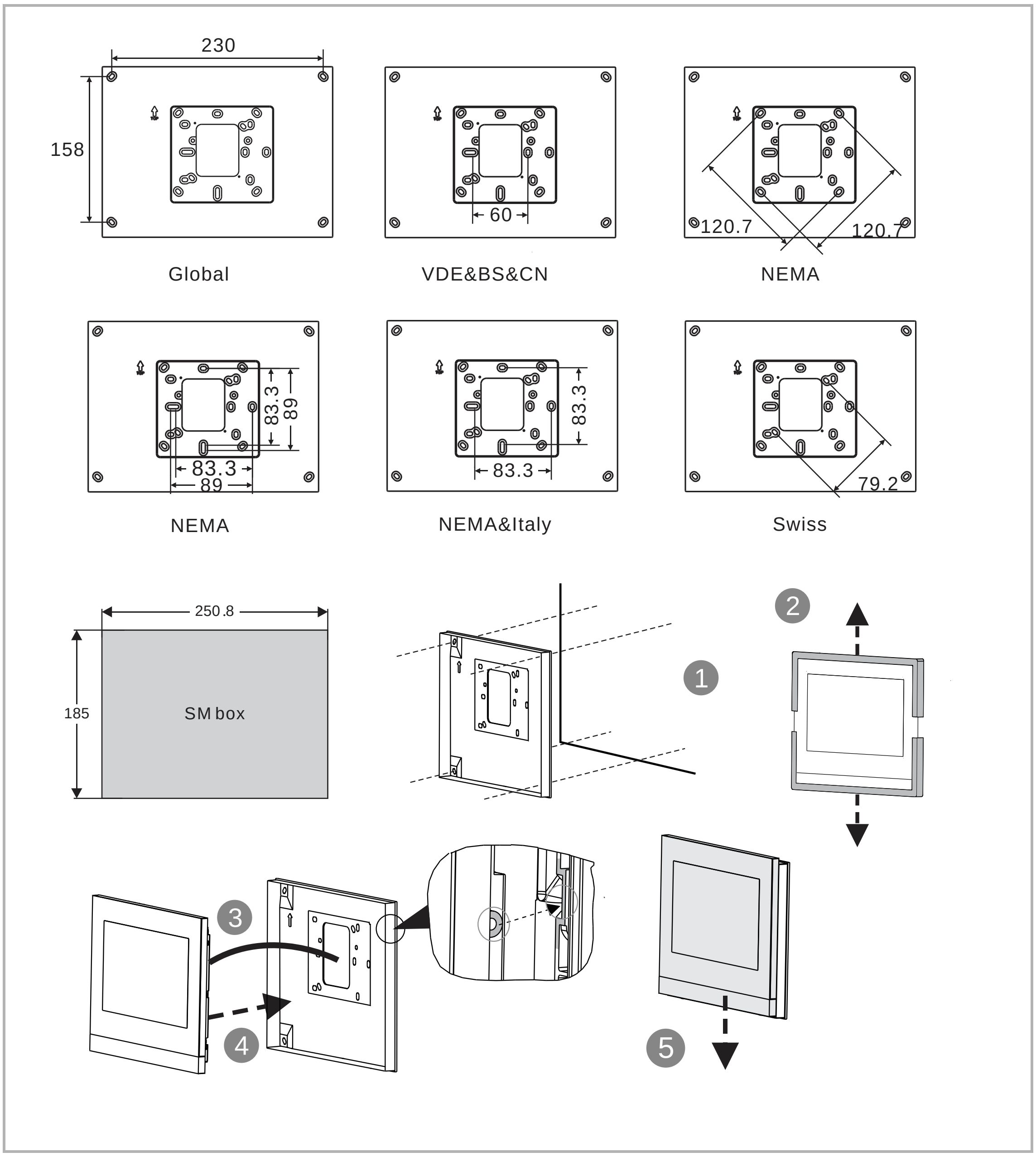


Surface-mounted installation

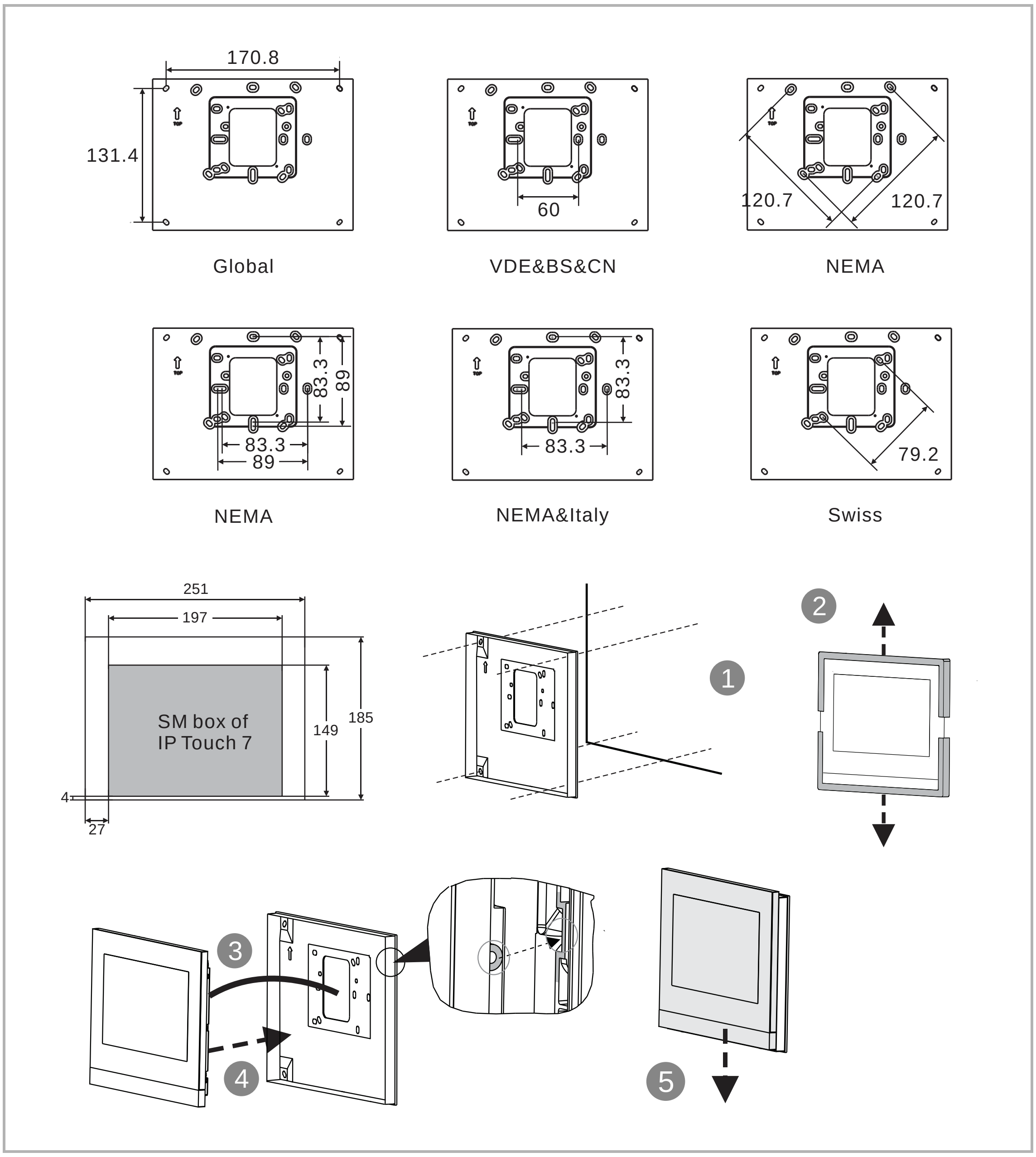
This chapter is not suitable for IP Touch 10 (LAN+LAN).

(unit: mm)

IP Touch 10 can use the surface-mounted box of IP Touch 10.

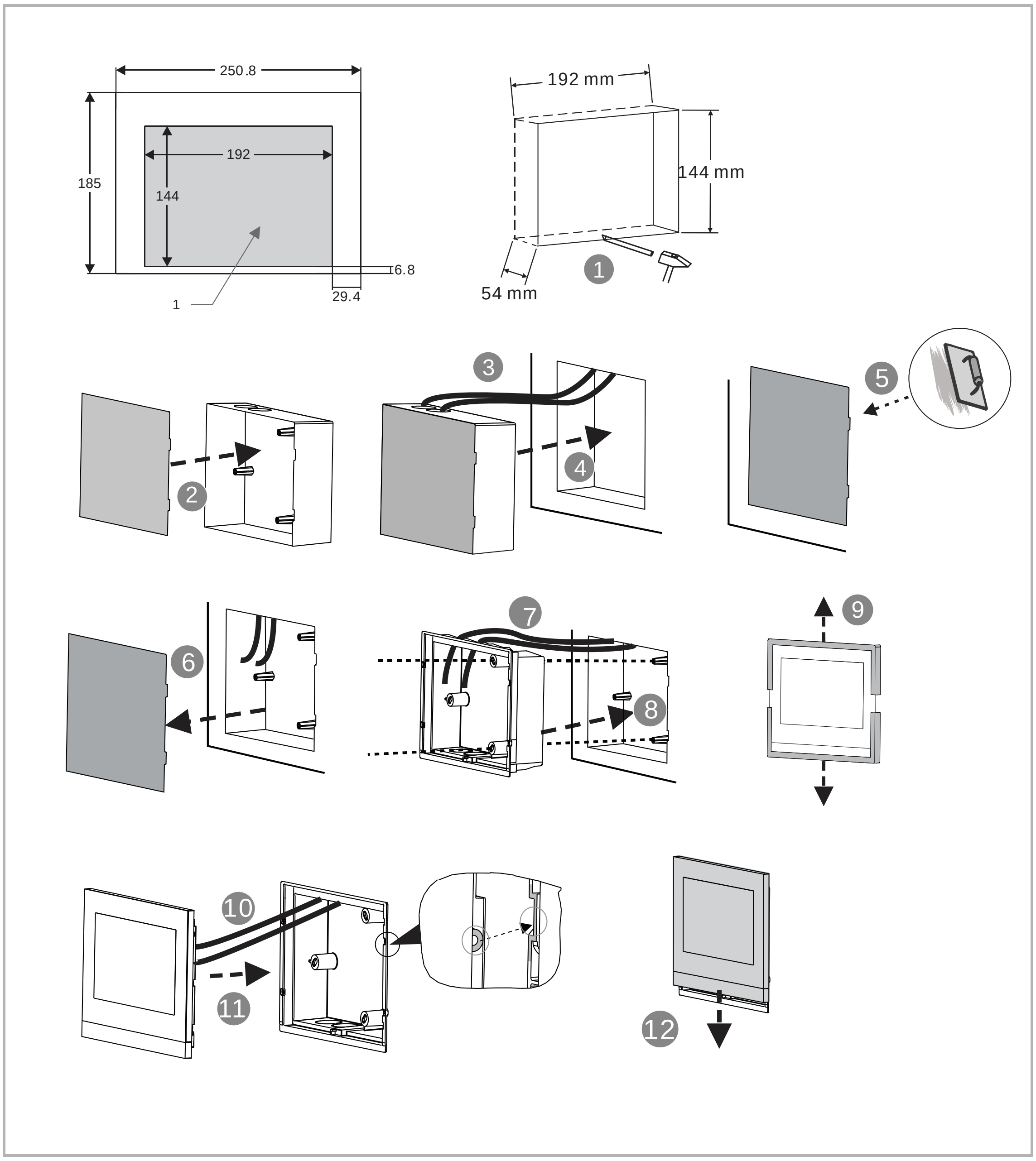


IP Touch 10 can also use the surface-mounted box of IP Touch 7.



Flush-mounted installation in the solid wall with pre-installation box

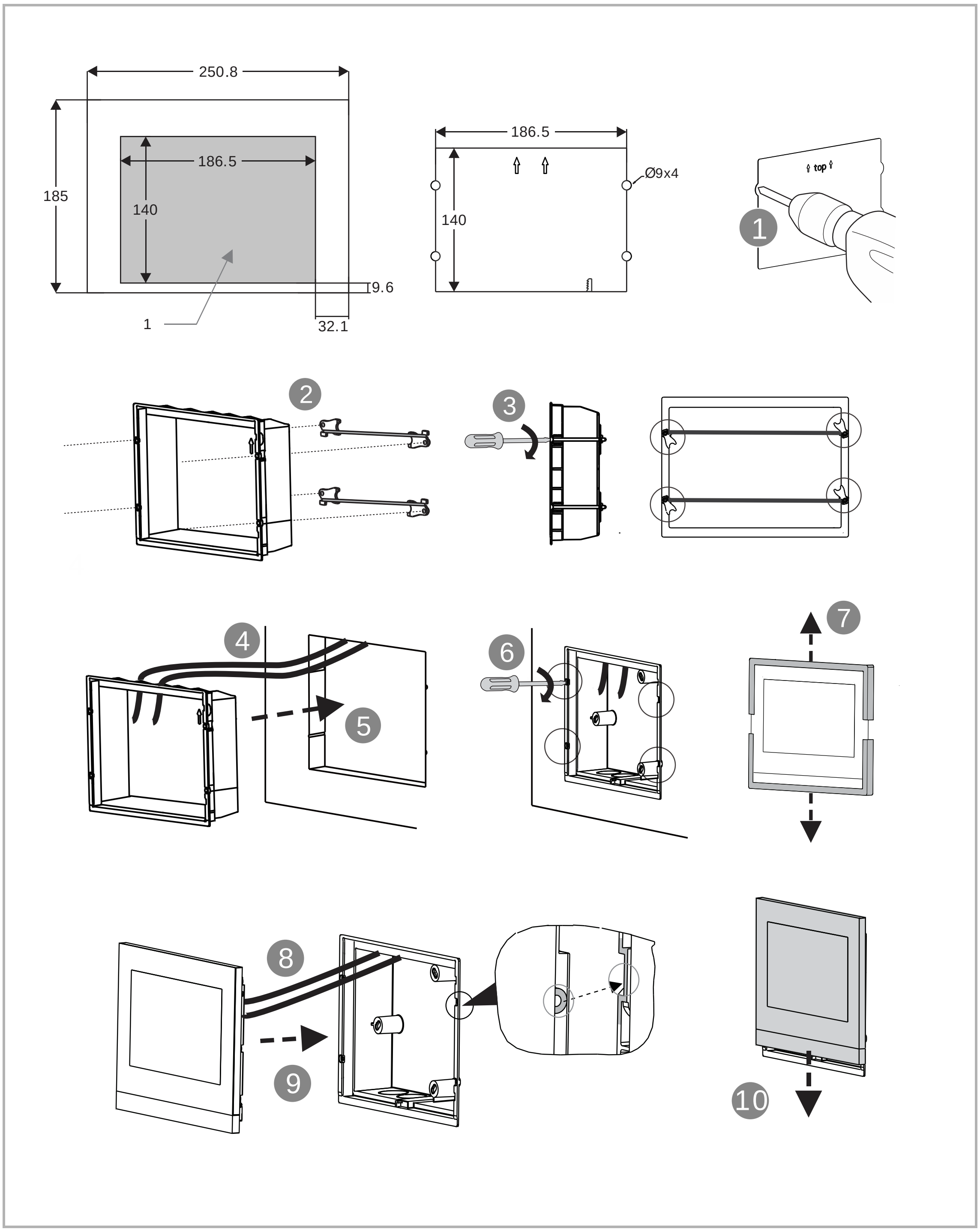
(unit: mm)



1	Hole size of the pre-installation box

Flush-mounted installation in the hollow wall

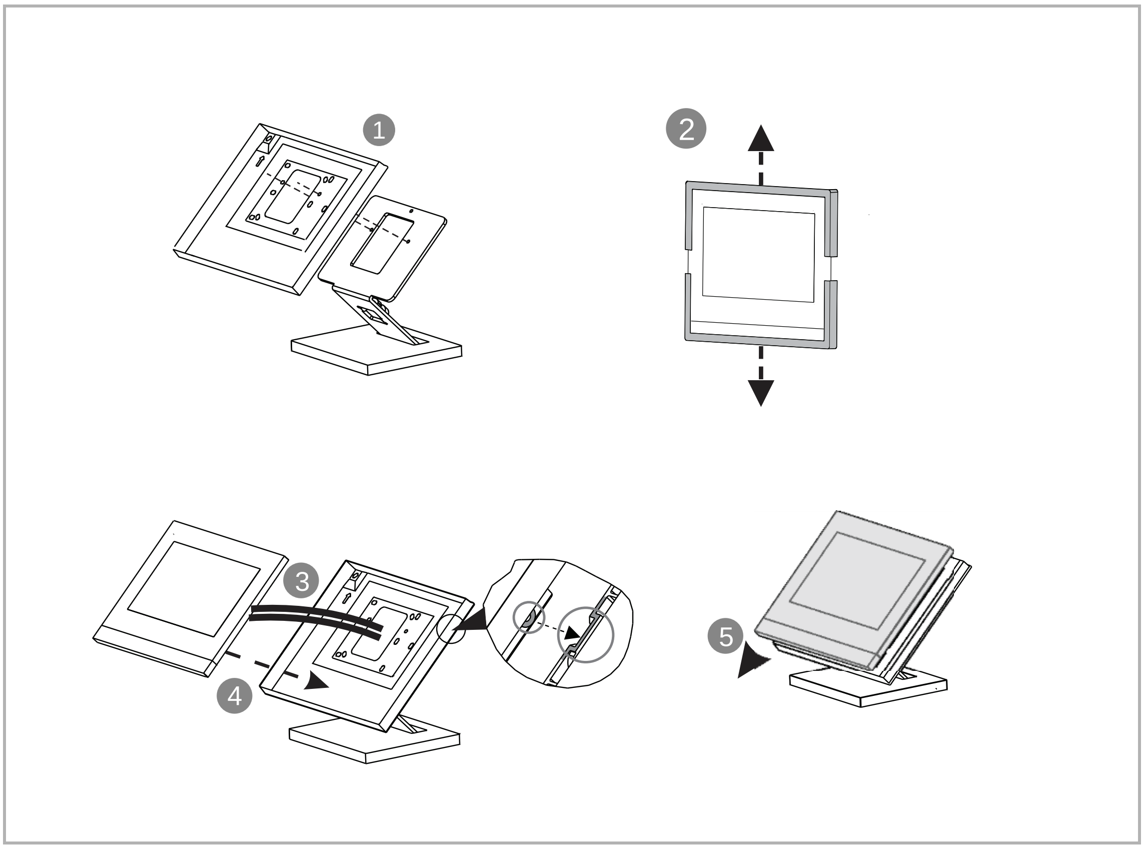
(unit: mm)



1	Hole size of flush-mounted box

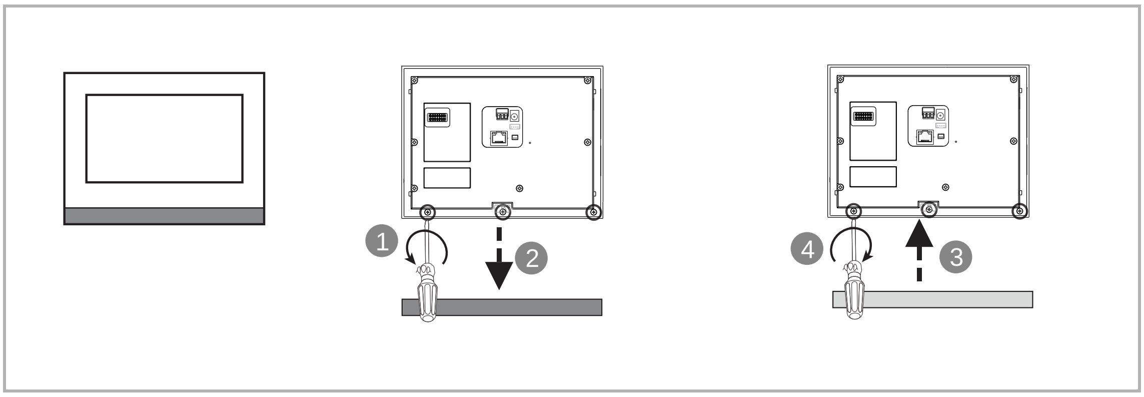
Desktop installation

This chapter is not suitable for IP Touch 10 (LAN+LAN).

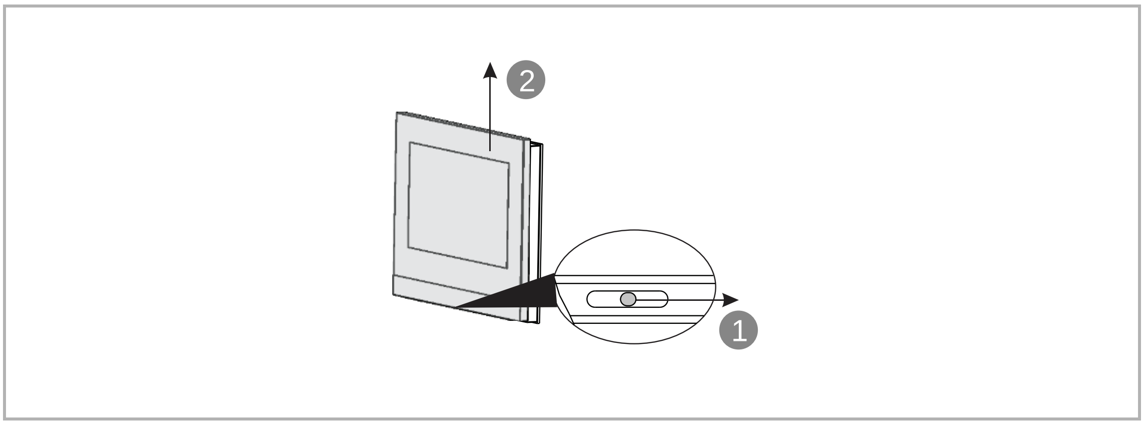


Replacing the end strip

4 screws need to be removed.



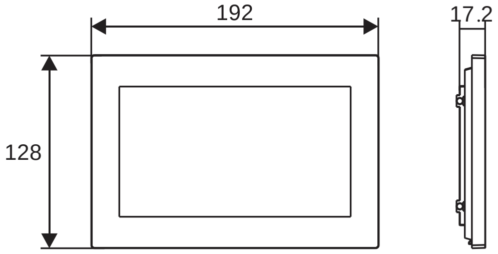
Dismantling



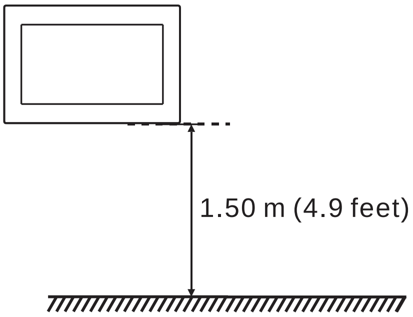
3.2.4 IP Touch Lite 7

Product dimension

(unit: mm)

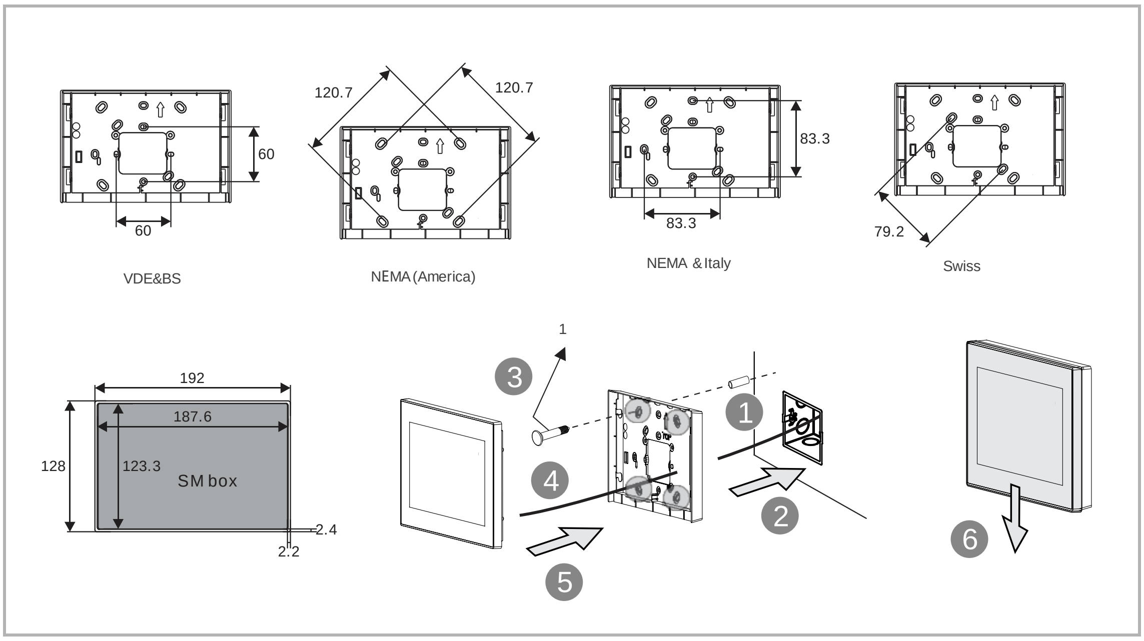


Installation height



Surface-mounted installation

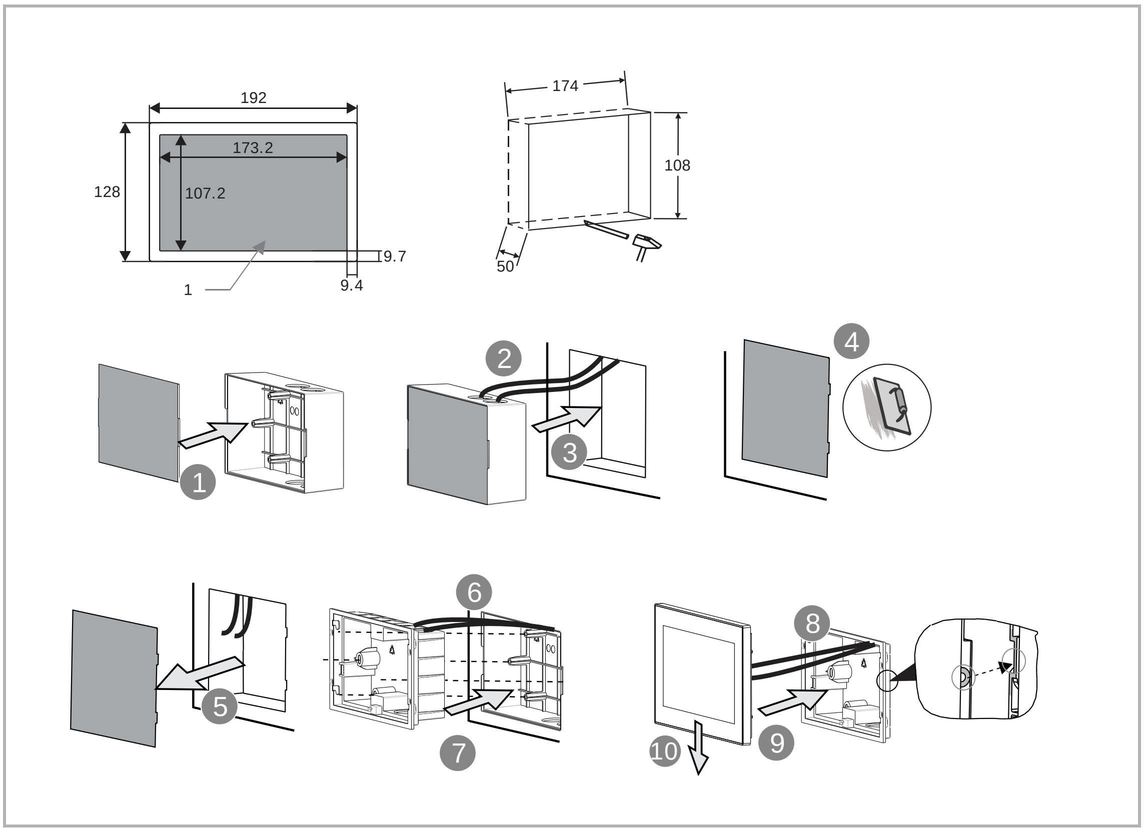
(unit: mm)



1	Screw the mounting bracket to accessory box. It is recommended to lock the positions marked in grey with screws to better secure the device.

Flush-mounted installation with pre-installation box

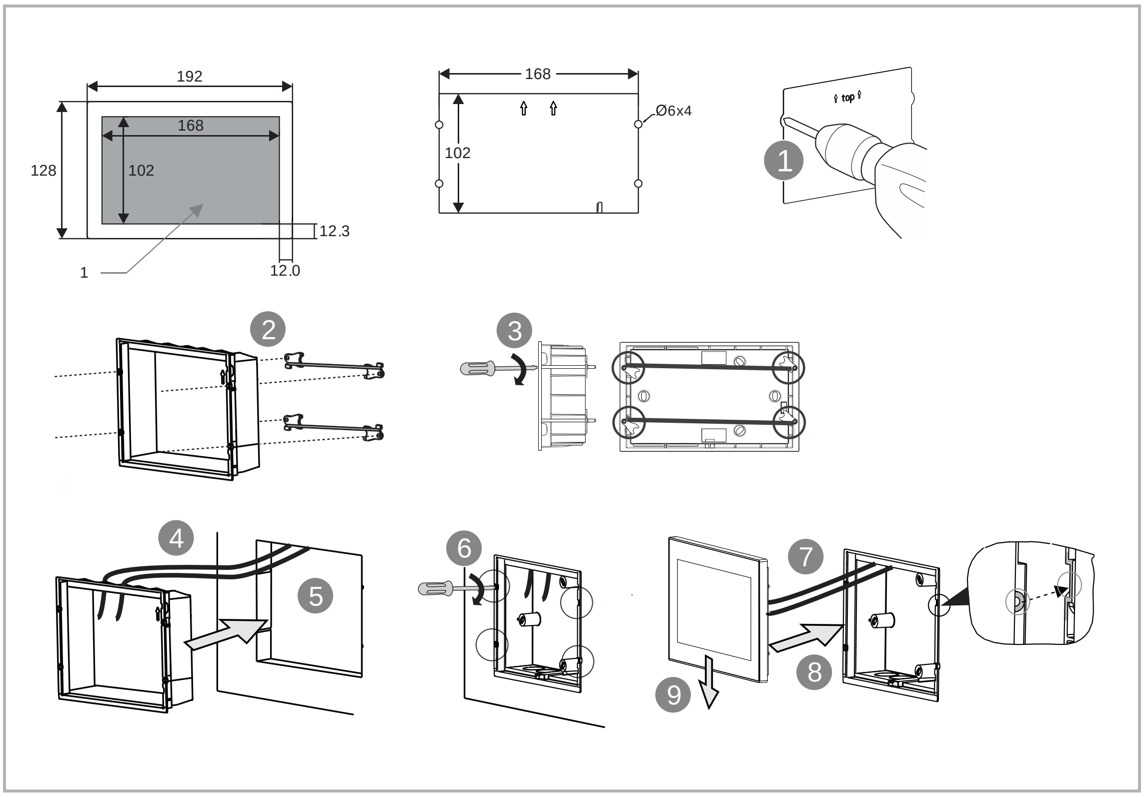
(unit: mm)



1	Hole size of pre-installation box

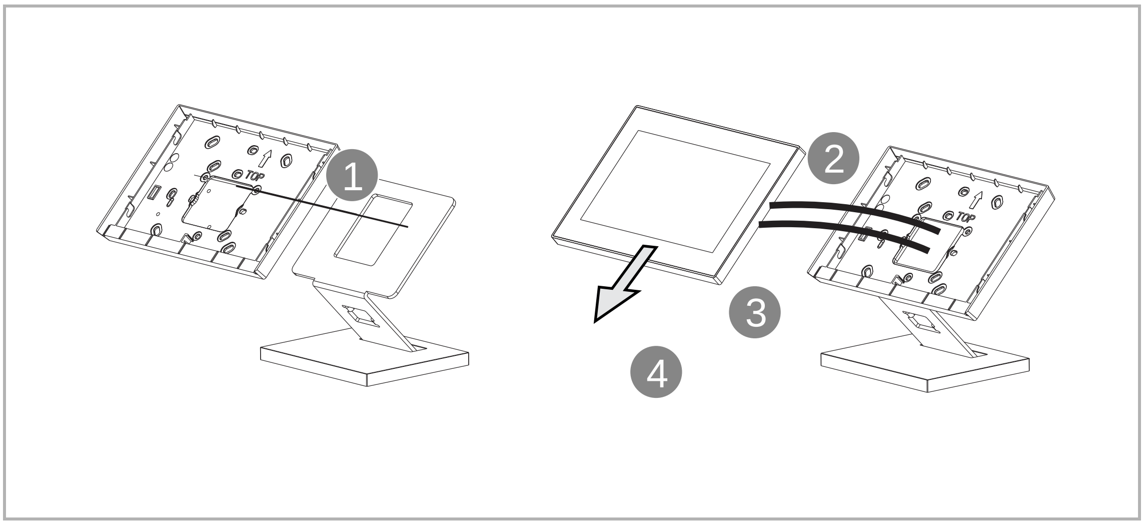
Flush-mounted installation in the hollow wall

(unit: mm)

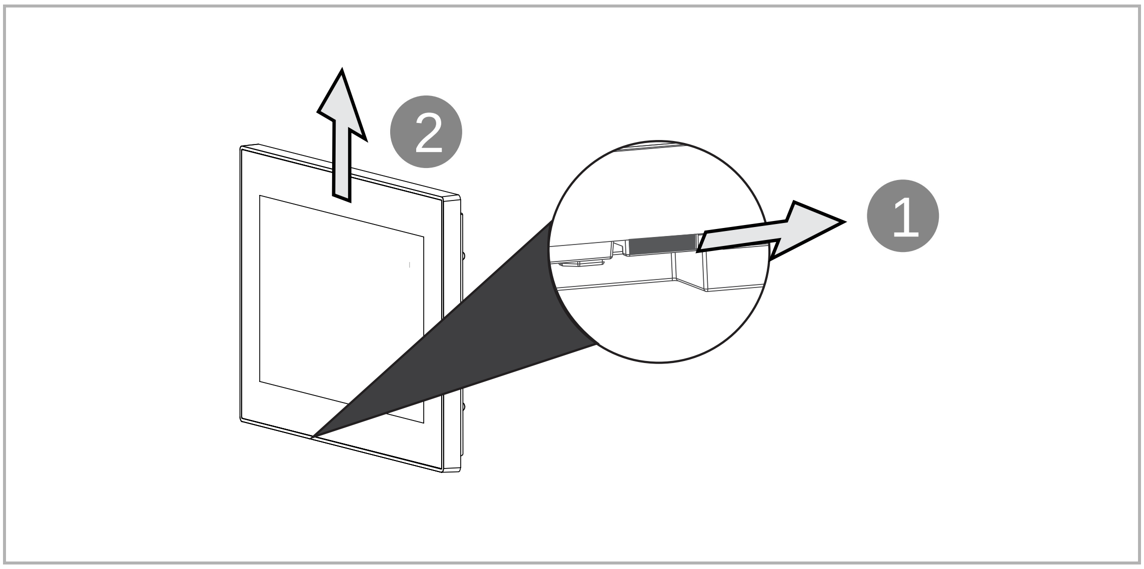


1	Hole size of flush-mounted box

Desktop installation



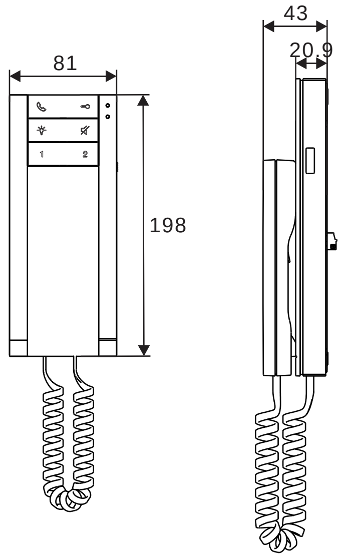
Dismantling



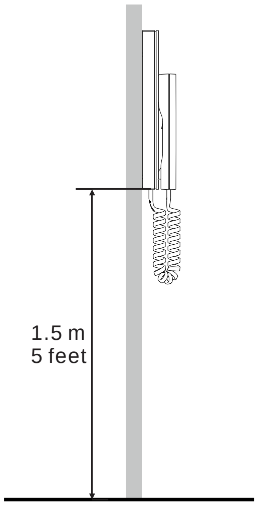
3.2.5 Audio IP

Product dimension

(unit: mm)

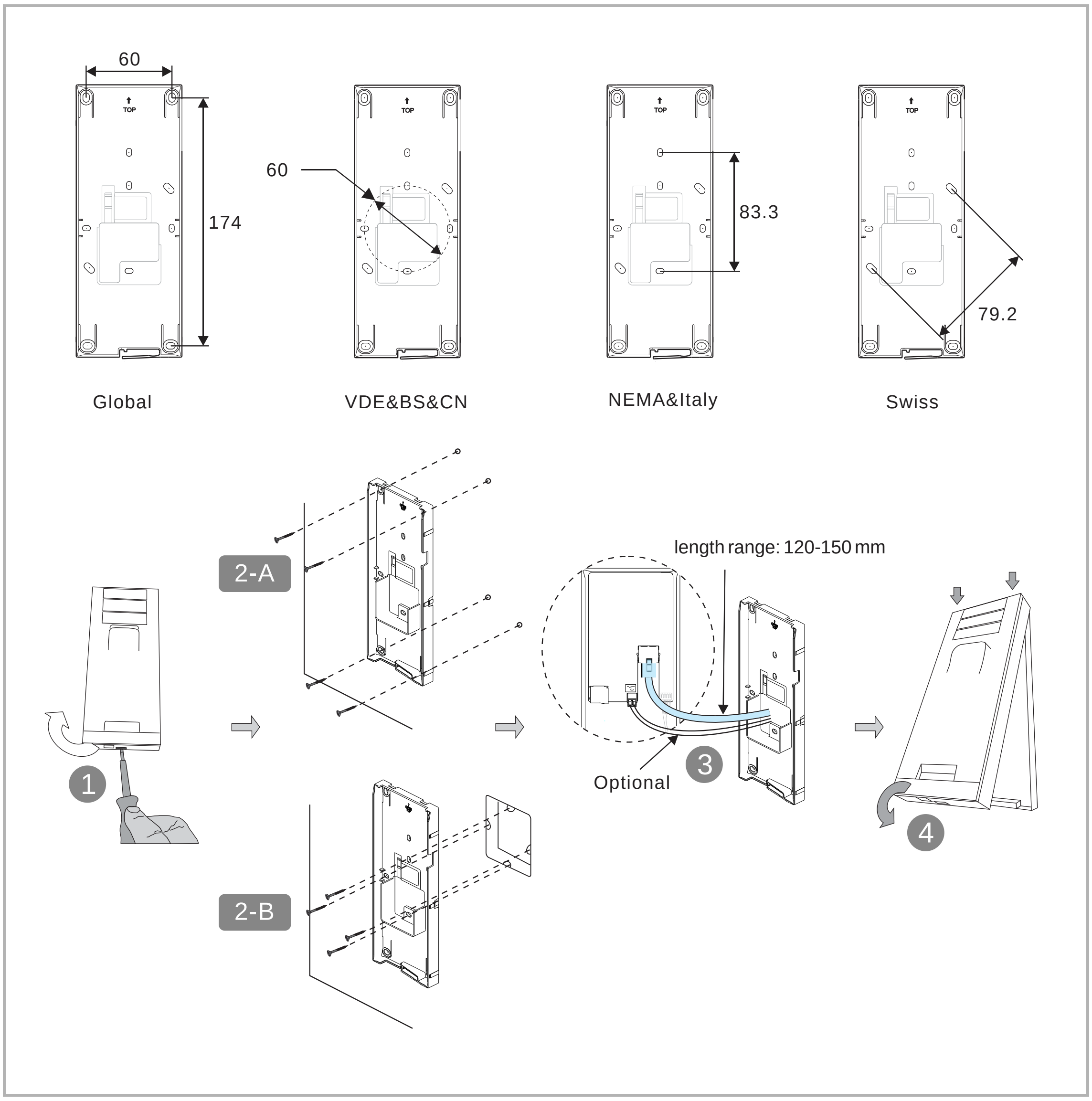


Installation height



Surface-mounted installation

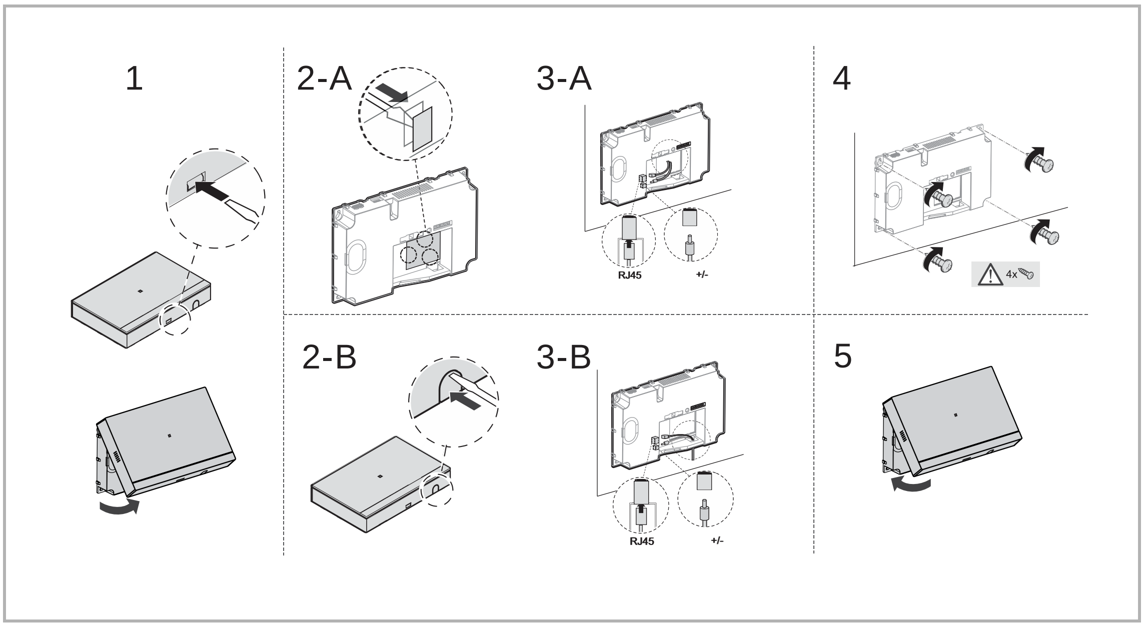
(unit: mm)



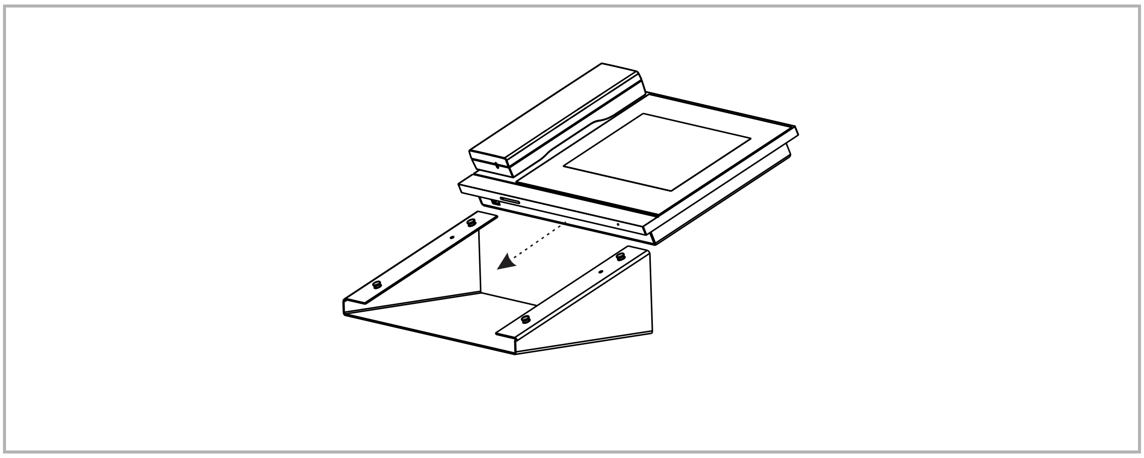
1	Disassemble the upper part from the bottom part by using a screwdriver.
2-A	Affix the bottom part on the wall.
2-B	Affix the bottom part on the box.
3	Connect the wires.
4	Latch the upper part onto the bottom part.

3.3 System devices

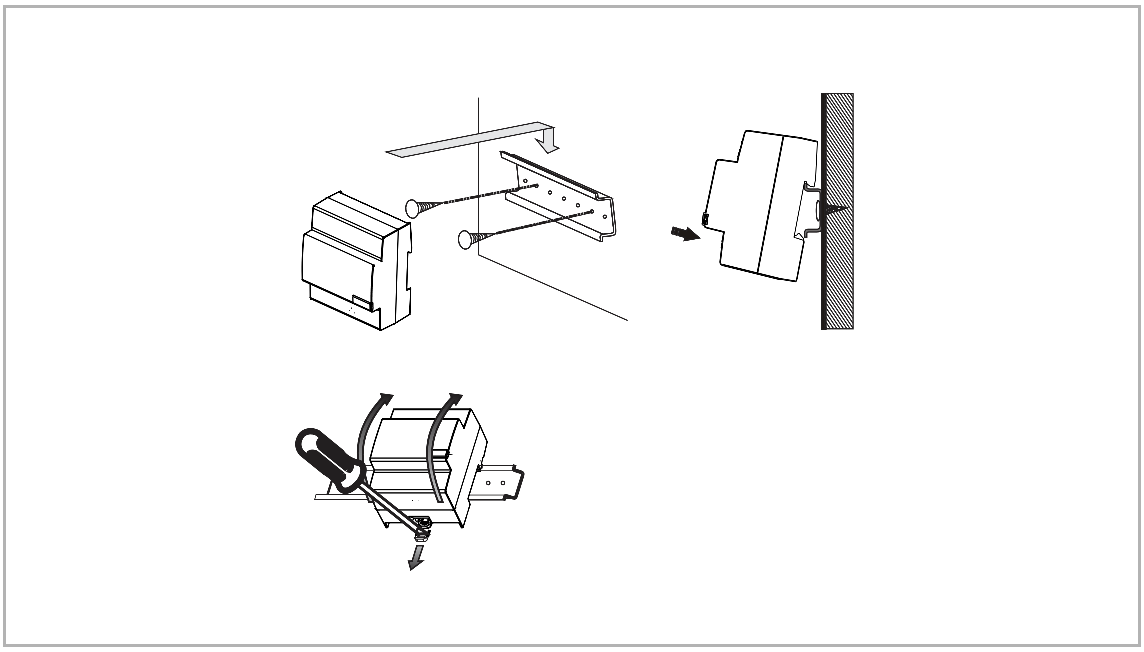
3.3.1 Smart Access Point



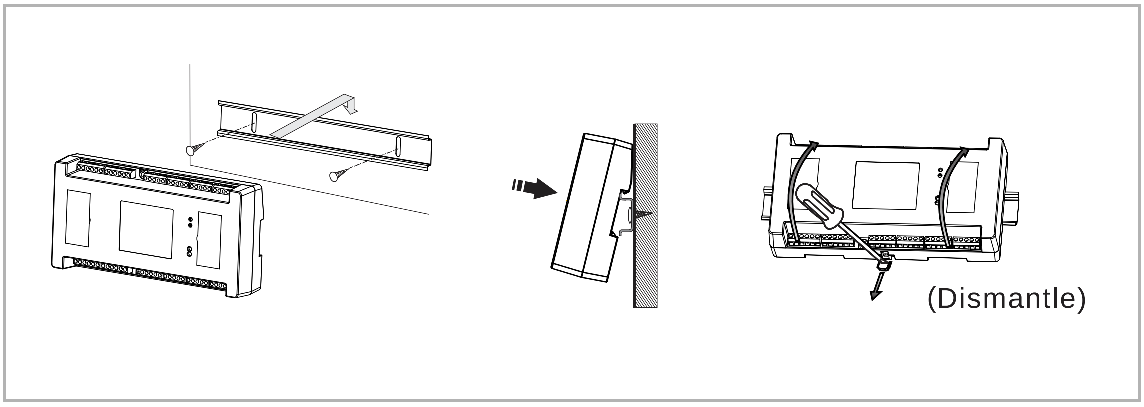
3.3.2 Guard Unit



3.3.3 IP Actuator and IP Elevator Controller



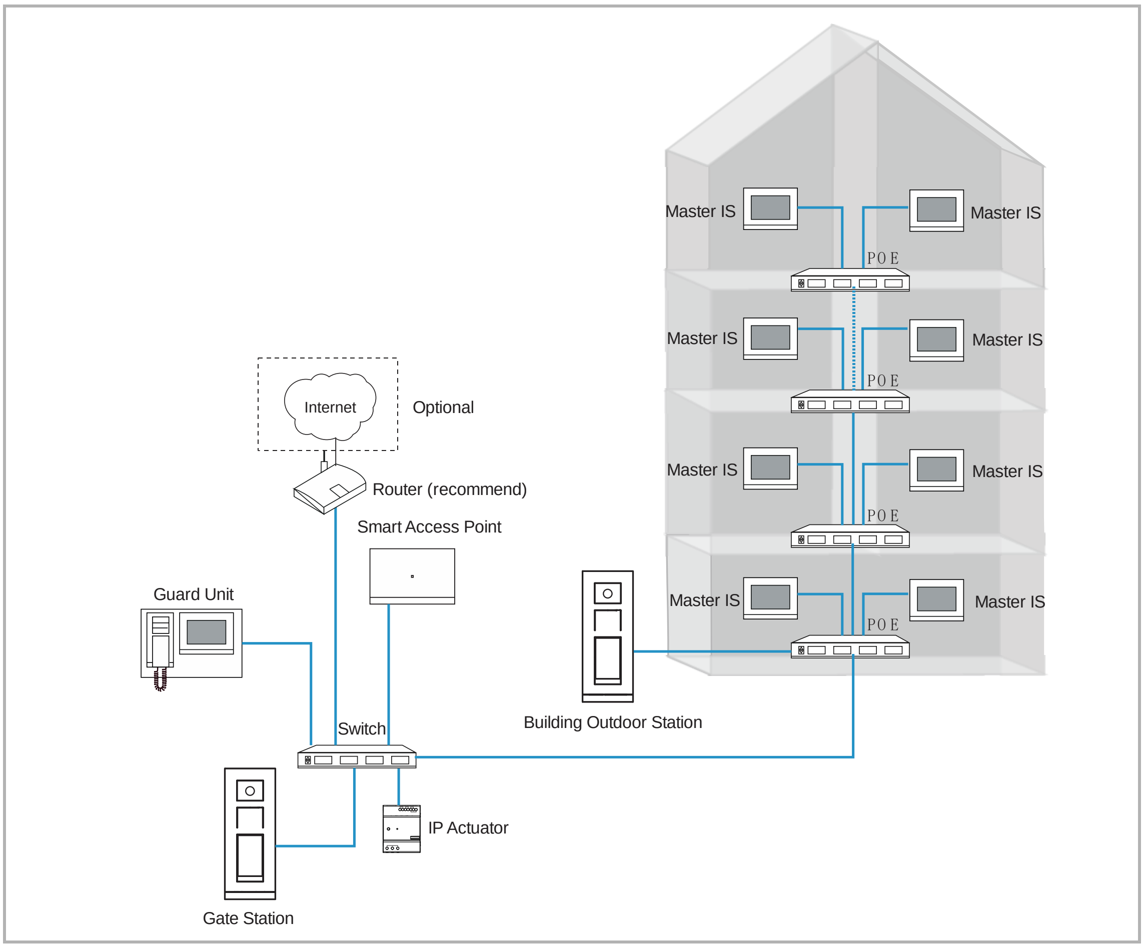
3.3.4 Lift Control Relay Module



4 Configuration Process

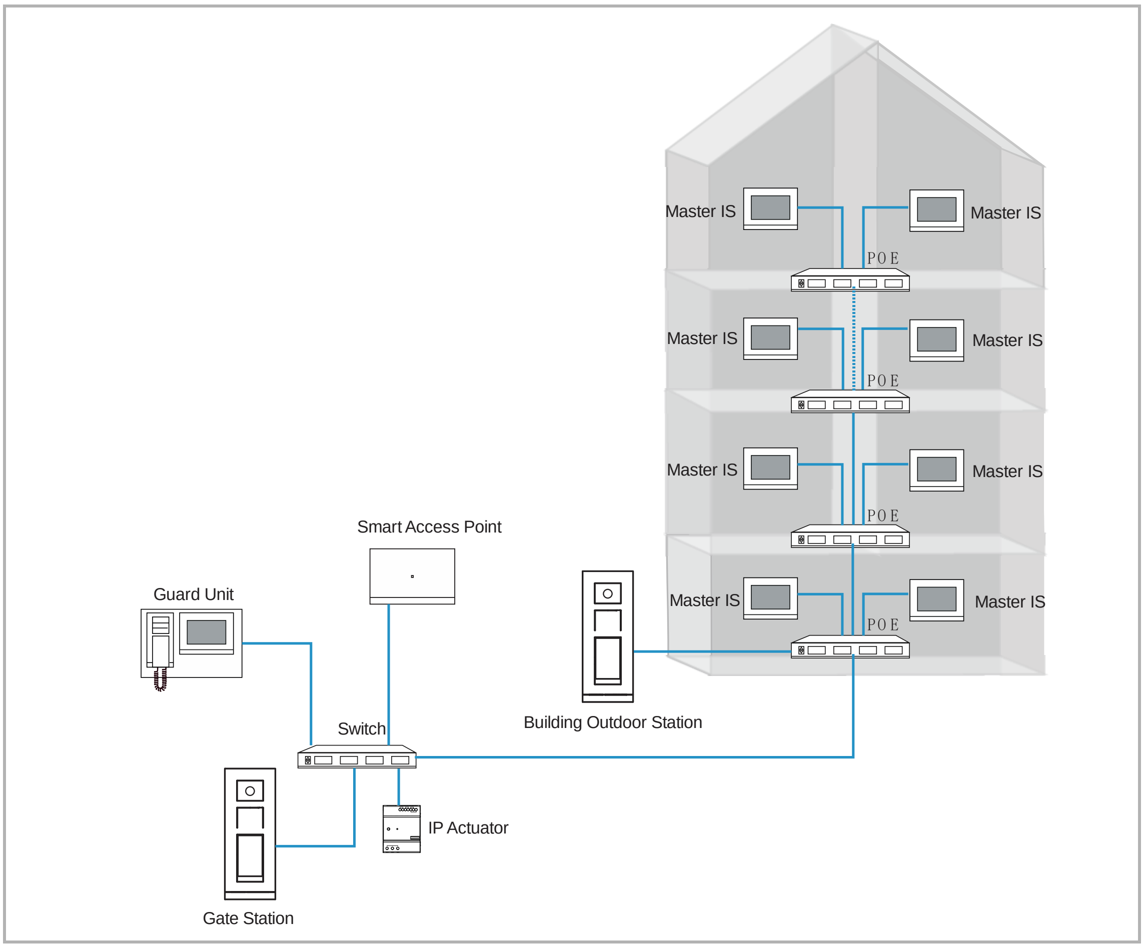
4.1 Multi Apartment Configuration with the SmartAP

4.1.1 Topology (DHCP)



- In this case, a SmartAP is needed.
- If the devices obtain the address from a DHCP server, a router is needed. Otherwise, a router is optional.
- Limitations for private devices used per single unit: up to 8 IS, 4 second confirmed OS, 4 IPA.

4.1.2 Topology (Legacy)



- In this case, a SmartAP is needed.
- Limitations for private devices used per single unit: up to 4 IS, 2 second confirmed OS, 2 IPA.

4.1.3 Adding devices via the SmartAP auto scan

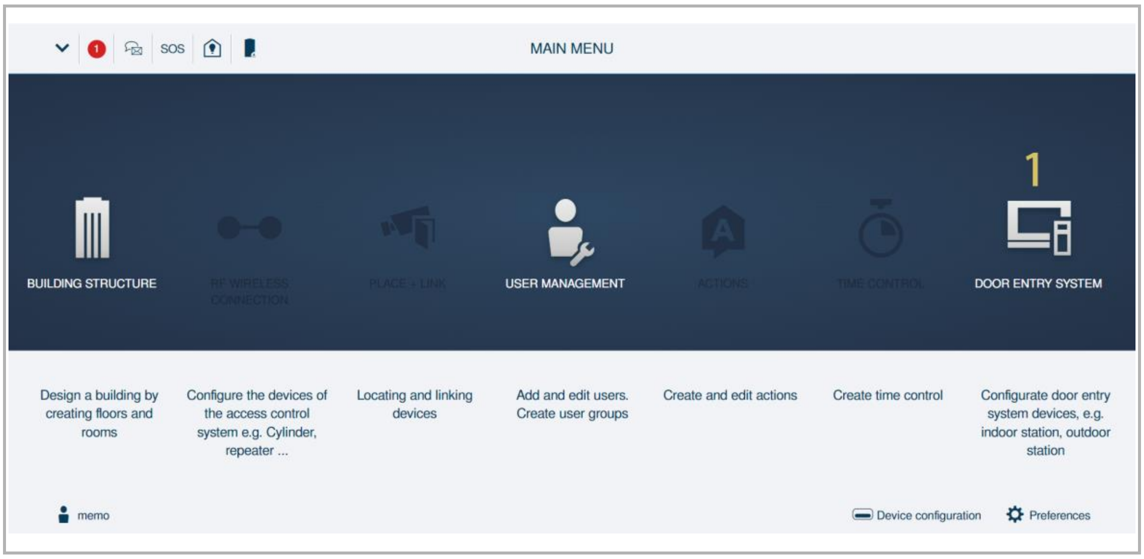
Note

Only the devices on the same network segment as the SmartAP can be added via the SmartAP auto scan.

- Audio IP and IP Elevator Controller cannot be added via the SmartAP auto scan. They should be added via the SmartAP manually. see chapter 4.1.4 “Adding devices via the SmartAP manually“ on page 138.
- All the devices to be added via the SmartAP auto scan should be set a different physical address before scanning.see chapter 10.4 “Configuring the physical address and IP mode“ on page 259.
- All the devices to be added via the SmartAP auto scan should not be signed by another SmartAP. If the devices have been signed by another SmartAP, you will need to clear the signatures.see chapter 10.3 “Clearing the signature of the device“ on page 258.
- Please ensure all the devices have been powered on.
- Please ensure the SmartAP has complete its initial setup before the configuration.see chapter 10.1 “Initial setup of the SmartAP“ on page 233.

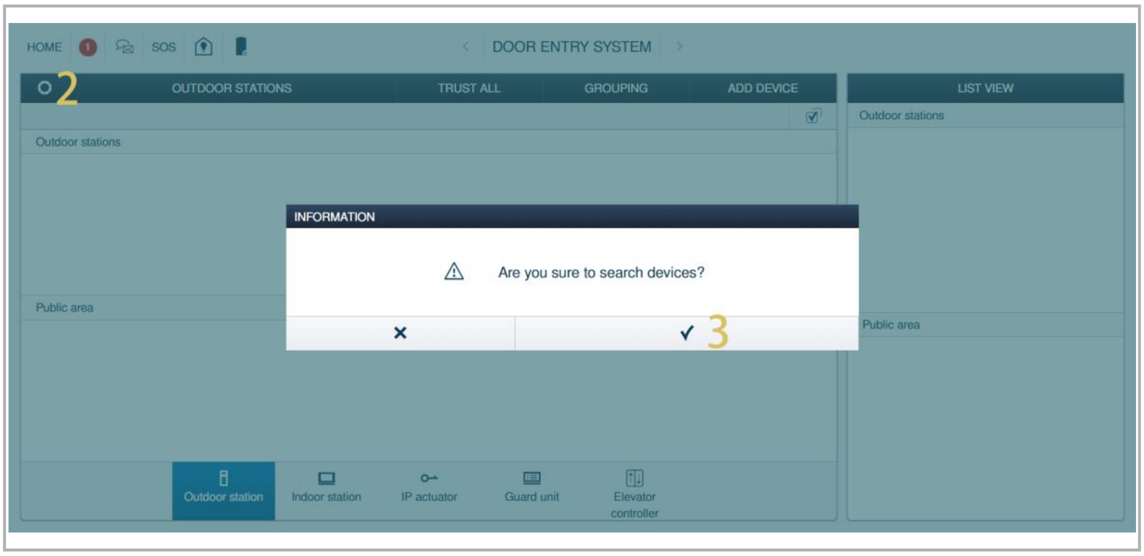
Please follow the steps below:

[1] On the "Main Menu" screen, click "Door entry system" to access the corresponding screen.

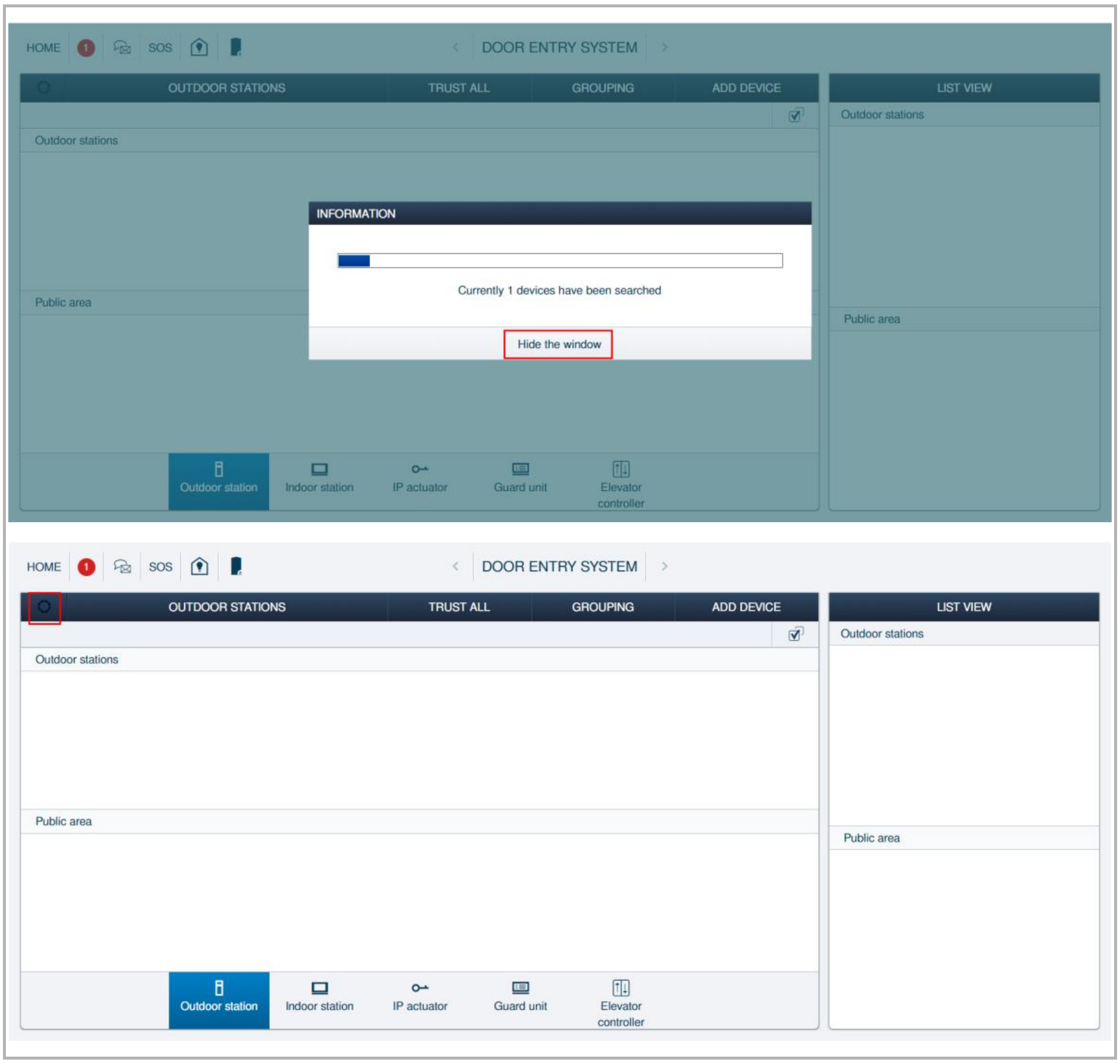

MAIN MENU
SOS
1
BUILDING STRUCTURE
RF WIRELESS CONNECTION
PLACE + LINK
USER MANAGEMENT
ACTIONS
TIME CONTROL
DOOR ENTRY SYSTEM
Design a building by creating floors and rooms
Configure the devices of the access control system e.g. Cylinder, repeater ...
Locating and linking devices
Add and edit users. Create user groups
Create and edit actions
Create time control
Configure door entry system devices, e.g. indoor station, outdoor station
memo
Device configuration
Preferences

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

[3] Click " √ " to continue.



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

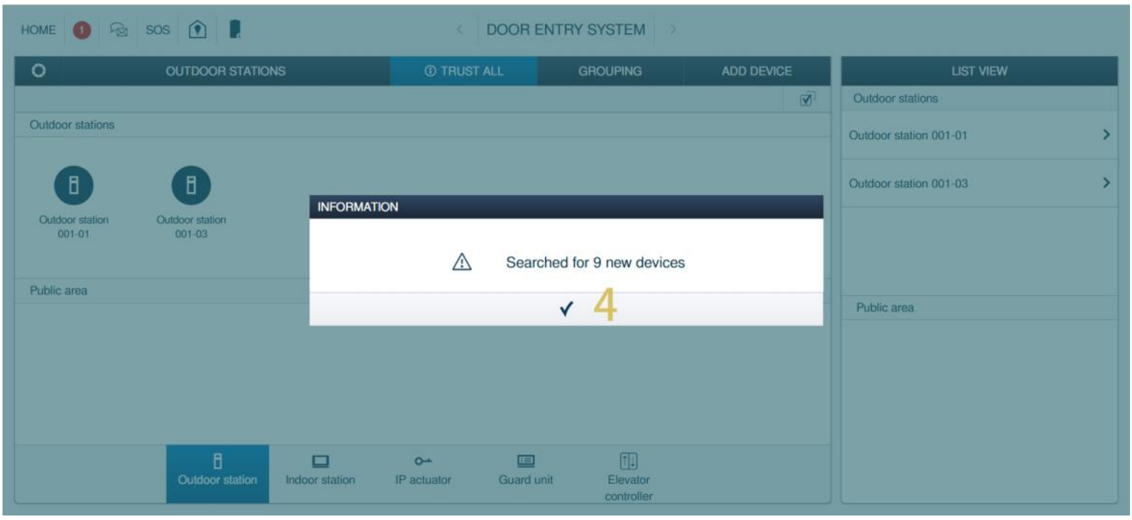


INFORMATION

Currently 1 devices have been searched

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

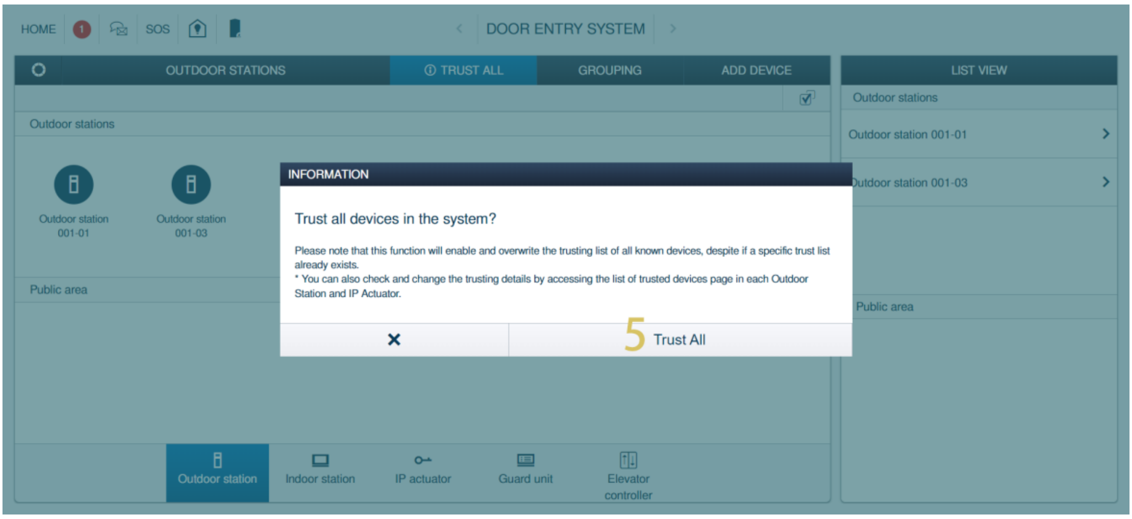
[5] Click "Trust All" to trust all devices in the system. For more details, see the "Trusting all devices" chapter on page XXX.



INFORMATION

Searched for 9 new devices

✓



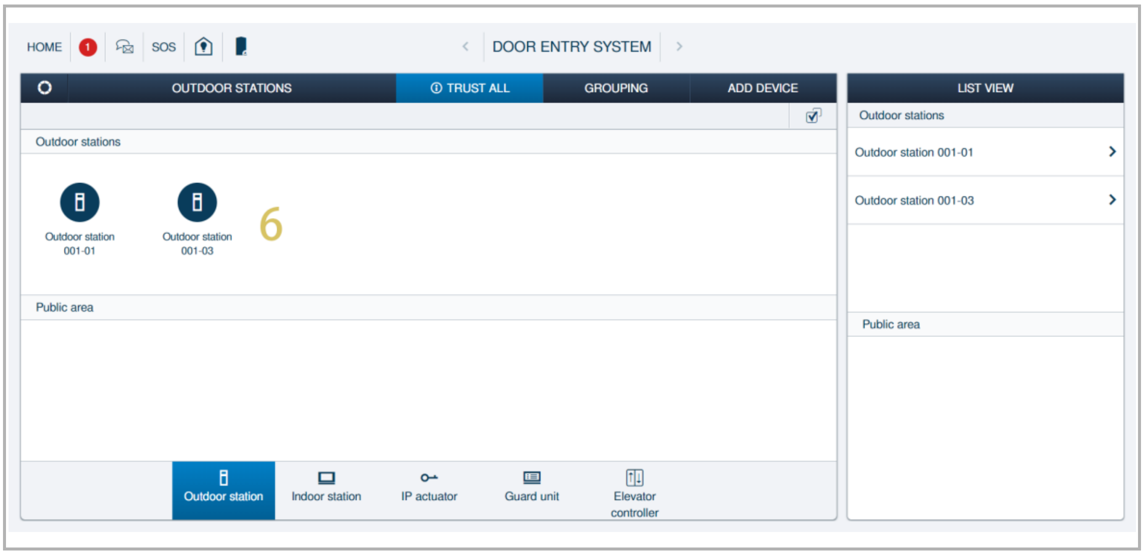
INFORMATION

Trust all devices in the system?

Please note that this function will enable and overwrite the trusting list of all known devices, despite if a specific trust list already exists.
* You can also check and change the trusting details by accessing the list of trusted devices page in each Outdoor Station and IP Actuator.

✕ Trust All

[6] The devices will be displayed on the screen if successful.



4.1.4 Adding devices via the SmartAP manually

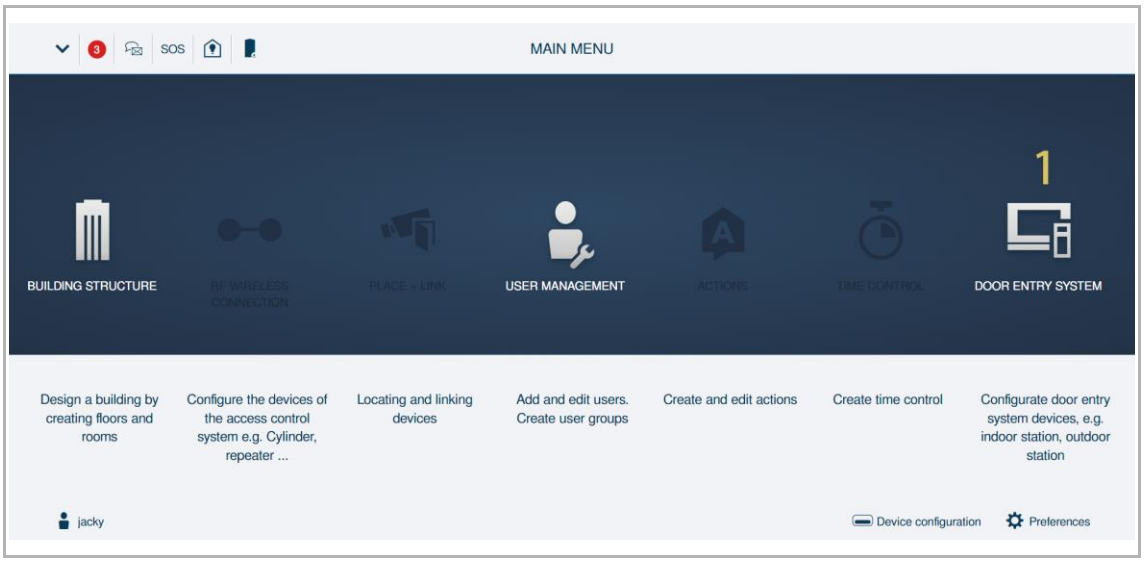
Note

All the devices can be added via the SmartAP manually.

- All the devices to be added via the SmartAP manually should not be signed by another SmartAP. If the devices have been signed by another SmartAP, you will need to clear the signatures.see chapter 10.3 “Clearing the signature of the device“ on page 258.
- Please ensure all the devices have been powered on.
- Please ensure the SmartAP has complete its initial setup before the configuration. see chapter 10.1 “Initial setup of the SmartAP“ on page 233.

Please follow the steps below:

[1] On the "Main Menu" screen, click "Door entry system" to access the corresponding screen.



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

Note

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

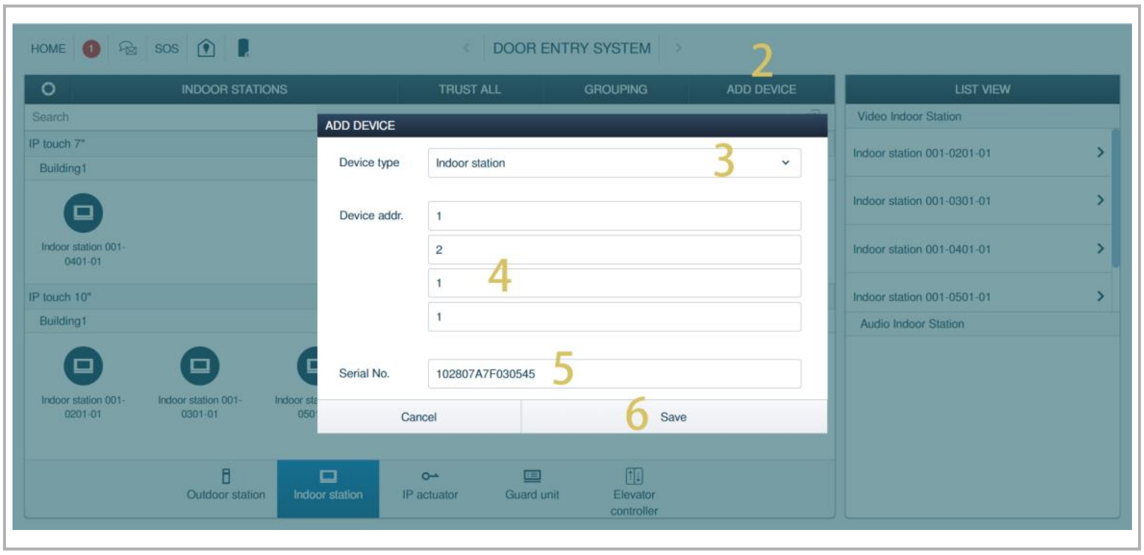
[3] Select a device type from the drop-down list (e.g. "Indoor station").

[4] Enter the physical address:

- Enter block number.
- Enter floor number.
- Enter room number.
- Enter device number.

[5] Enter serial number.

[6] Click "Save" to save.



ADD DEVICE

Device type: Indoor station

Device addr.: 1 / 2 / 1 / 1

Serial No.: 102807A7F030545

4.1.5 Adding devices via the SmartAP & APP

Note
All the devices can be added via the SmartAP & APP.

- All the devices to be added via the SmartAP & APP should not be signed by another SmartAP. If the devices have been signed by another SmartAP, you will need to clear the signatures.see chapter 10.3 “Clearing the signature of the device“ on page 258.
- Please ensure all the devices have been powered on.
- Please ensure the SmartAP has complete its initial setup before the configuration.see chapter 10.1 “Initial setup of the SmartAP“ on page 233.

QR code of the device

Usually there is a QR code attached to the back of the device. The serial number can be obtained by scanning this QR code.

Adding devices on the APP

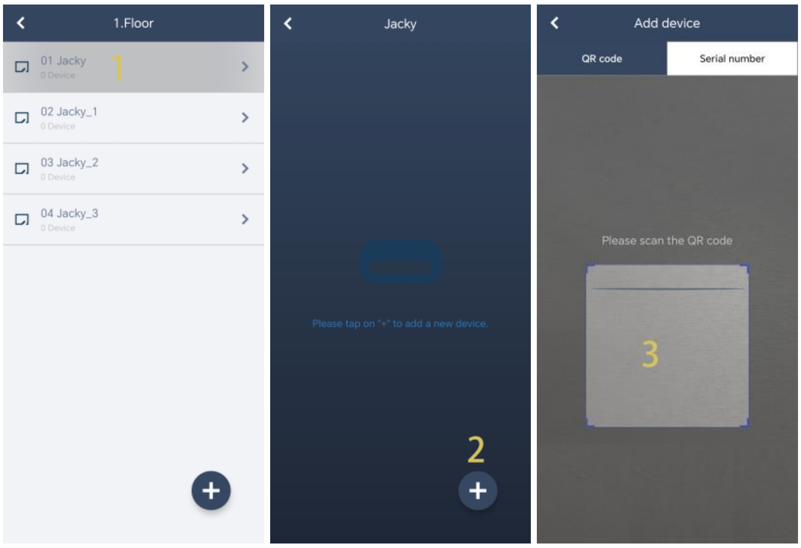
- Please ensure a building structure has been created on APP..

Please follow the steps below:

[1] On the designated floor screen, tap the designated room.

[2] On the designated room screen, tap " ⊕ ".

[3] On the "Add device" screen, scan the QR code displayed on the panel.



Please tap on "+" to add a new device.

Please scan the QR code

[4] On the "Device" screen, serial number of the device will be displayed.

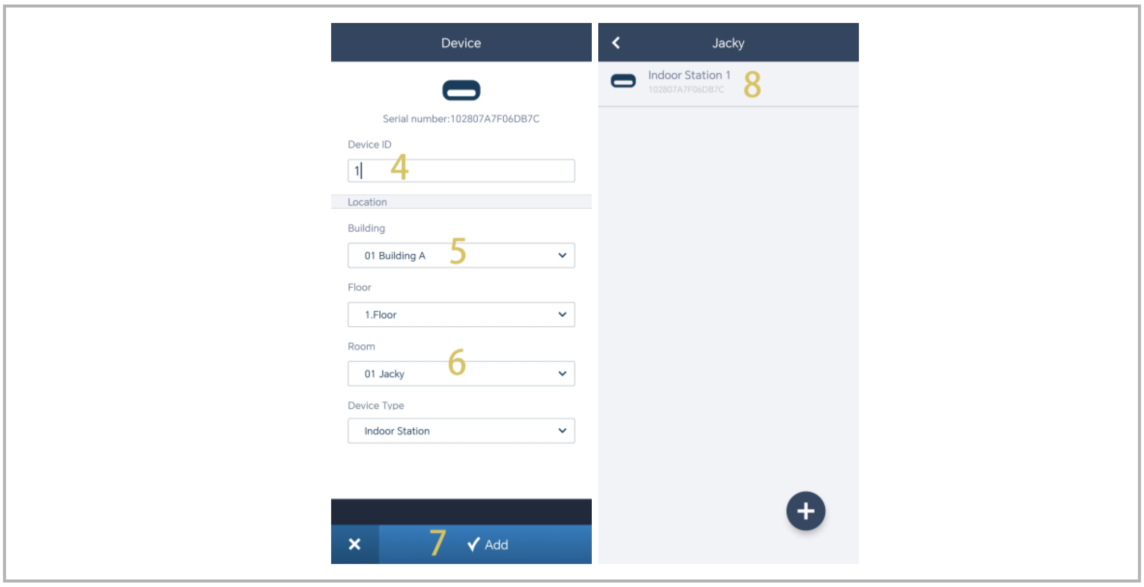
[5] Check the location.

[6] Check the device type.

[7] Tap "Add" to add a new device.

[8] The result is displayed on the screen if successful.

Repeat steps 1~7 to add multiple devices.



Device

Serial number:102807A7F06DB7C

Device ID: 1

Location

Building: 01 Building A

Floor: 1.Floor

Room: 01 Jacky

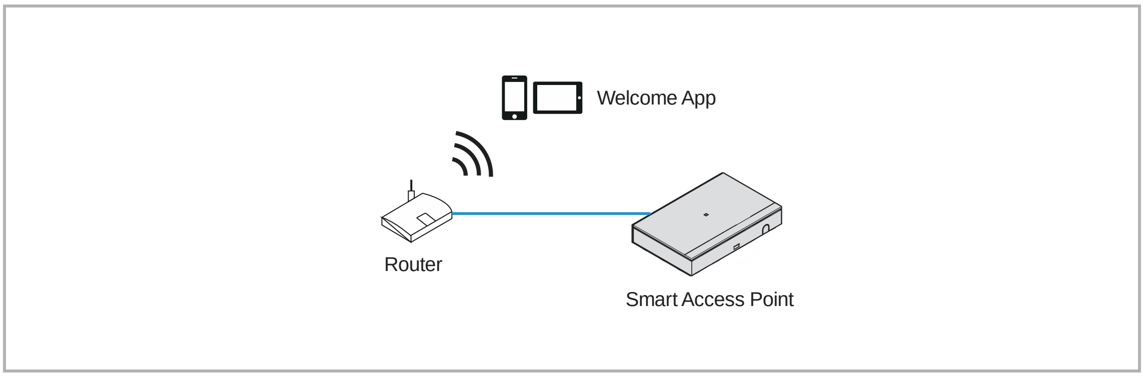
Device Type: Indoor Station

Importing the building structure from APP to SmartAP

- SmartAP can import the building created in the APP.
- You can import one building once or several buildings as a batch.

Precondition

- The APP must be on the same network with SmartAP.
- The building structure has been created in the APP.



Importing rule

The 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.

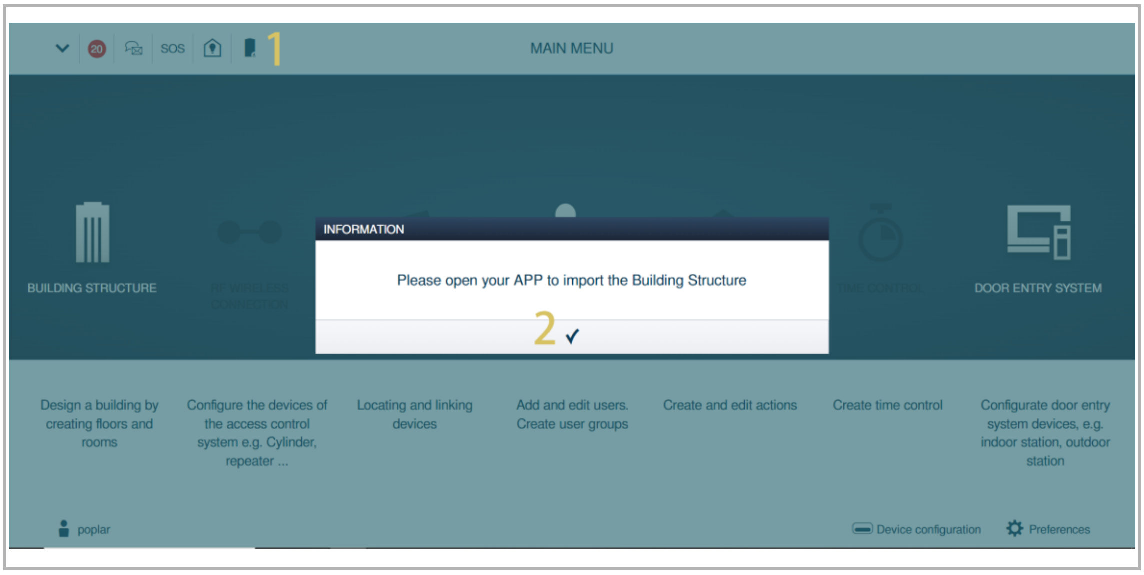
APP	SmartAP before	SmartAP after
B+	A, B, C	A, B+, C
B+, C+	A, B, C	A, B+, C+
D, E, F	A, B, C	A, B, C, D, E, F

Importing process

Please follow the steps below:

[1] On the home screen of the SmartAP, click " ▮ ".

[2] A pop-up window will appear, please keep the window open and do not click "√".



INFORMATION

Please open your APP to import the Building Structure

1
MAIN MENU
SOS
20
BUILDING STRUCTURE
DOOR ENTRY SYSTEM
2 ✓
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
Configure door entry system devices, e.g. indoor station, outdoor station
poplar
Device configuration
Preferences

[3] On the "Projects" screen of the APP, swipe the designated project name to the right.

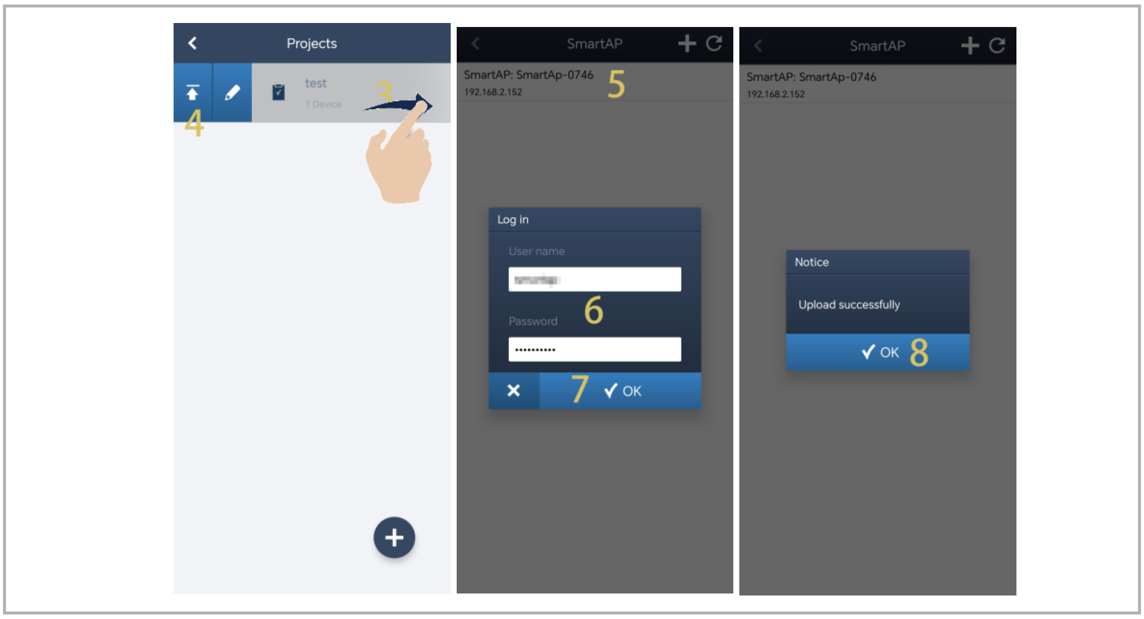
[4] Tap " ⇧ ".

[5] Tap the designated SmartAP in the list.

[6] Enter the account and the password of the designated SmartAP.

[7] Tap "OK".

[8] "Upload successfully" will be displayed if successful. Tap "OK".



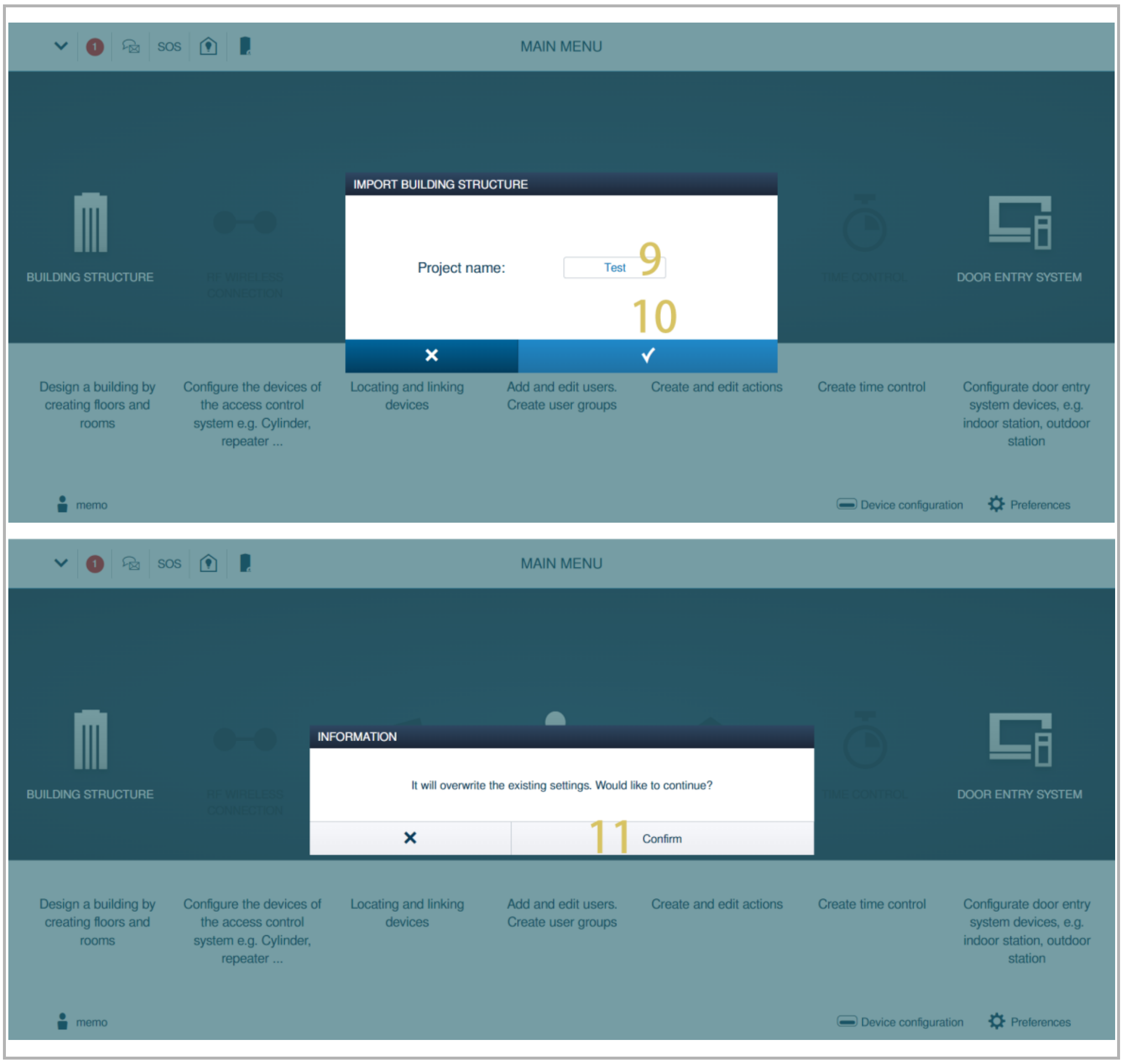
Notice

Upload successfully

[9] On the configuration screen of SmartAP, the project name will be displayed on the screen.

[10]Click "√".

[11]Click "Confirm".



IMPORT BUILDING STRUCTURE

Project name: Test

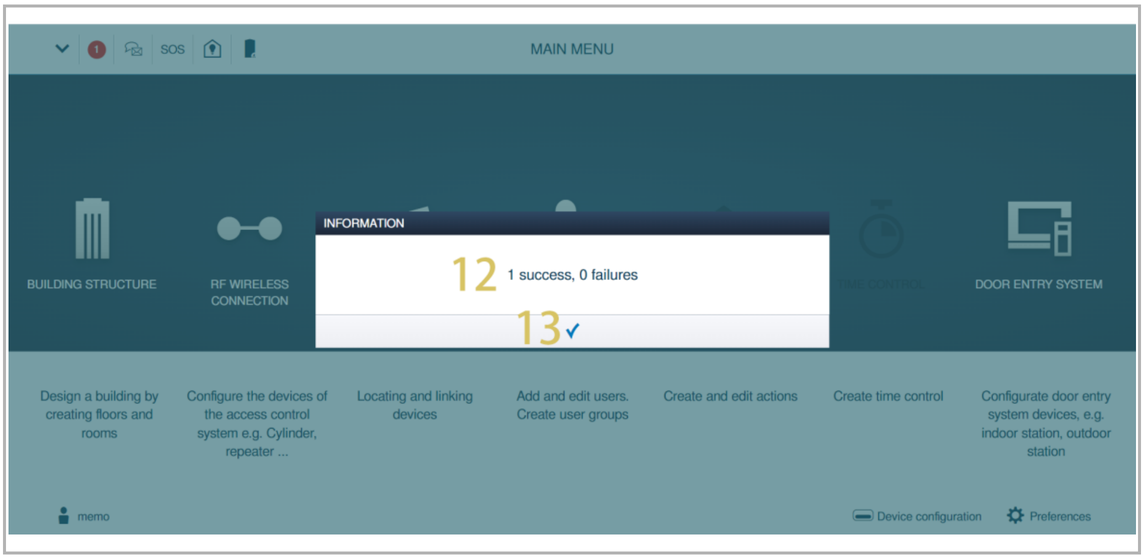
INFORMATION

It will overwrite the existing settings. Would like to continue?

SOS
MAIN MENU
BUILDING STRUCTURE
RF WIRELESS CONNECTION
TIME CONTROL
DOOR ENTRY SYSTEM
9
10
✕
✓
11
Confirm
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
memo
Device configuration
Preferences

[12]The import result will be displayed.

[13]Click "√" to complete the import process.


SOS
MAIN MENU
BUILDING STRUCTURE
RF WIRELESS CONNECTION
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
memo
Device configuration
Preferences
12
13
✓

INFORMATION

1 success, 0 failures

4.1.6 Devices Diagnosis

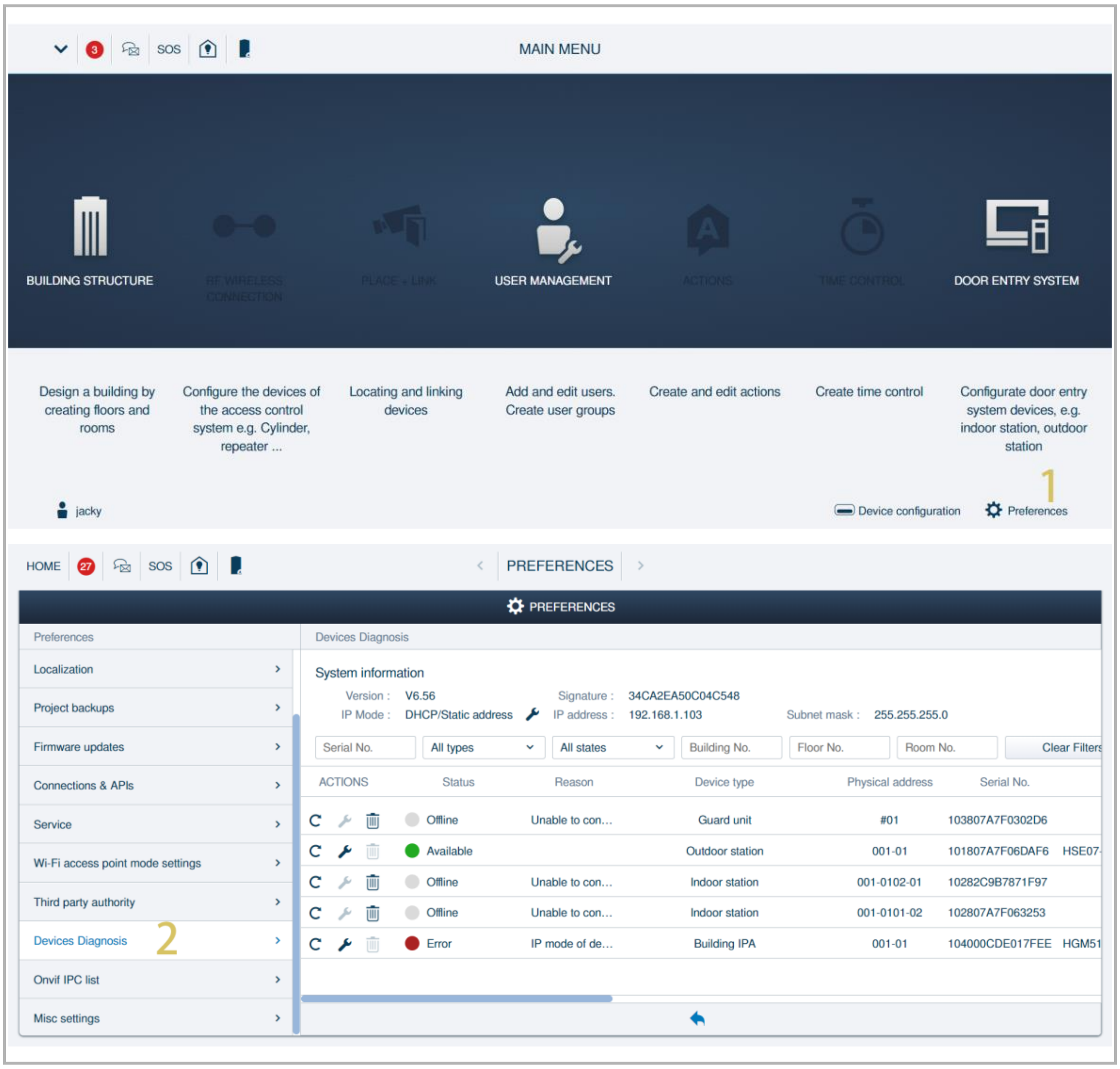
It is recommended to check the status of all devices to ensure normal use.

Access the "Devices Diagnosis" screen

Please follow the steps below:

[1] On the "Main Menu" screen, click "Preferences".

[2] Click "Devices Diagnosis" to access the corresponding screen.

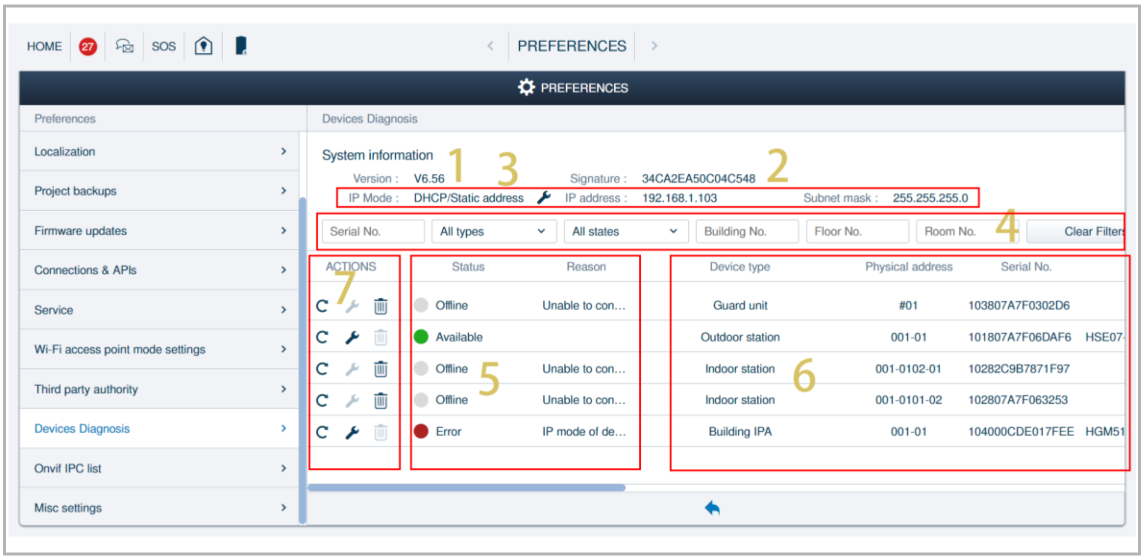


System information

Version : V6.56
Signature : 34CA2EA50C04C548
IP Mode : DHCP/Static address
IP address : 192.168.1.103
Subnet mask : 255.255.255.0

ACTIONS	Status	Reason	Device type	Physical address	Serial No.	
	○ Offline	Unable to con…	Guard unit	#01	103807A7F0302D6	
	● Available		Outdoor station	001-01	101807A7F06DAF6	HSE07-
	○ Offline	Unable to con…	Indoor station	001-0102-01	10282C9B7871F97	
	○ Offline	Unable to con…	Indoor station	001-0101-02	102807A7F063253	
	● Error	IP mode of de…	Building IPA	001-01	104000CDE017FEE	HGM51

Overview of Devices Diagnosis



System information

Version : V6.56 Signature : 34CA2EA50C04C548

IP Mode : DHCP/Static address 🔧 IP address : 192.168.1.103 Subnet mask : 255.255.255.0

Serial No. | All types | All states | Building No. | Floor No. | Room No. | Clear Filters

ACTIONS	Status	Reason	Device type	Physical address	Serial No.	
⟳ 🔧 🗑	⚪ Offline	Unable to con…	Guard unit	#01	103807A7F0302D6	
⟳ 🔧 🗑	🟢 Available		Outdoor station	001-01	101807A7F06DAF6	HSE07-
⟳ 🔧 🗑	⚪ Offline	Unable to con…	Indoor station	001-0102-01	10282C9B7871F97	
⟳ 🔧 🗑	⚪ Offline	Unable to con…	Indoor station	001-0101-02	102807A7F063253	
⟳ 🔧 🗑	🔴 Error	IP mode of de…	Building IPA	001-01	104000CDE017FEE	HGM51

No.	Description
1	Software version of the SmartAP
2	**Signature of the SmartAP** If the signature of the device which is displayed on the "Signature" column is not the same as the signature of this SmartAP, "Error" will be displayed.
3	**IP mode of the SmartAP** Click " 🔧 " to change the IP mode of the SmartAP.
4	**Filters** ▪ It is allowed to display the designated devices according to the filters (e.g., "Serial no.", "Device type", "States" etc.) ▪ Click "Clear Filters" to empty the filters.
5	**Status of the devices** 🟢 Available= The device has been added by the SmartAP successfully 🔴 Error = The device has been detected by the SmartAP but failed to be added ⚪ Offline = The device has not been detected by the SmartAP.
6	Other information of the devices
7	**Actions of the devices** Click " 🔧 " to configure the IP mode and the IP address of the device, you can also re-sign the device here. Click " ⟳ " to refresh the status of the device. Click " 🗑 " to remove the device from the list.
8	**Refresh all** Click it to refresh the status of all the devices

Error diagnosis

"Abnormal" will be displayed due to the following problems.

- The same physical address has been set on different devices
- The same IP address has been set on different devices
- IP mode of this device is different from that of the SmartAP
- The IP address segment of this device is different from that of the SmartAP
- IP mode of Subsidiary IS is different from that of Master IS
- IP address segment of Subsidiary IS is different from that of Master IS
- If master IS is offline, the related Subsidiary IS, 2nd OS and Private IPA will turn to "Abnormal"
- When the IP mode is changed from DHCP/Static IP mode to legacy mode, the device number of the device is out of range.
- The signature of the device is different from that of the SmartAP.

Offline diagnosis

"Offline" will be displayed due to the following problems.

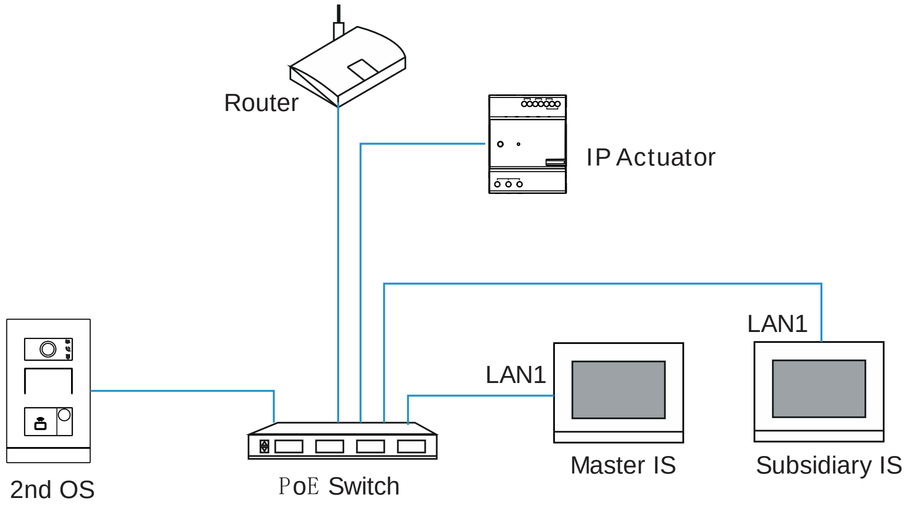
- The device is offline
- The device doesn’t obtain the IP address when IP mode is set to "DHCP".
- The serial number entered is not correct when adding the device manually.
- The IP address of the device conflicts with that of the SmartAP.
- The IGMP Snooping function is disabled on the router, multicast packets are suppressed.

4.1.7 Managing the trusted devices

For more details, see chapter 10.8 “Managing the trusted devices“ on page 293.

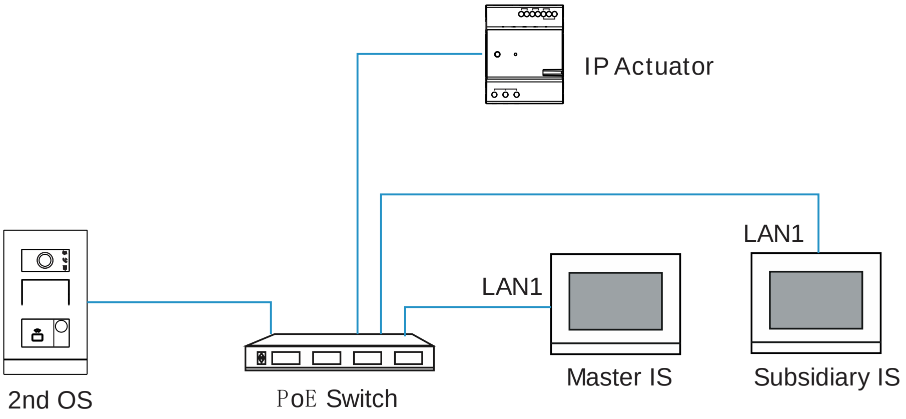
4.2 Single House Configuration without the SmartAP

4.2.1 Topology (DHCP)



- In this case, no SmartAP is needed.
- In this case, a router is needed for use.
- In this case, all devices are connected to the same network.
- In this case, 1 2nd confirmed Outdoor Station, 1 IP Actuator and max. 4 Indoor Stations are recommened.
- In this case, the 2nd OS could be an IP pushbutton OS or a Mini OS with IC.
- This configuration will be carried out on the Master IS.
- In this configuration, the IPA and 2nd OS will be added to the trusted devices list.

4.2.2 Topology (Legacy)



- In this case, no SmartAP is needed.
- In this case, all devices are connected to the same network.
- In this case, 1 2nd confirmed Outdoor Station, 1 IP Actuator and max. 4 Indoor Stations are recommended.
- In this case, the 2nd OS could be an IP pushbutton OS or a Mini OS with IC.
- This configuration will be carried out on the Master IS.
- In this configuration, the IPA and 2nd OS will be added to the trusted devices list.

4.2.3 Preparation

- Please ensure that all the devices have been connected according to the topology before the configuration.
- Please ensure all the devices have been powered on.
- Please ensure all the devices have been restored to factory default settings to prevent unknown abnormal results.see chapter 10.5 “Restoring to factory default“ on page 271.
- Please ensure all indoor stations connect to the switch via LAN1.

4.2.4 Configuring the Master IS

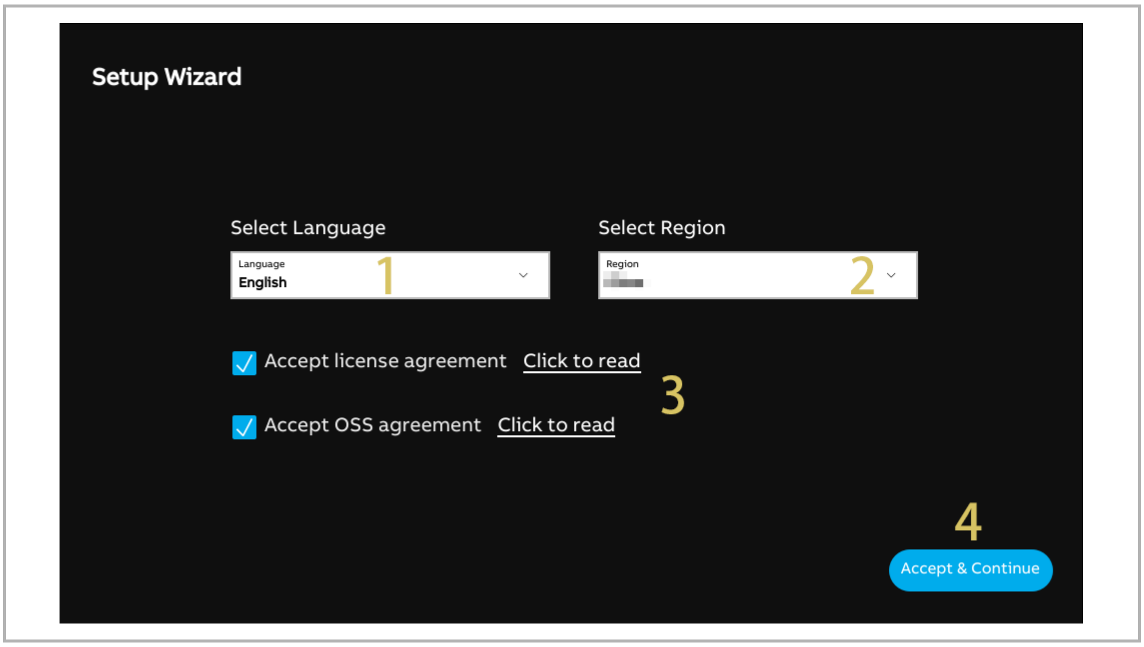
When the IS is powered on the first time or it is restored to factory default settings, it will access the "Setup Wizard". Please follow the steps below:

[1] On the "Setup wizard" screen, select the language from the drop-down list.

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

[3] Tick the check box to accept the licences. Or tap "Click to read" to view the details of the licence.

[4] Tap "Accept & continue" to access the next screen.



Setup Wizard

Select Language

Language: English

Select Region

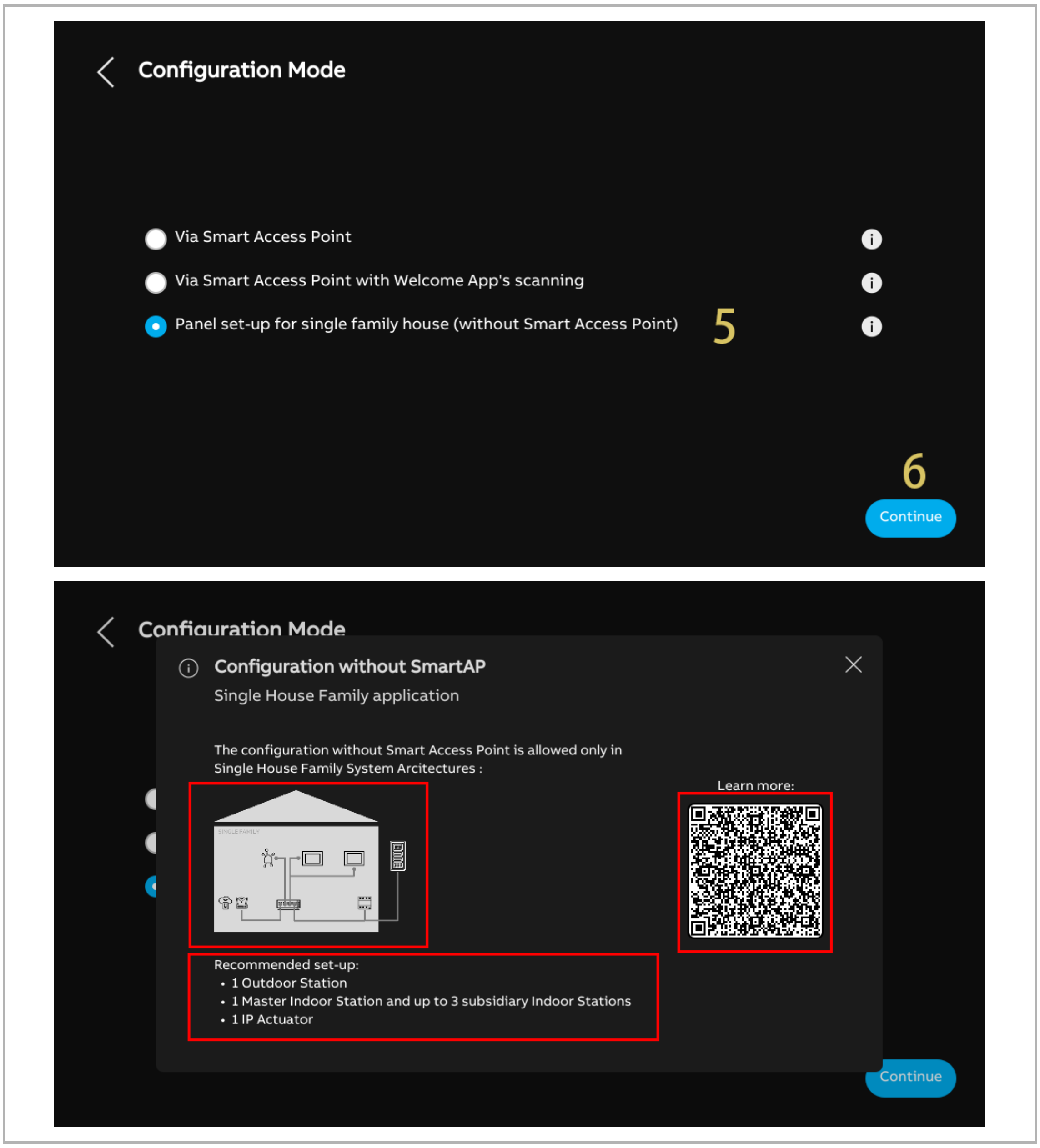
Region: [redacted]

☑ Accept license agreement Click to read

☑ Accept OSS agreement Click to read

[5] On the "Configuration Mode" screen, select "Panel set-up for single family house", tap " ⓘ " to see the system topology, system recommended capacity, and you can download the product manual by scanning the QR code on the right.

[6] Tap "Continue".



Configuration Mode

○ Via Smart Access Point ⓘ

○ Via Smart Access Point with Welcome App's scanning ⓘ

● Panel set-up for single family house (without Smart Access Point) ⓘ

Configuration without SmartAP

Single House Family application

The configuration without Smart Access Point is allowed only in Single House Family System Arcitectures :

Learn more:

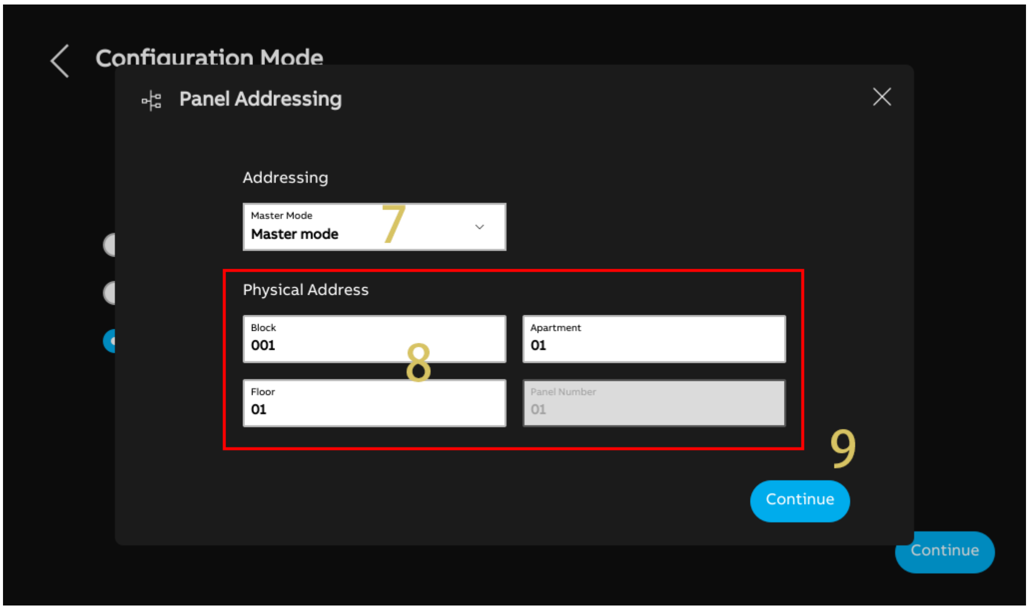
Recommended set-up:

- 1 Outdoor Station
- 1 Master Indoor Station and up to 3 subsidiary Indoor Stations
- 1 IP Actuator

[7] On the "Panel Addressing" screen, select "Master mode". Only one Indoor Station can be set to "Master mode" in the same apartment.

[8] Enter the block number, the floor number and the apartment number or accept the default value. The "Panel number" is preset as "01" and cannot be modified while the "Master mode" is selected.

[9] Tap "Continue".



Addressing

Master Mode: Master mode

Physical Address

Block: 001

Apartment: 01

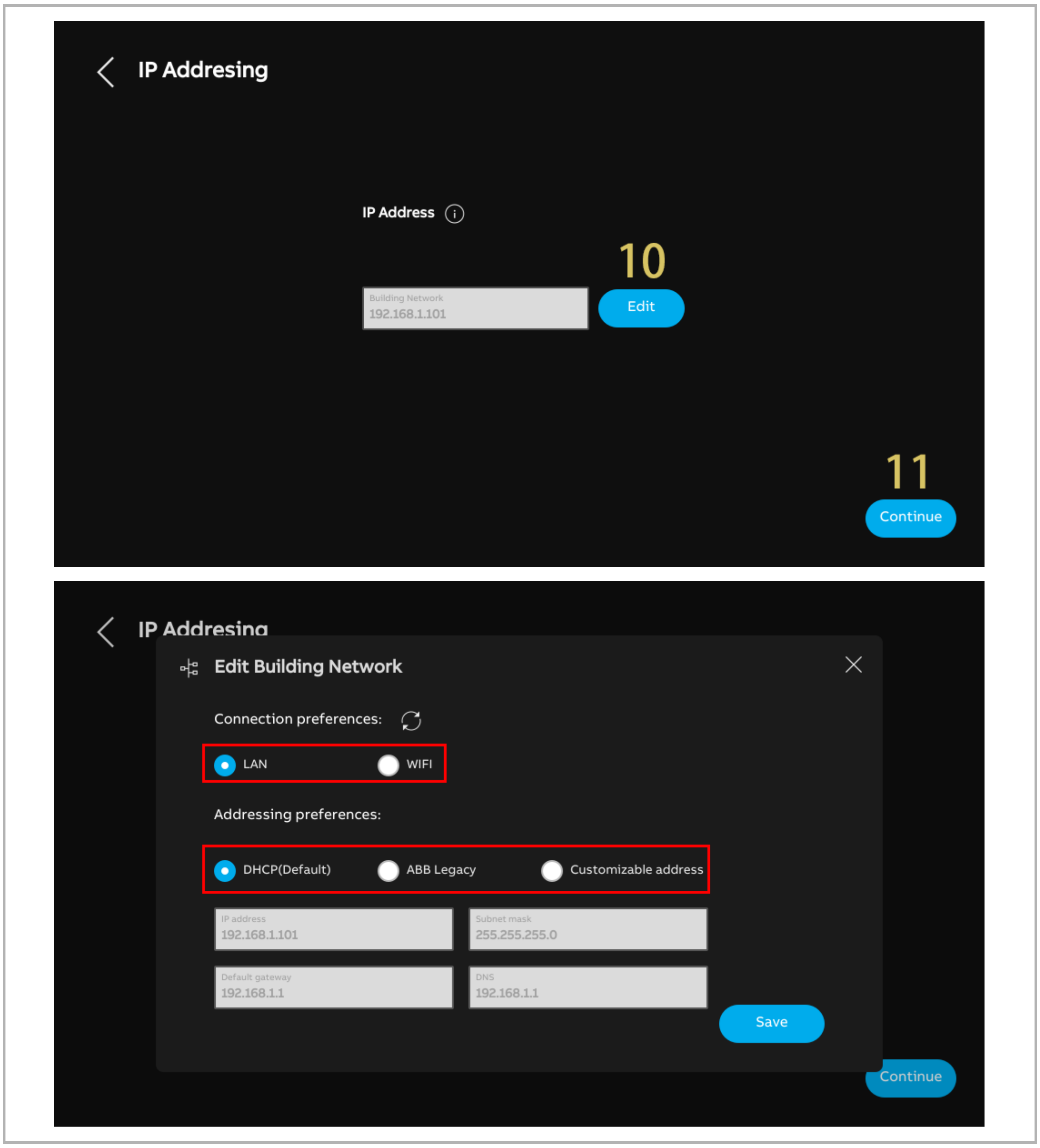
Floor: 01

Panel Number: 01

[10]On the "IP Addressing" screen, tap "Edit" to access the corresponding screen.

- Select the connection type, it can be set to "LAN" or "WiFi".
- Select the address type, it can set to "DHCP", "Customizable address" or "ABB Legacy". If "ABB Legacy" is selected, the IP address will be "10.0.x.x".
- Please tap "Save" if the settings have been changed.

[11]Tap "Continue".



IP Address

Building Network: 192.168.1.101

Connection preferences:

● LAN ○ WIFI

Addressing preferences:

● DHCP(Default) ○ ABB Legacy ○ Customizable address

IP address: 192.168.1.101

Subnet mask: 255.255.255.0

Default gateway: 192.168.1.1

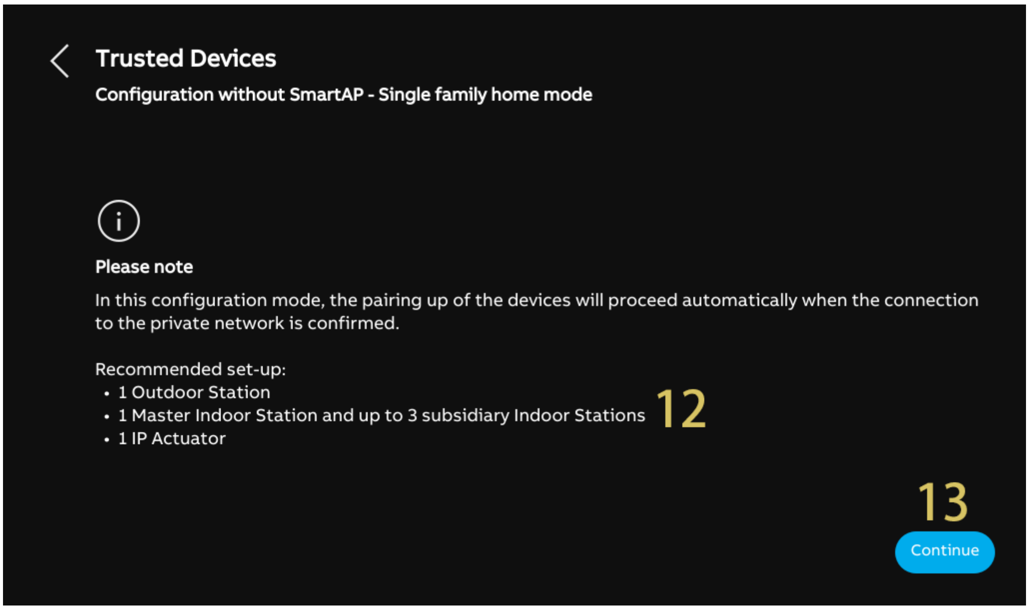
DNS: 192.168.1.1

[12]On the "Trusted Devices" screen, check the system recommended capacity again.

[13]Tap "Continue".

[14]Check the system topology.

[15]Tap "Continue" to start searching the devices in the single-family house.



Trusted Devices

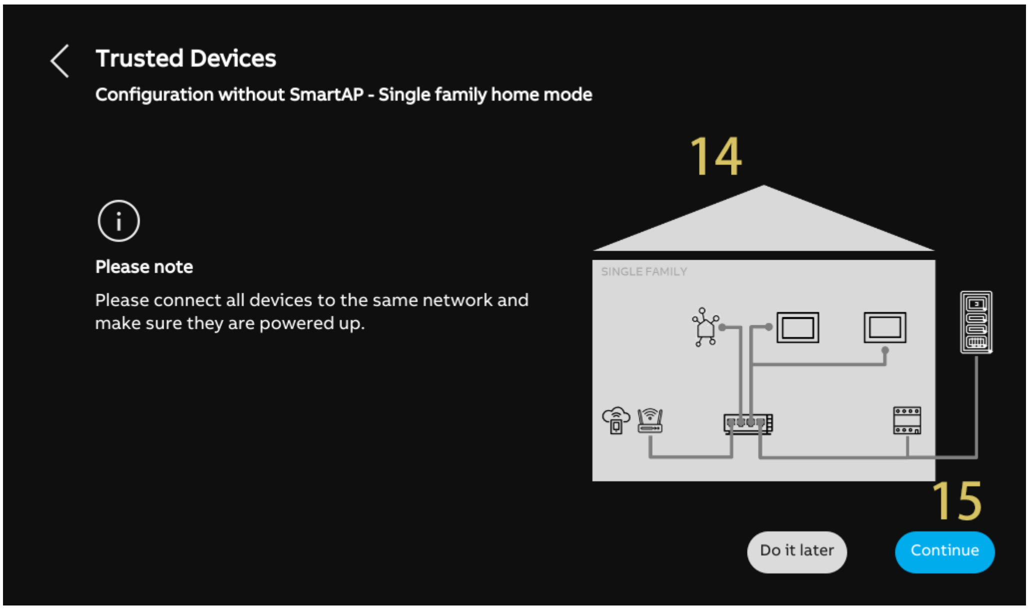
Configuration without SmartAP - Single family home mode

Please note

In this configuration mode, the pairing up of the devices will proceed automatically when the connection to the private network is confirmed.

Recommended set-up:

- 1 Outdoor Station
- 1 Master Indoor Station and up to 3 subsidiary Indoor Stations
- 1 IP Actuator



Trusted Devices

Configuration without SmartAP - Single family home mode

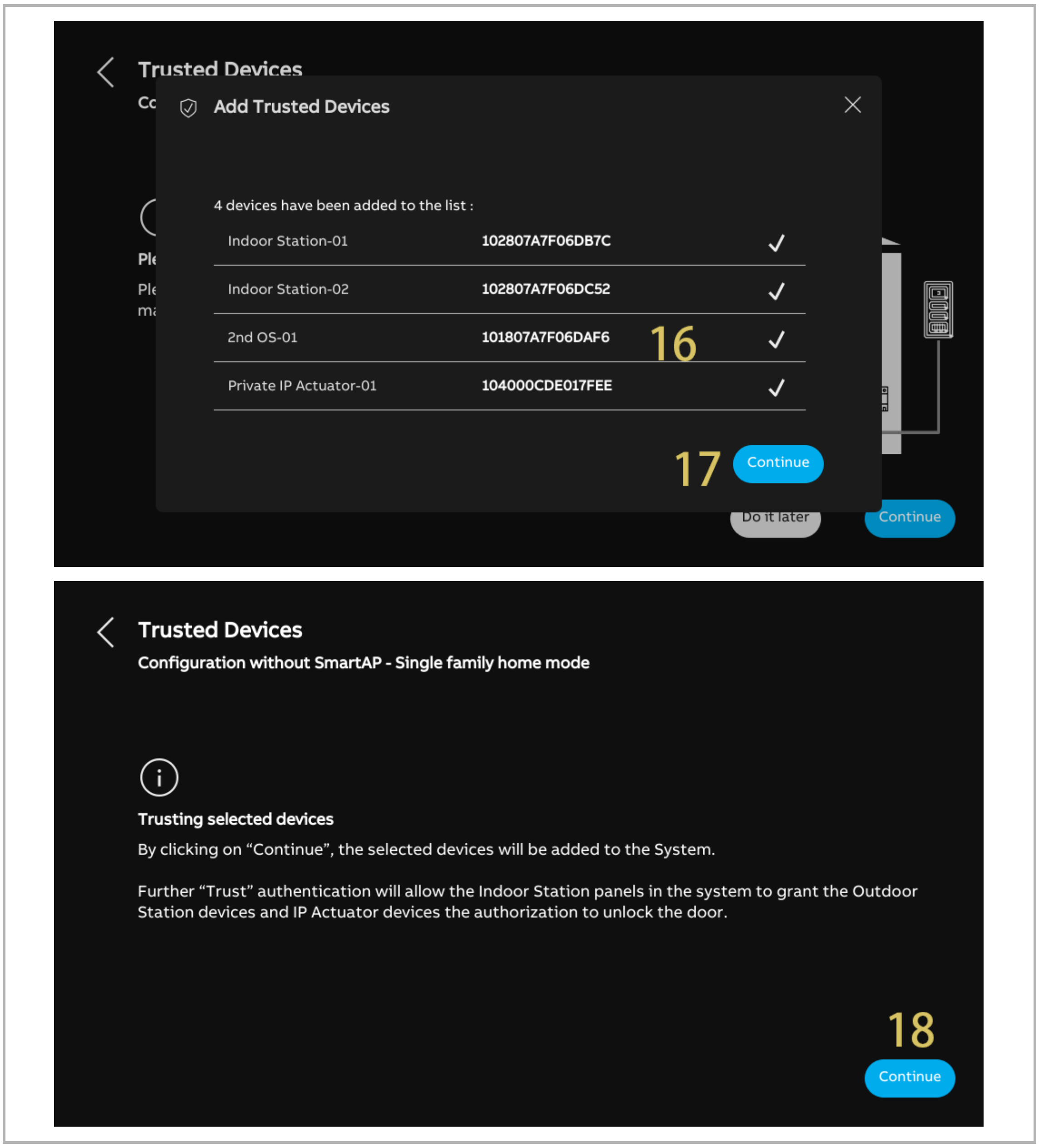
Please note

Please connect all devices to the same network and make sure they are powered up.

[16]All the related devices are displayed on the list.

[17]Tap "Continue".

[18]Tap "Continue".



4 devices have been added to the list :

Indoor Station-01	102807A7F06DB7C	✓
Indoor Station-02	102807A7F06DC52	✓
2nd OS-01	101807A7F06DAF6	✓
Private IP Actuator-01	104000CDE017FEE	✓

Trusting selected devices

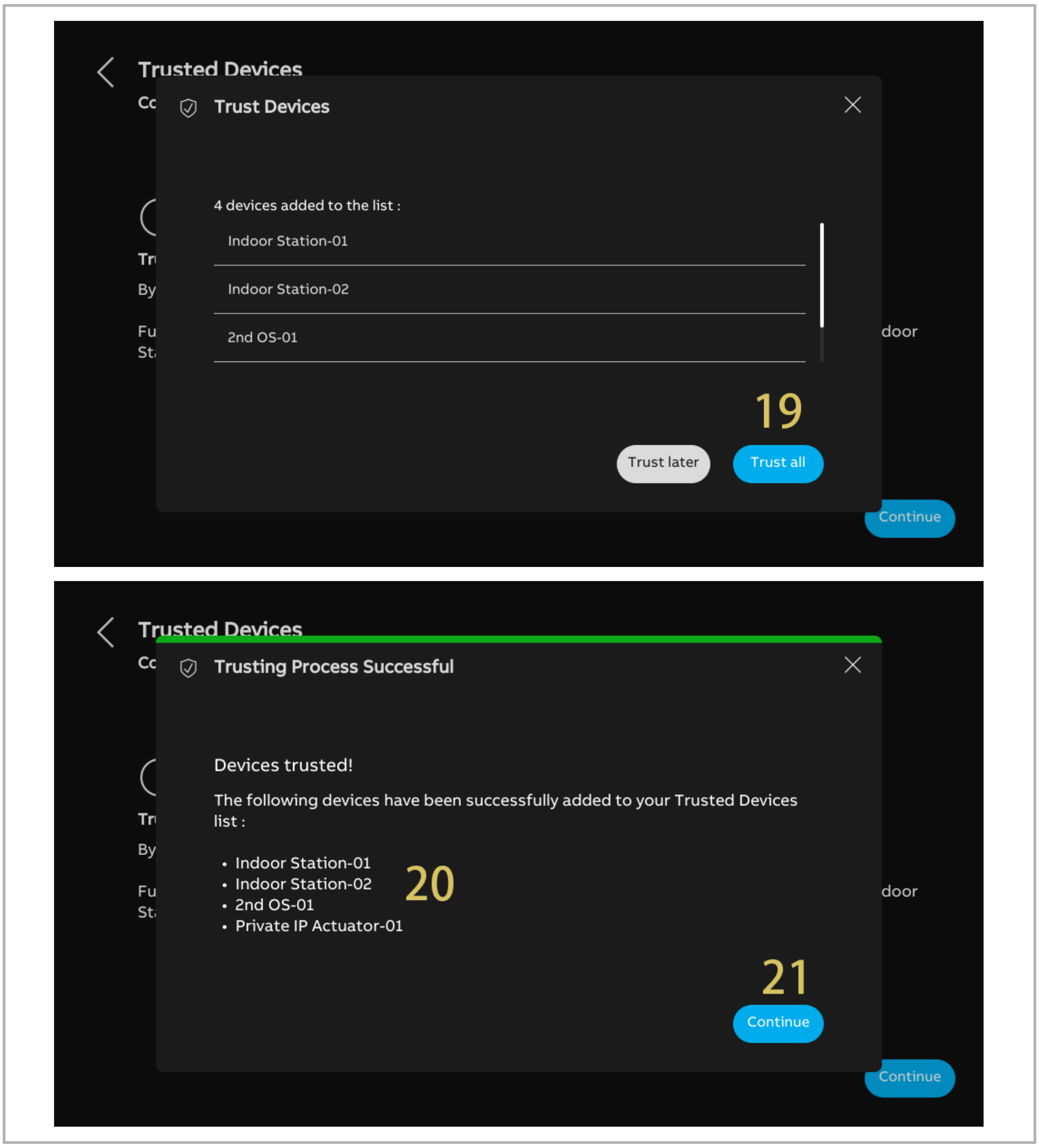
By clicking on “Continue”, the selected devices will be added to the System.

Further “Trust” authentication will allow the Indoor Station panels in the system to grant the Outdoor Station devices and IP Actuator devices the authorization to unlock the door.

[19]Tap "Trust all".

[20]All the related devices will be displayed on the screen.

[21]Tap "Continue".



4 devices added to the list :

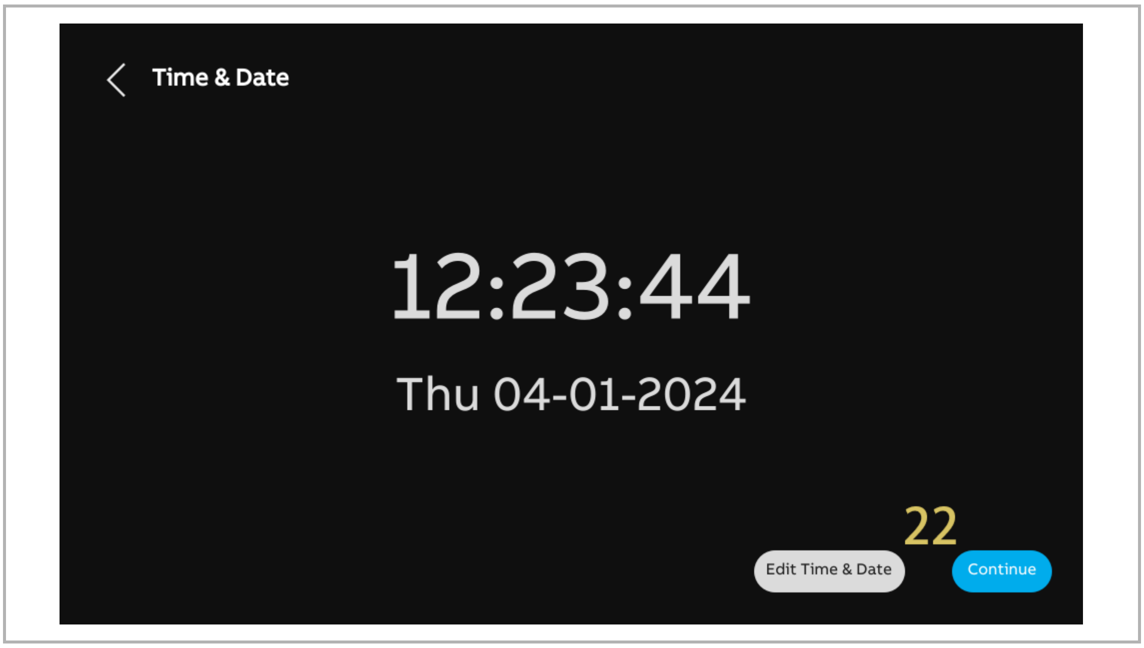
- Indoor Station-01
- Indoor Station-02
- 2nd OS-01

Devices trusted!

The following devices have been successfully added to your Trusted Devices list :

- Indoor Station-01
- Indoor Station-02
- 2nd OS-01
- Private IP Actuator-01

[22]On the "Time & date" screen, you can carry out this setting at this time or tap "Continue" to skip this setting for the moment.



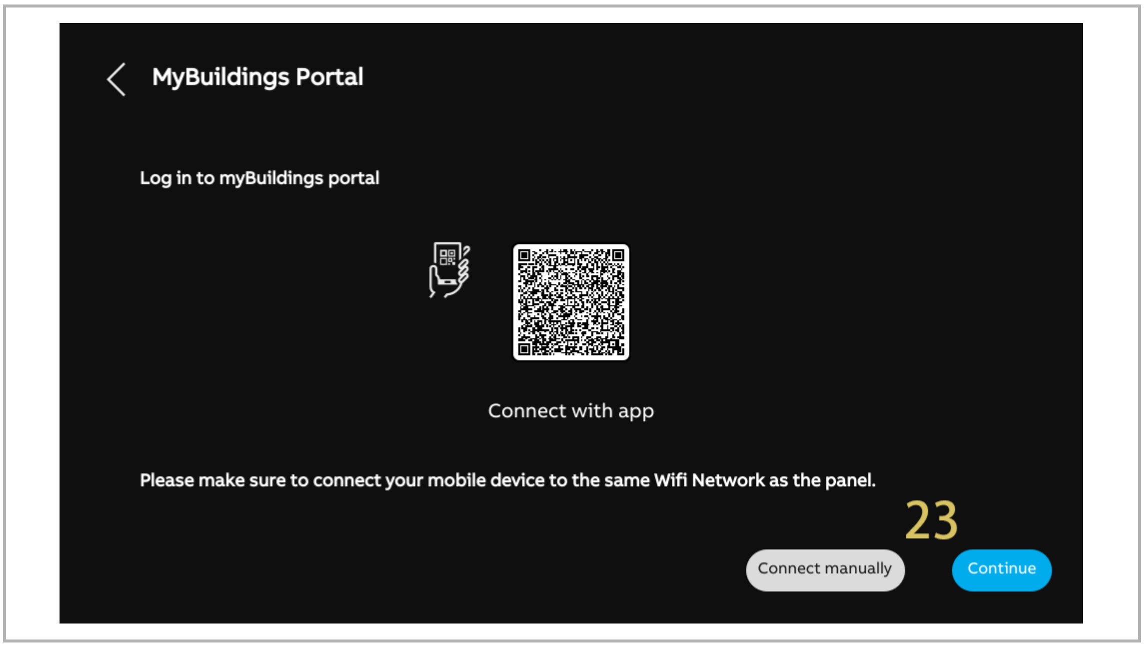
Time & Date

12:23:44

Thu 04-01-2024

[23]On the "MyBuildings portal" screen, you can carry out this setting at this time or tap "Continue" to skip this setting initially if the App is not ready.

- For more details, see the product manual of the designated Indoor Station.



MyBuildings Portal

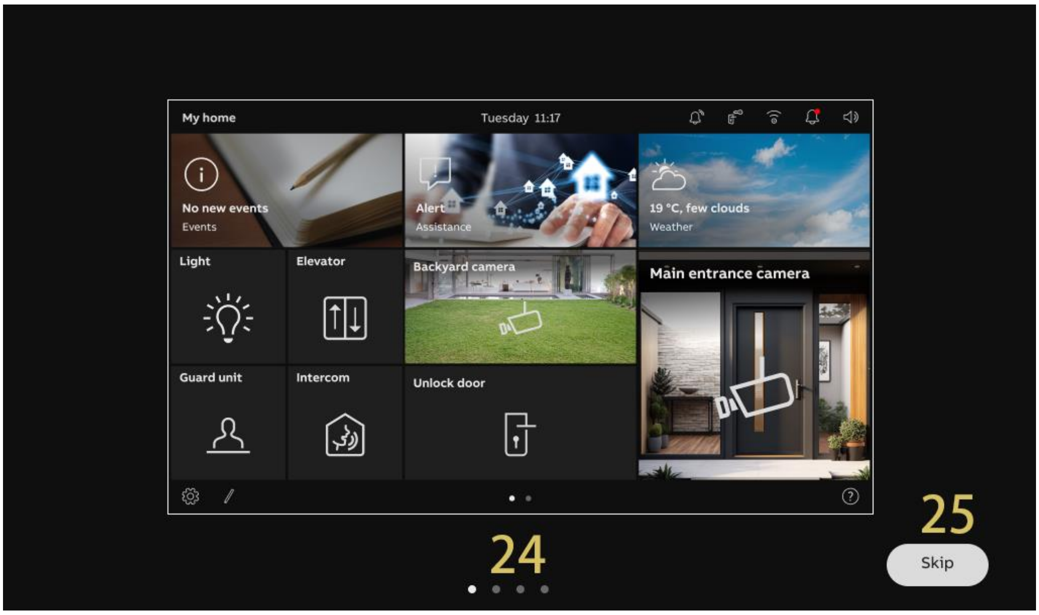
Log in to myBuildings portal

Connect with app

Please make sure to connect your mobile device to the same Wifi Network as the panel.

[24]There are 4 screens to guide you how to use the panel.

[25]Tap "Skip" if you are already familiar with the panel.



Note

After configuring the Master IS, the 2nd OS and the IPA have both finished their configuration. However, the Subsidiary IS still needs some steps to complete its configuration. see chapter 4.2.5 “Configuring the Subsidiary IS“ on page 163.

The outdoor station will be automatically set as a 2nd OS, and the IPA will be automatically set as a private IPA.

At the same time, the IPA will be automatically set as the default lock of the outdoor station.

4.2.5 Configuring the Subsidiary IS

Please ensure the Master IS has completed the Wizard Setup before continuing the configuration of the Subsidiary IS:

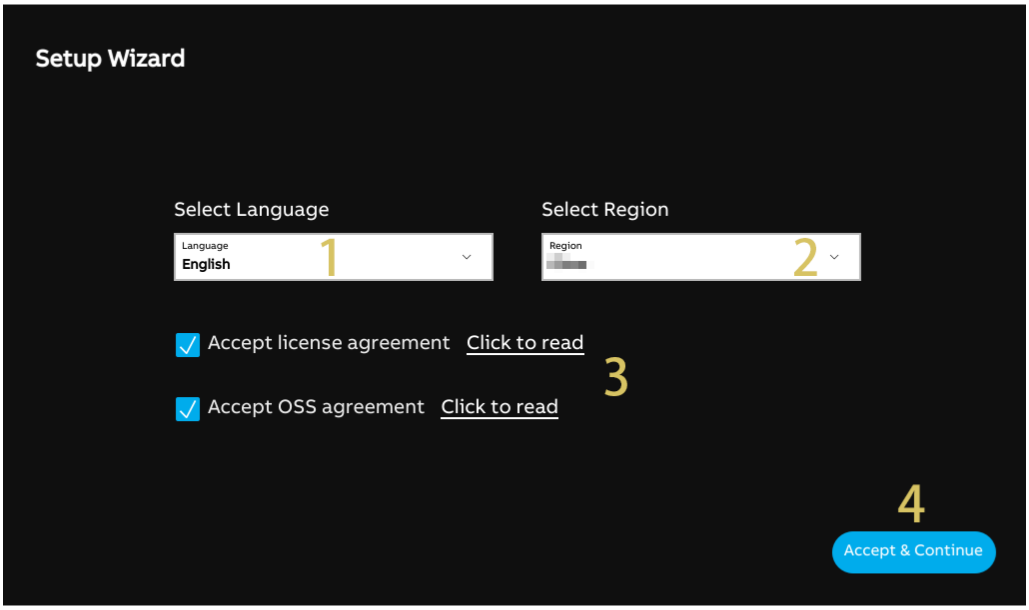
Please follow the steps below to continue the configuration of the Subsidiary IS:

[1] On the "Setup wizard" screen, select the language from the drop-down list.

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

[3] Tick the check box to accept the licences. Or tap "Click to read" to view the details of the licence.

[4] Tap "Accept & continue" to access the next screen.



Setup Wizard

Select Language

Language: English

Select Region

Region: [redacted]

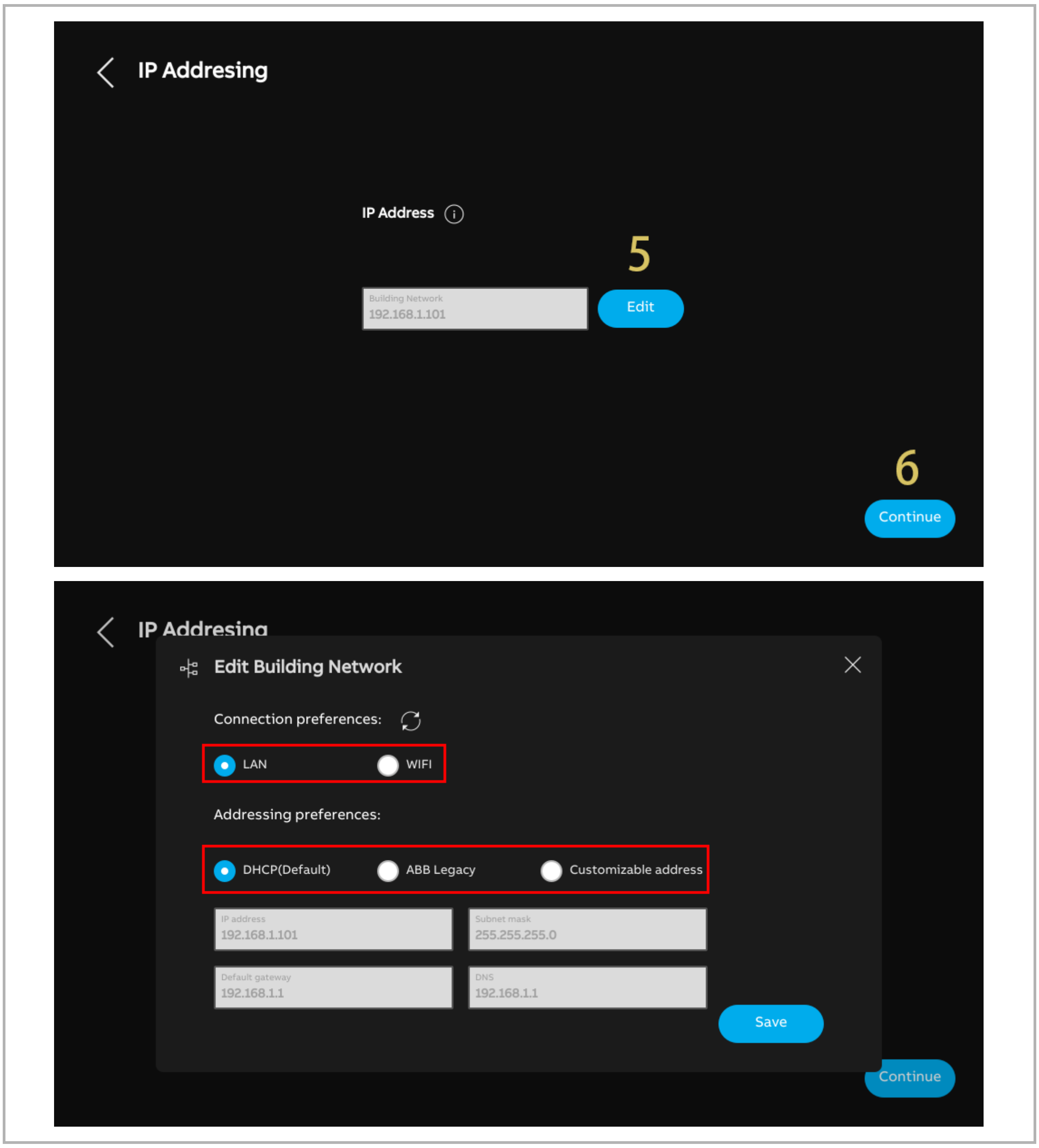
☑ Accept license agreement Click to read

☑ Accept OSS agreement Click to read

[5] On the "IP Addressing" screen, tap "Edit" to access the corresponding screen.

- Select the connection type, it can be set to "LAN" or "WiFi".
- Select the address type, it can set to "DHCP", "Customizable address" or "ABB Legacy". If "ABB Legacy" is selected, IP address will be "10.0.x.x".
- The address type of the Subsidiary IS should be the same as that of the Master IS.
- Please tap "Save" if the settings have been changed.

[6] Tap "Continue".



IP Address

Building Network: 192.168.1.101

Connection preferences: ● LAN ○ WIFI

Addressing preferences: ● DHCP(Default) ○ ABB Legacy ○ Customizable address

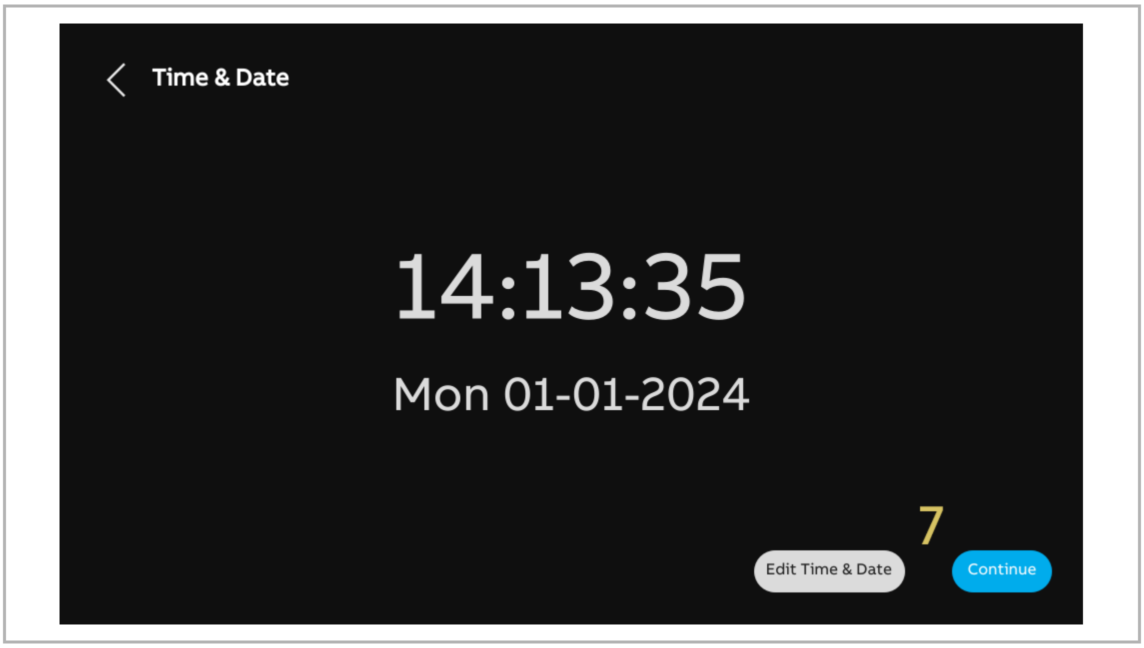
IP address: 192.168.1.101

Subnet mask: 255.255.255.0

Default gateway: 192.168.1.1

DNS: 192.168.1.1

[7] On the "Time & date" screen, you can carry out this setting at this time or tap "Continue" to skip this setting for the moment.



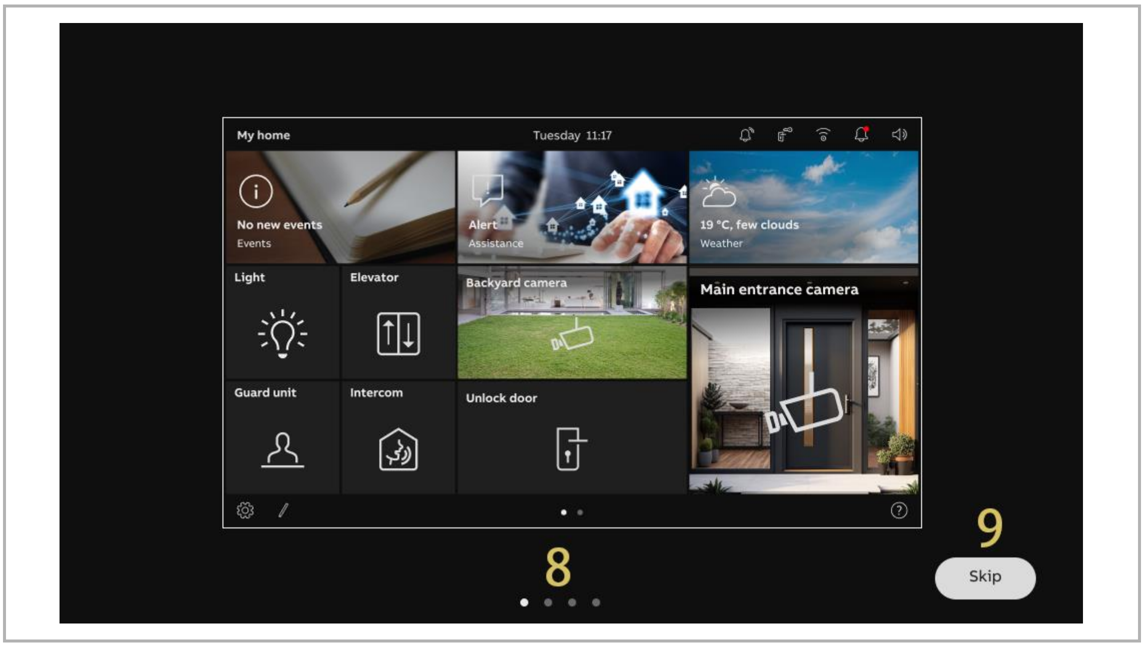
Time & Date

14:13:35

Mon 01-01-2024

[8] There are 4 screens to guide you how to use the panel.

[9] Tap "Skip" if you are already familiar with the panel.



4.2.6 Adding new trusted devices via auto search

IPA and 2nd OS with IC can only release the lock when they have been added to the trusted devices list.

If the designated device has not been added to the trusted device list during the "Setup Wizard", you can add them afterwards via auto search.

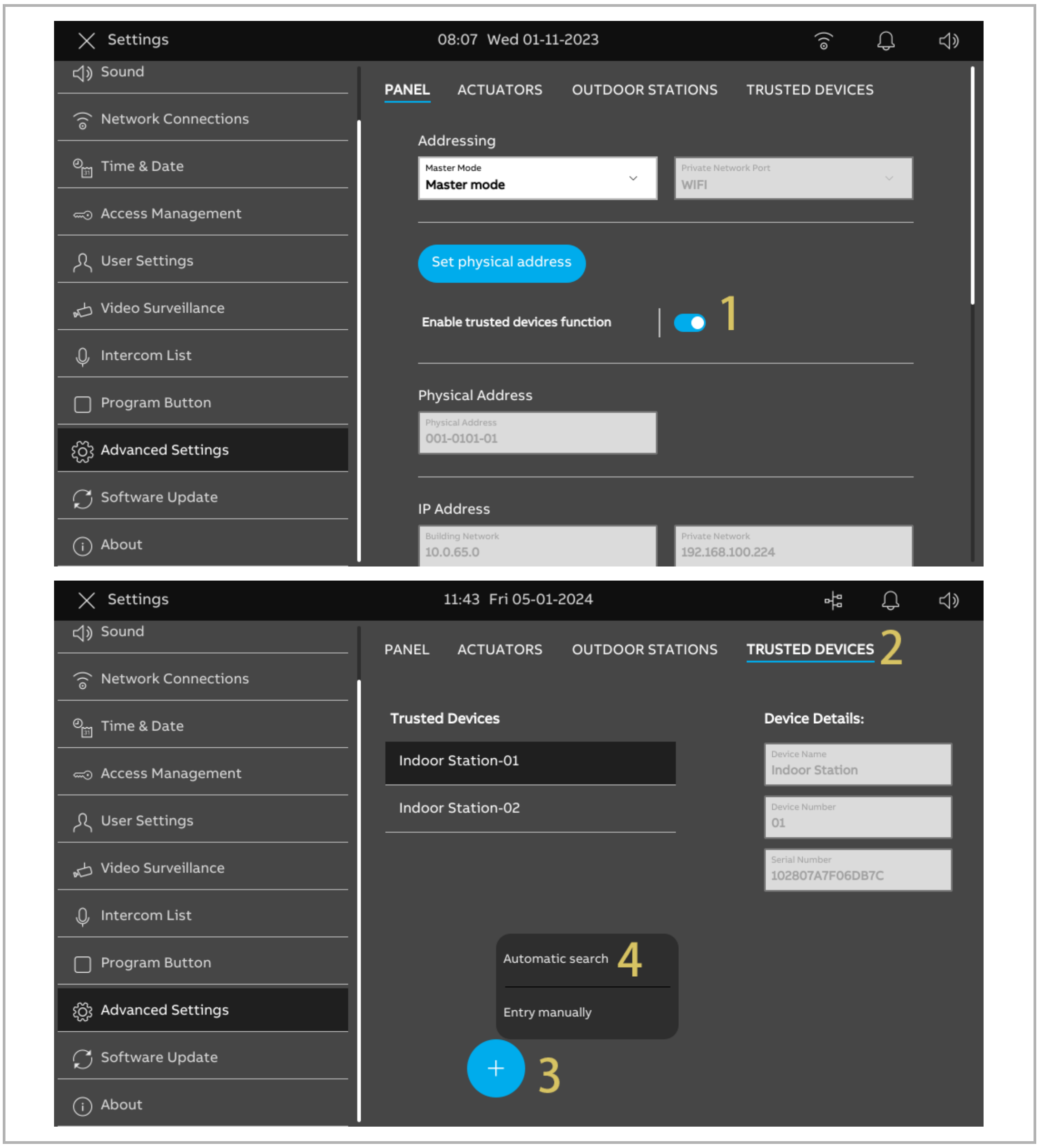
Please follow the steps below:

[1] On the "Advanced Settings" screen, ensure "Enable trusted devices function" is enabled.

[2] On the "Advanced Settings" screen, tap "Trusted Devices" to access the corresponding screen.

[3] Tap " + ".

[4] Tap "Automatic search".



Addressing

Master Mode: Master mode

Private Network Port: WIFI

Enable trusted devices function: ON

Physical Address

Physical Address: 001-0101-01

IP Address

Building Network: 10.0.65.0

Private Network: 192.168.100.224

Trusted Devices

Indoor Station-01

Indoor Station-02

Device Details:

Device Name: Indoor Station

Device Number: 01

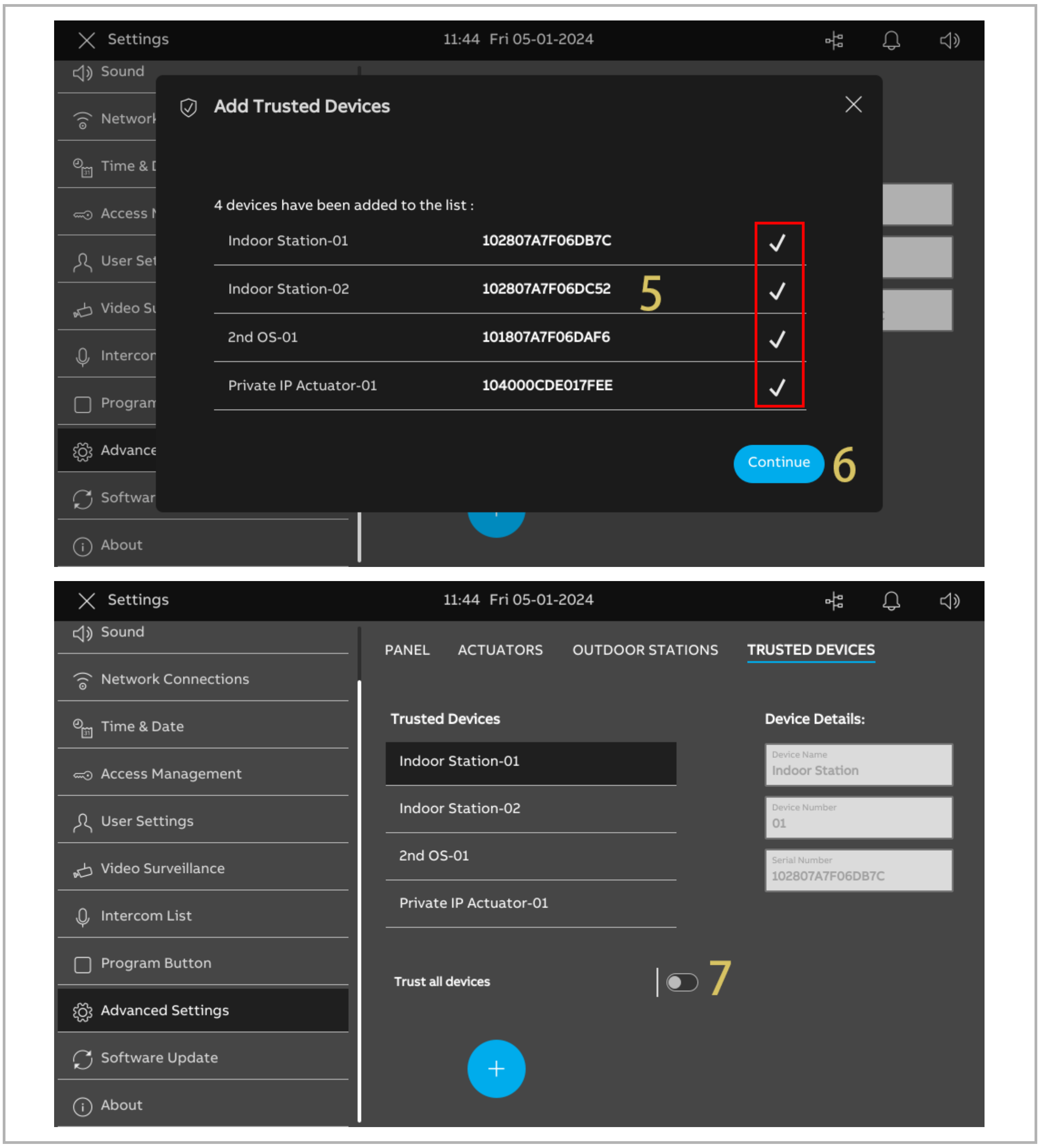
Serial Number: 102807A7F06DB7C

[5] The devices on the same home network will be displayed on the list.

- " √ " means the device has been configured successfully. Otherwise please restore the designated device to the default factory settings.

[6] Tap "Continue".

[7] Enable the "Trust all devices".



Add Trusted Devices

4 devices have been added to the list :

Indoor Station-01	102807A7F06DB7C	✓
Indoor Station-02	102807A7F06DC52	✓
2nd OS-01	101807A7F06DAF6	✓
Private IP Actuator-01	104000CDE017FEE	✓

Trusted Devices

- Indoor Station-01
- Indoor Station-02
- 2nd OS-01
- Private IP Actuator-01

Device Details:

Device Name: Indoor Station

Device Number: 01

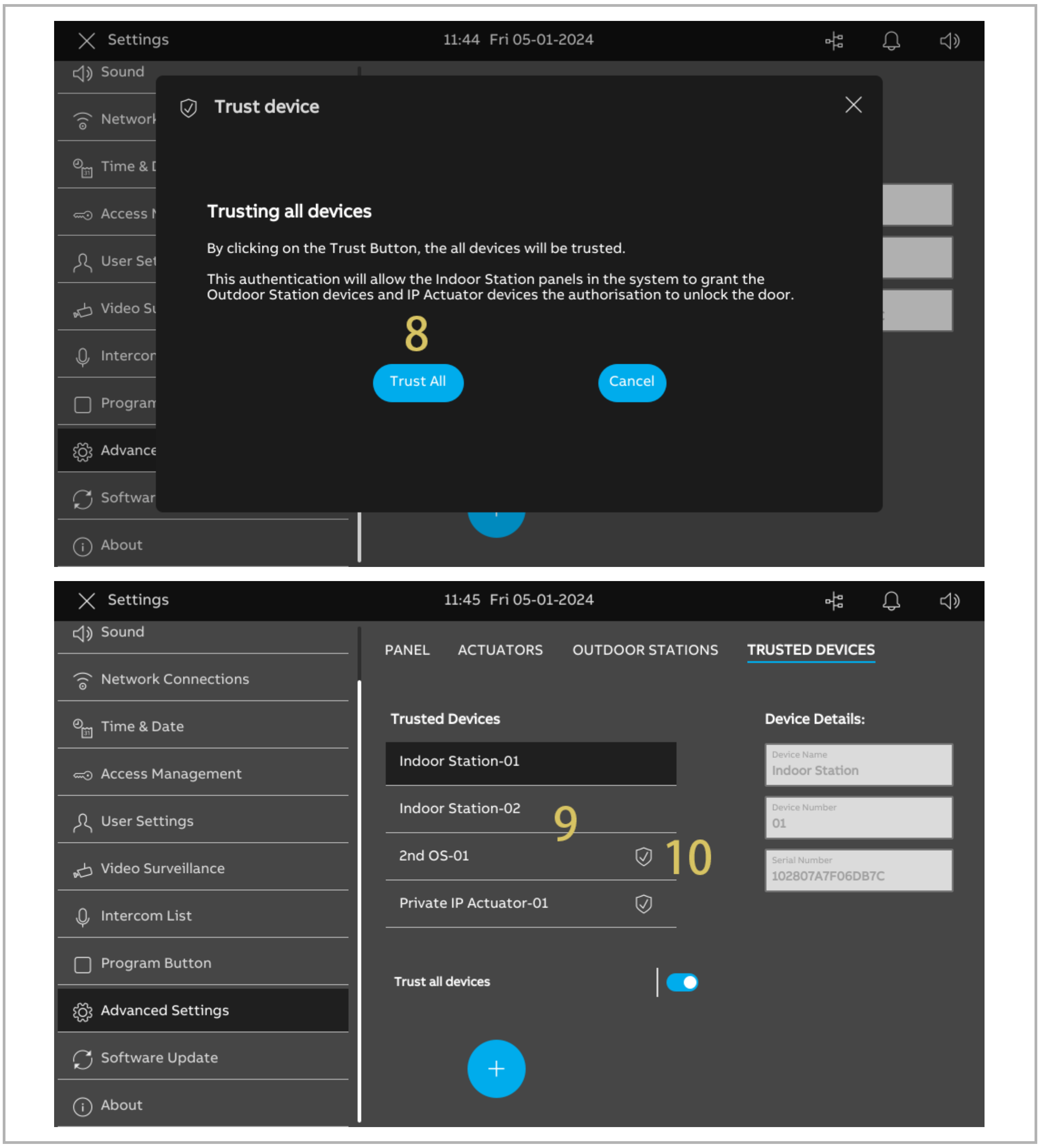
Serial Number: 102807A7F06DB7C

Trust all devices ○

[8] Tap "Trust All".

[9] All trusted devices will be displayed on the screen.

[10] 🛡 will be displayed on the right to indicate the 2nd OS with IC or IP Actuator can use the unlock function.



Trust device

Trusting all devices

By clicking on the Trust Button, the all devices will be trusted.

This authentication will allow the Indoor Station panels in the system to grant the Outdoor Station devices and IP Actuator devices the authorisation to unlock the door.

Trust All

Cancel

Trusted Devices

- Indoor Station-01
- Indoor Station-02
- 2nd OS-01 🛡
- Private IP Actuator-01 🛡

Trust all devices ●

Device Details:

Device Name: Indoor Station

Device Number: 01

Serial Number: 102807A7F06DB7C

4.2.7 Adding new trusted devices manually

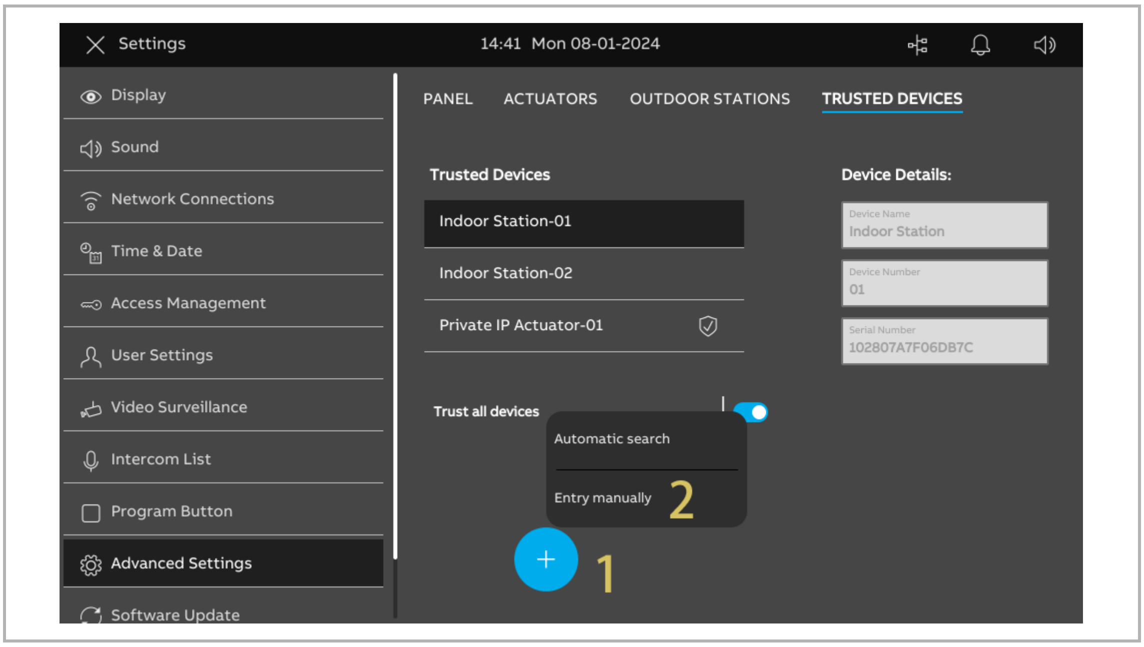
IPA and 2nd OS with IC can release the lock only when they have been added to the trusted devices list.

If the designated device has not been added to the trusted device list during the "Setup Wizard", you can add them manually.

Please follow the steps below:

[1] On the "Trusted Devices" screen, tap " + ".

[2] Select "Entry manually".



Device Name
Indoor Station

Device Number
01

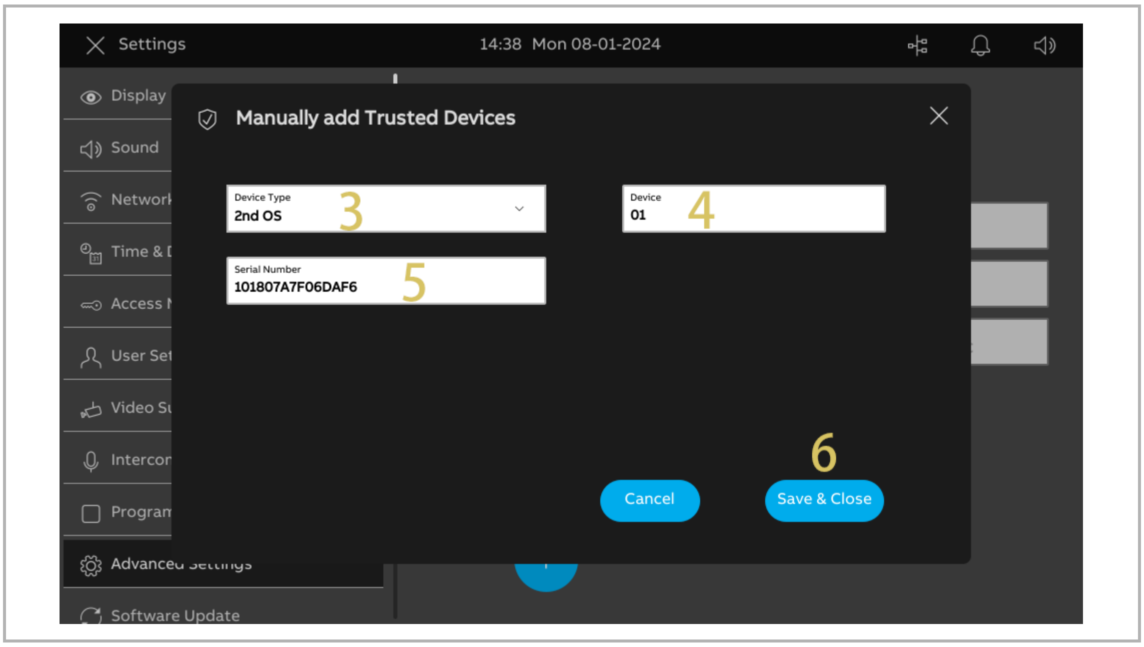
Serial Number
102807A7F06DB7C

[3] Select the device type from the drop-down list. It can be set to "2nd OS", "Private IP actuator" or "Indoor station".

[4] Enter the device number.

[5] Enter the serial number.

[6] Tap "Save & Close".



Manually add Trusted Devices

Device Type: 2nd OS

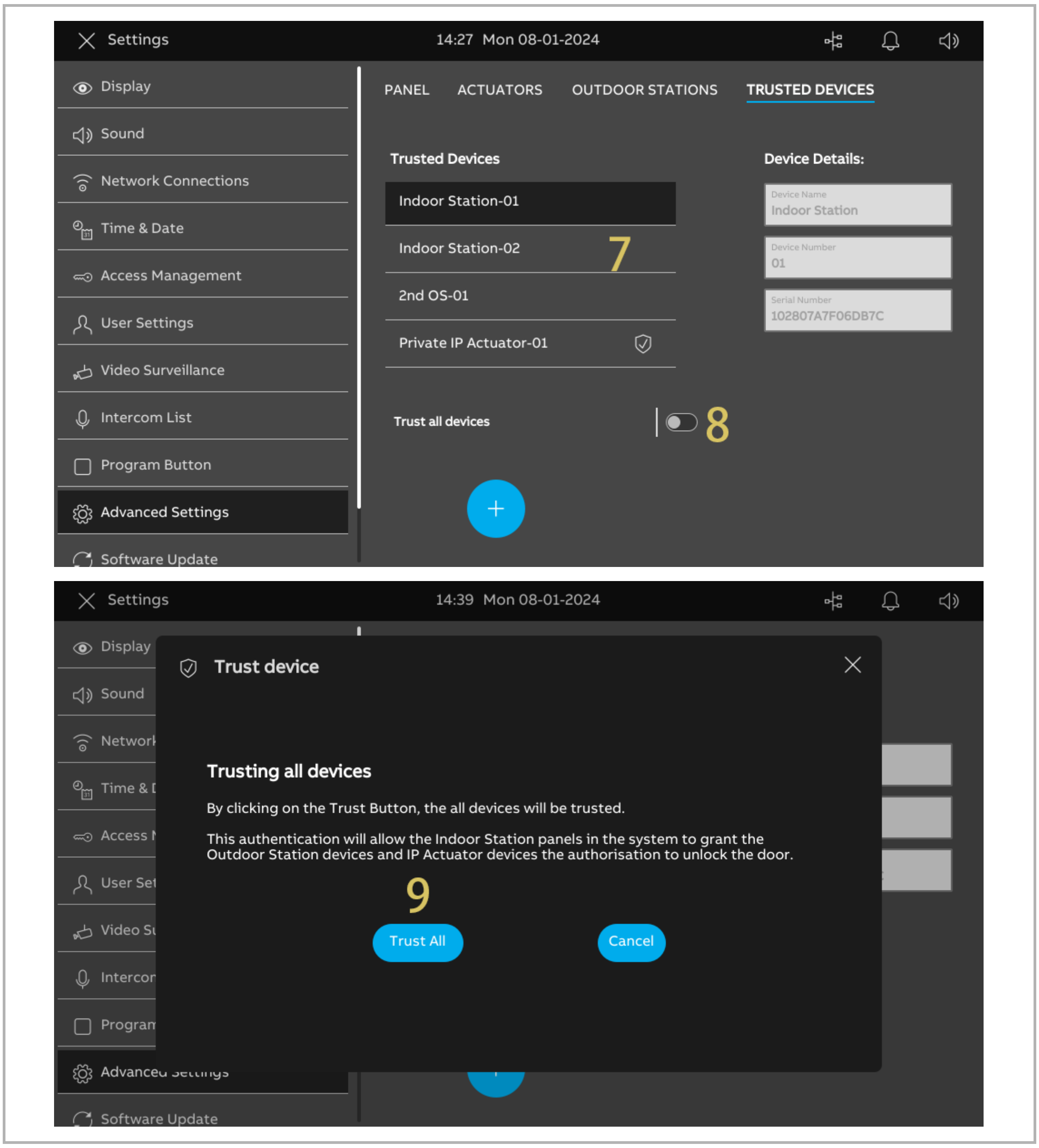
Device: 01

Serial Number: 101807A7F06DAF6

[7] The designated device has been added to the list.

[8] Tap "Trust all devices".

[9] Tap "Trust All".



Device Name: Indoor Station

Device Number: 01

Serial Number: 102807A7F06DB7C

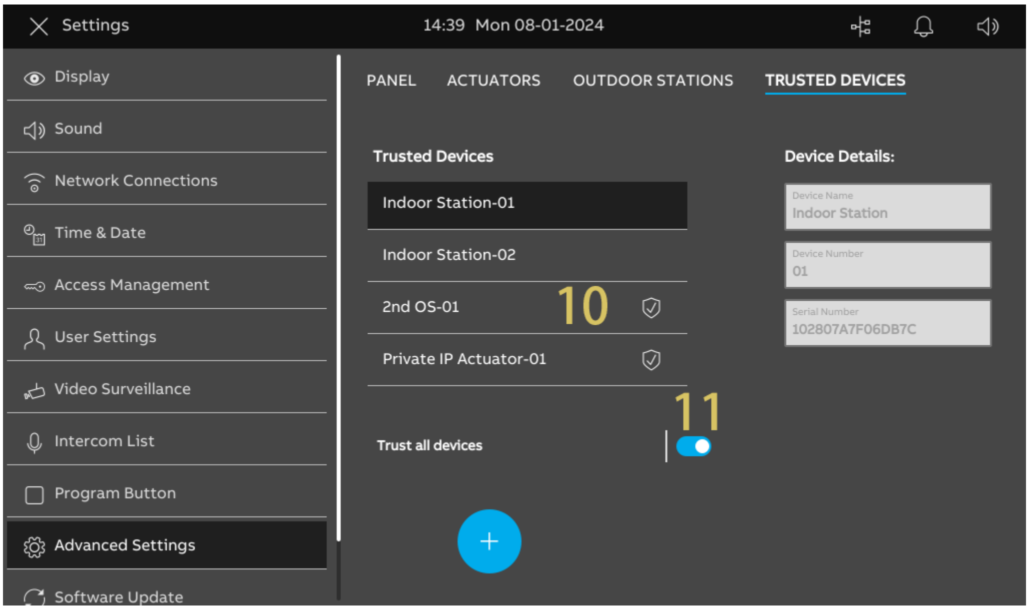
Trusting all devices

By clicking on the Trust Button, the all devices will be trusted.

This authentication will allow the Indoor Station panels in the system to grant the Outdoor Station devices and IP Actuator devices the authorisation to unlock the door.

[10]The designated device is now a trusted device, and 🛡 will be displayed on the right to indicate the 2nd Outdoor Station or the IP Actuator can use the unlock function.

[11]"Trust all devices" will be enabled if all devices have been set to trusted.



Device Name: Indoor Station

Device Number: 01

Serial Number: 102807A7F06DB7C

Trust all devices: on

4.2.8 Removing the trusted device

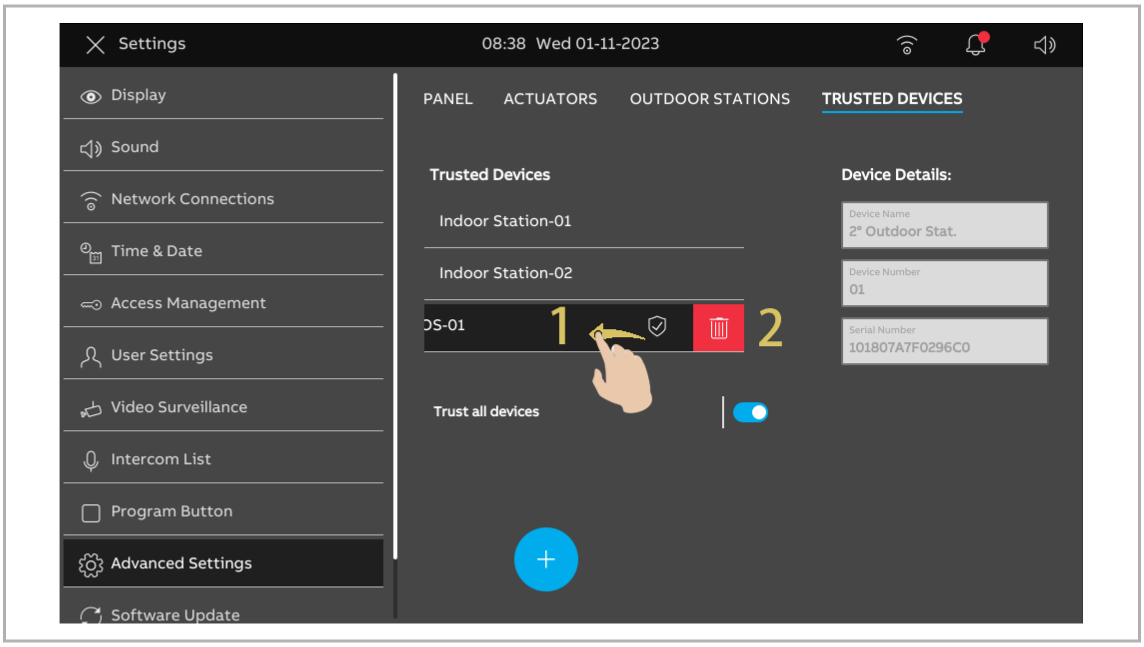
Please follow the steps below:

[1] On the "Trusted Devices" screen, swipe the relevant device to the left.

[2] Tap " 🗑 " to remove the device.

Note

If the device is removed from the trusted devices list, it cannot use the unlock function any more.



Trusted Devices

Indoor Station-01

Indoor Station-02

OS-01

Trust all devices

Device Details:

Device Name: 2º Outdoor Stat.

Device Number: 01

Serial Number: 101807A7F0296C0

5 Grouping and Forwarding

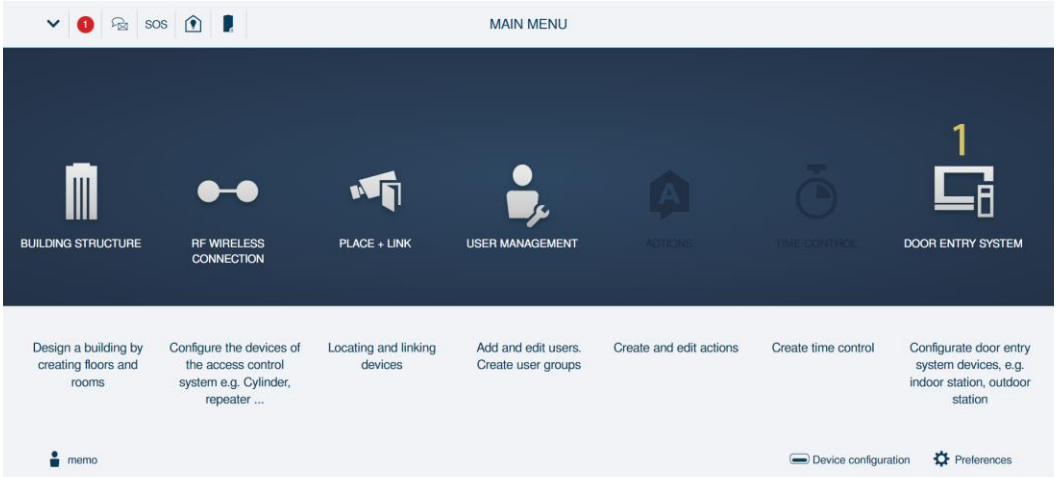
5.1 Grouping Management Function

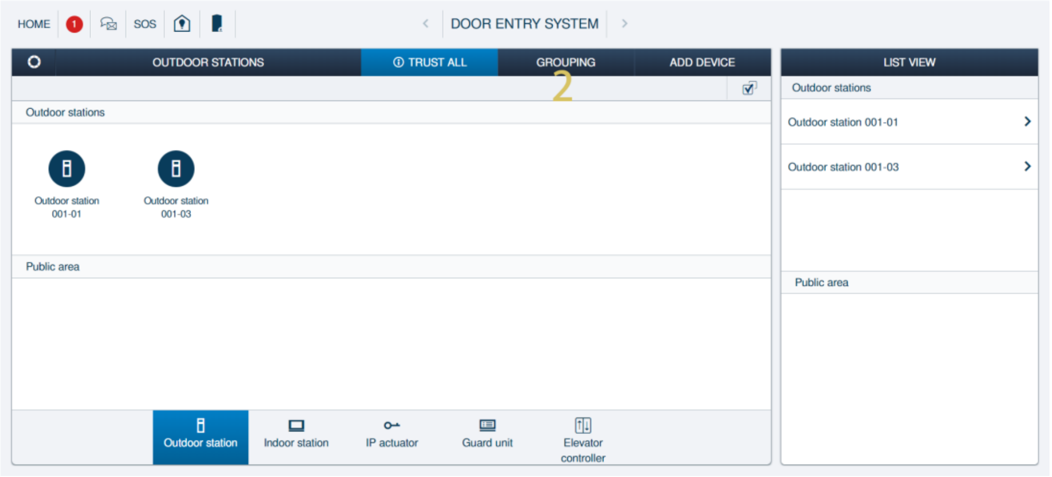
The Grouping call feature allows the multiple calls of different Indoor Stations, independently of their mode, apartment location and type, as long as they all belong to the same Building System.

Please follow the steps below:

[1] On the "Main Menu" screen of SmartAP, click "Door Entry System".

[2] Click "Grouping".


SOS
MAIN MENU
1
BUILDING STRUCTURE
RF WIRELESS CONNECTION
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
memo
Device configuration
Preferences

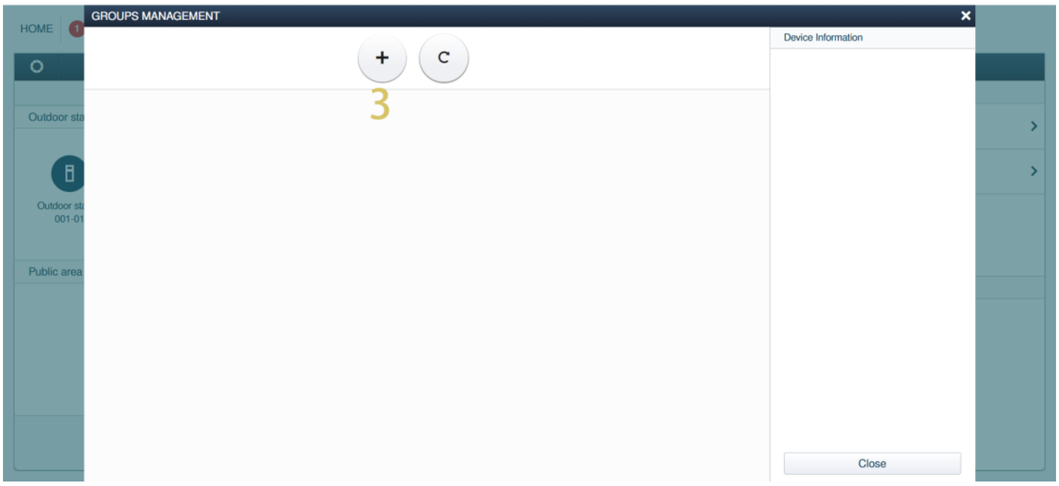


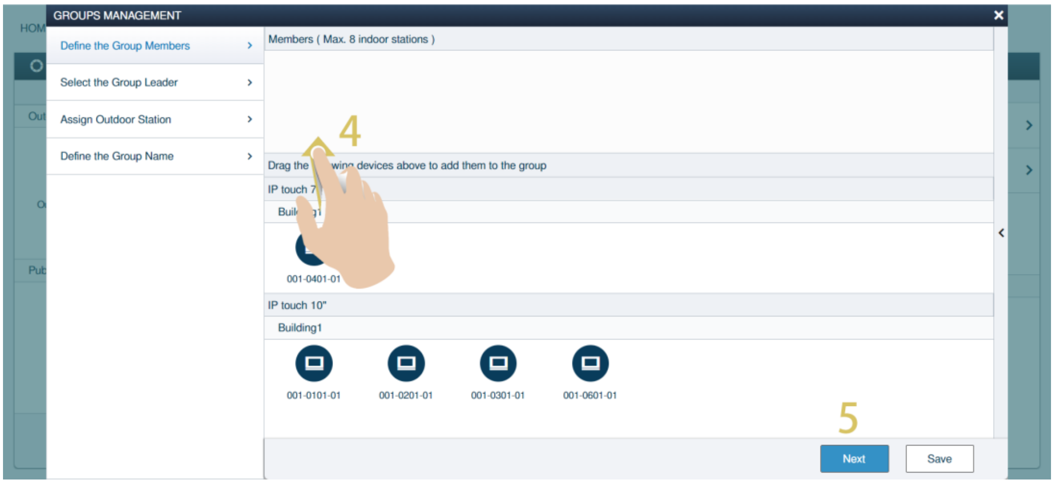
[3] Click " + " to add a new group.

[4] Drag the designated Indoor Stations to the "Members" section.

- Maximum 8 Indoor Stations can be supported.

[5] Click "Next".





[6] Select an Indoor Staton as a leader.

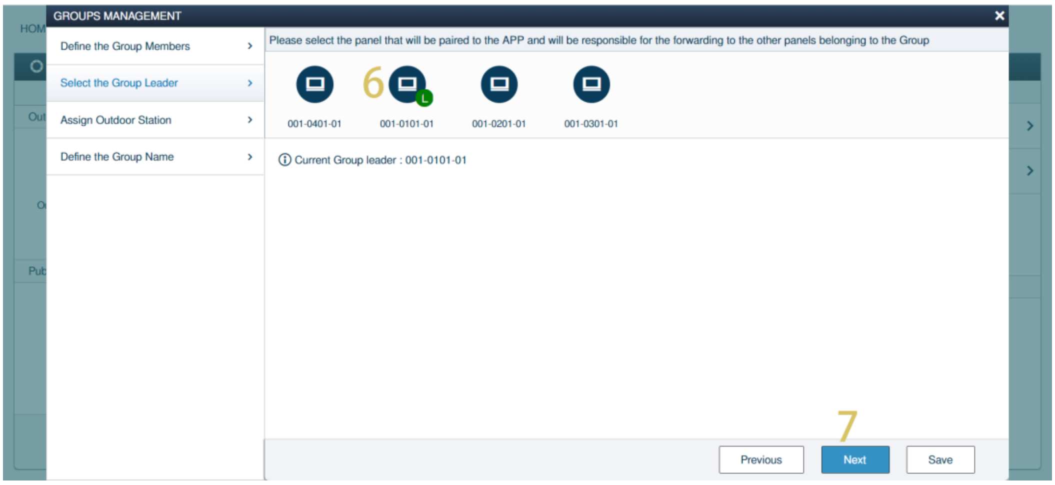
[7] Click "Next".

[8] Drag the designated Outdoor Stations to the "Outdoor Stations" section.

- If no pushububtton Outdoor Station is selected, please continue step 13.
- If a pushububtton Outdoor Station is selected, please continue step 9.

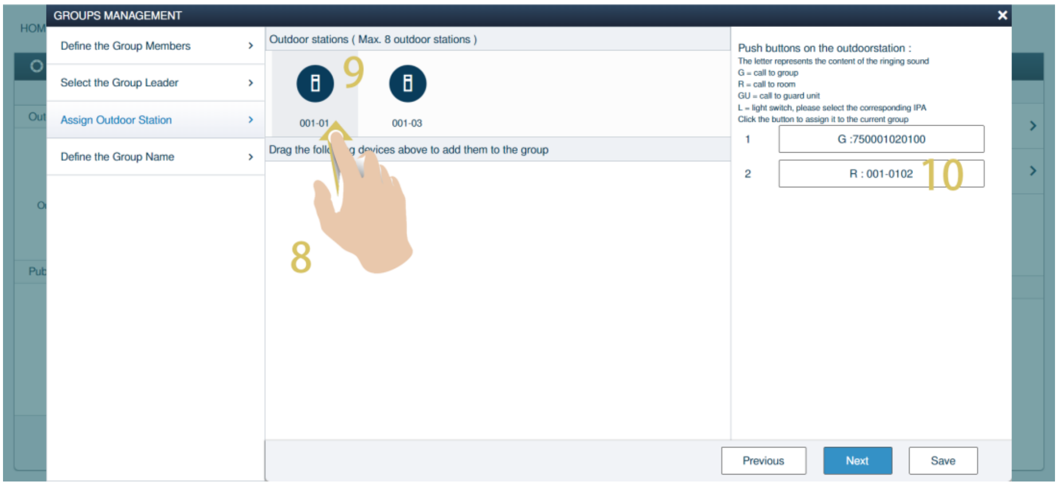
[9] Tap a Pushbutton Outdoor Station.

[10]Tap the designated pusubutton.



Please select the panel that will be paired to the APP and will be responsible for the forwarding to the other panels belonging to the Group

ⓘ Current Group leader : 001-0101-01



Drag the following devices above to add them to the group

Push buttons on the outdoorstation :
The letter represents the content of the ringing sound
G = call to group
R = call to room
GU = call to guard unit
L = light switch, please select the corresponding IPA
Click the button to assign it to the current group

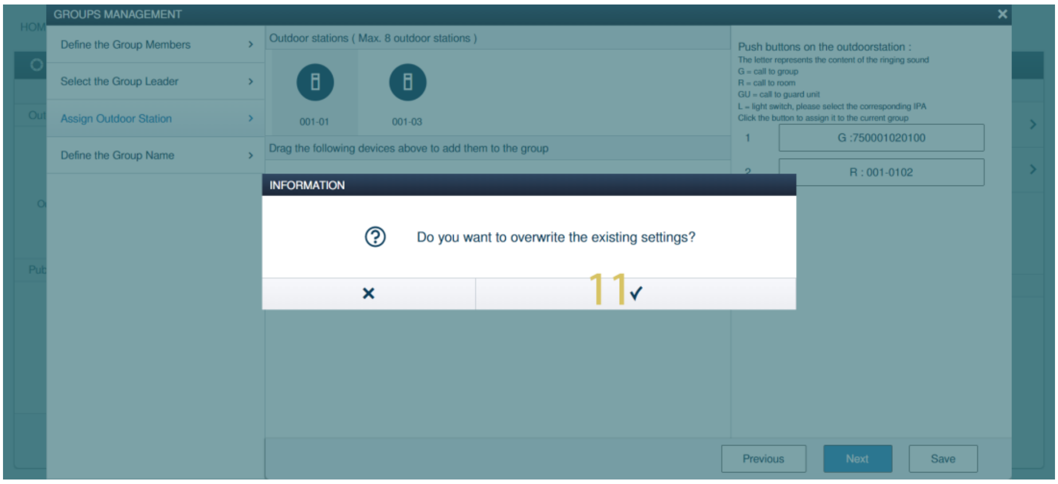
1 G :750001020100

2 R : 001-0102

[11]Click " √ " to overwirte the existing setting of the pushbutton.

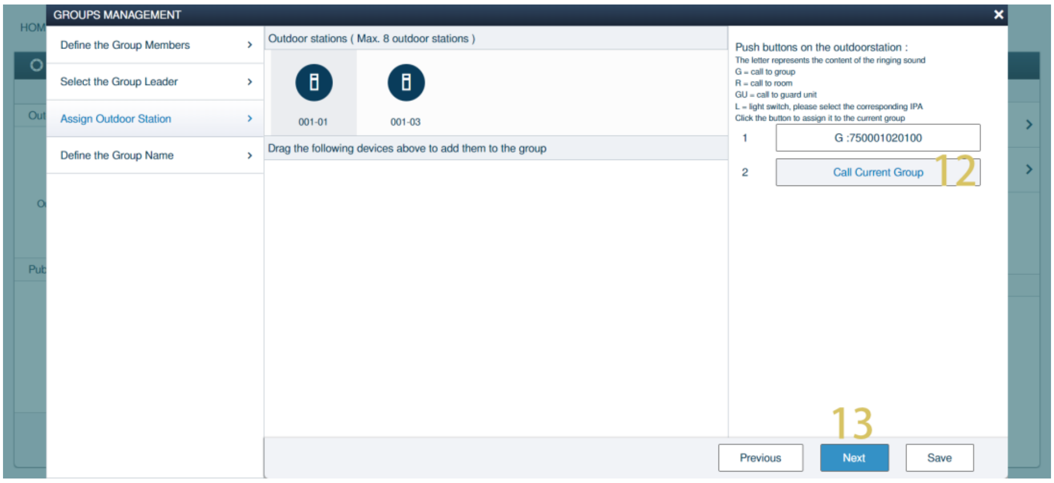
[12]"Call Current Group" will be displayed to indicate the grouping call is activated.

[13]Click "Next".



Push buttons on the outdoorstation :
The letter represents the content of the ringing sound
G = call to group
R = call to room
GU = call to guard unit
L = light switch, please select the corresponding IPA
Click the button to assign it to the current group

Do you want to overwrite the existing settings?

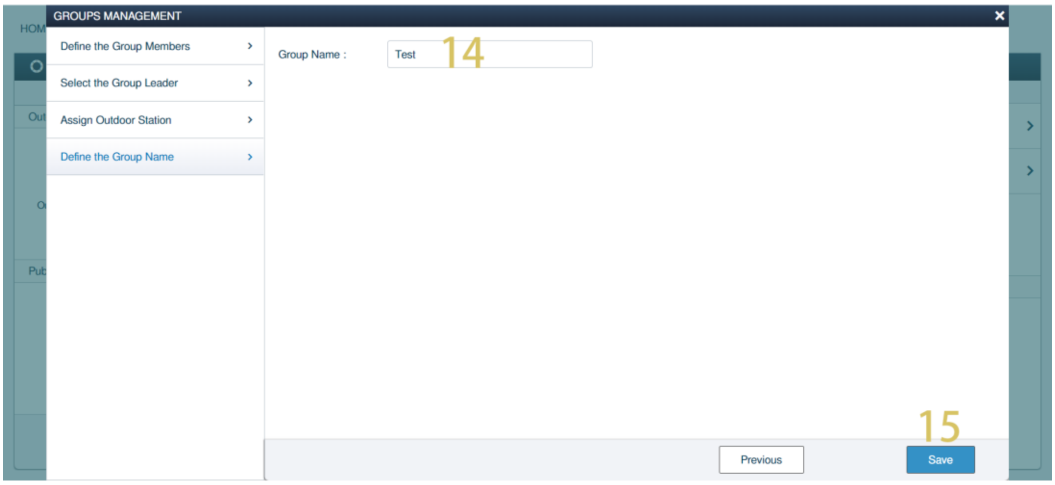


Push buttons on the outdoorstation :
The letter represents the content of the ringing sound
G = call to group
R = call to room
GU = call to guard unit
L = light switch, please select the corresponding IPA
Click the button to assign it to the current group

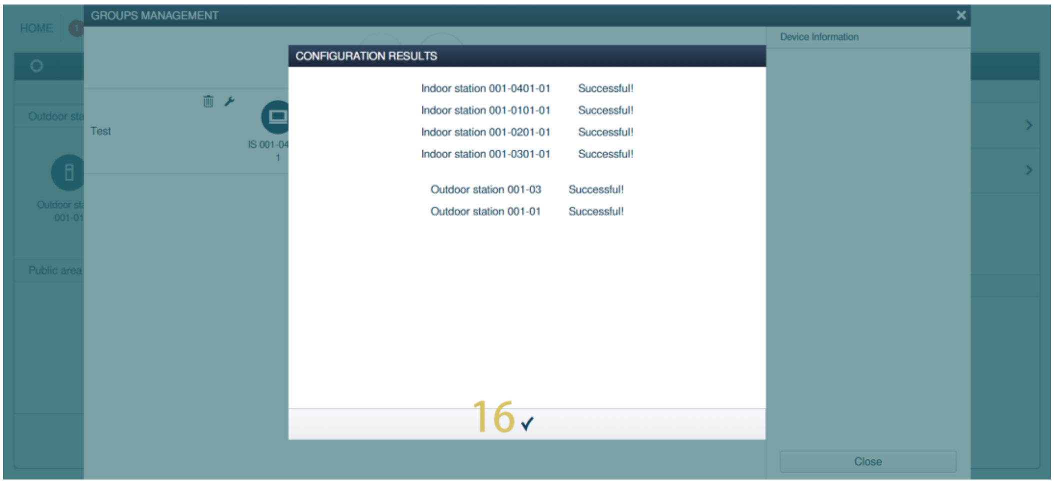
[14]Enter the group name.

[15]Click "Save".

[16]All the deivces in the group will be displayed on the screen. Click " √ ".



Group Name : Test



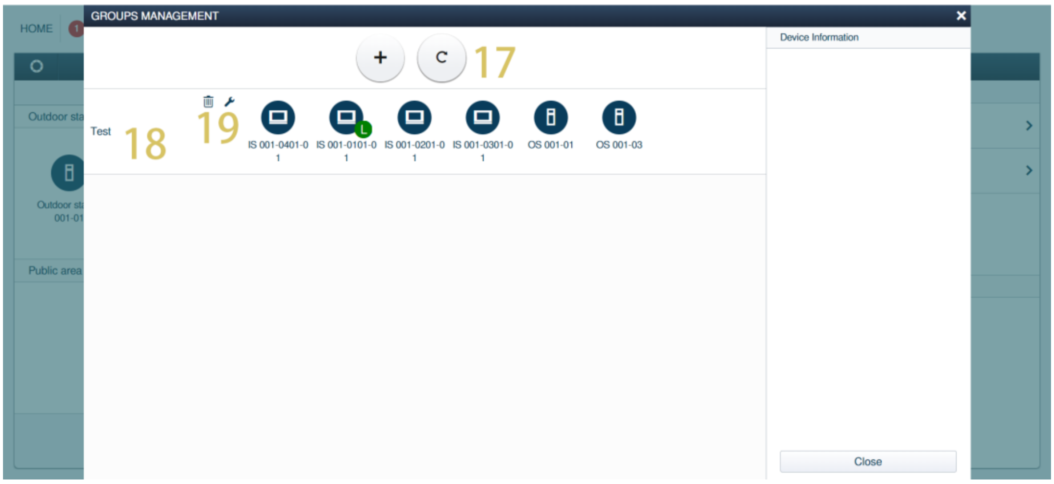
Indoor station 001-0401-01	Successful!
Indoor station 001-0101-01	Successful!
Indoor station 001-0201-01	Successful!
Indoor station 001-0301-01	Successful!
Outdoor station 001-03	Successful!
Outdoor station 001-01	Successful!

[17]Click " c " to refresh the screen.

[18]The group is displayed on the screen.

[19]Manage the group.

- Click " 🔧 " to edit the group.
- Click " 🗑 " to remove the group.



5.2 Forwarding Call Feature

5.2.1 Forwarding Call for Indoor Stations

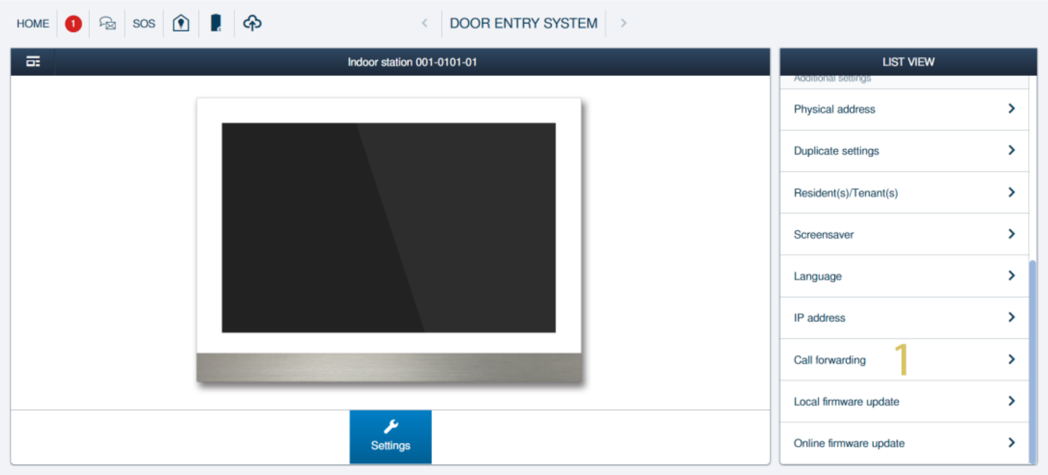
The Forwarding call feature allows the call destinated to one Indoor Station to be redirected to a determined alternative Indoor Station, directly, in specific time slots, or in case of missing answer within a selected time.

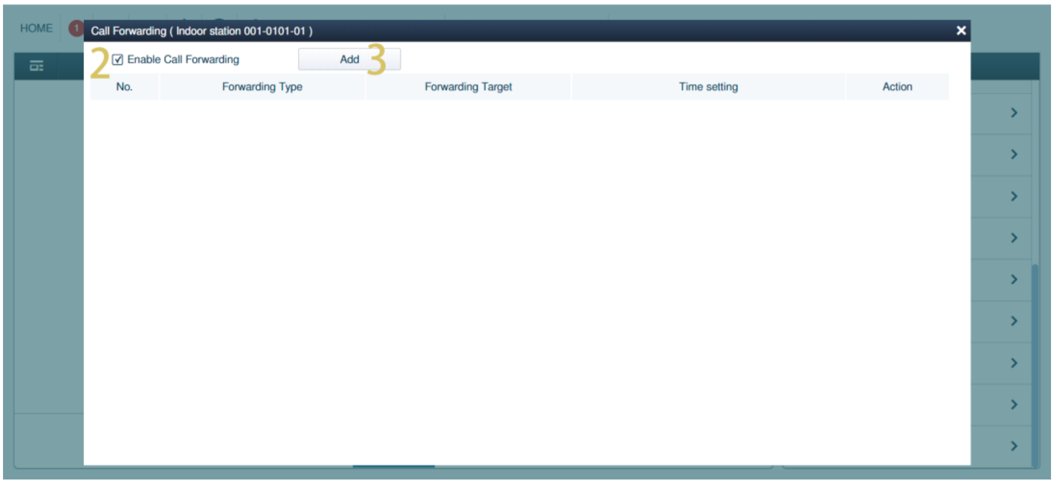
Please follow the steps below:

[1] On the designated Indoor Station screen of SmartAP, click "Call forwarding".

[2] Tick the checkbox to enable the function.

[3] Click "Add".





[4] Select the forwarding type. It can be set to "Direct Forwarding" or "No Answer".

- If "No Answer" is selected, you need to set "Duration", it can be set to "15","20" or "25". The call will be forwarded after the duration time specified.
- If "Direct Forwarding" is selected, the call will be redirected immediately.

[5] Click "Select" to select the target device.

[6] Set the effective time, it can be set to "Specified time slot" or "Always".

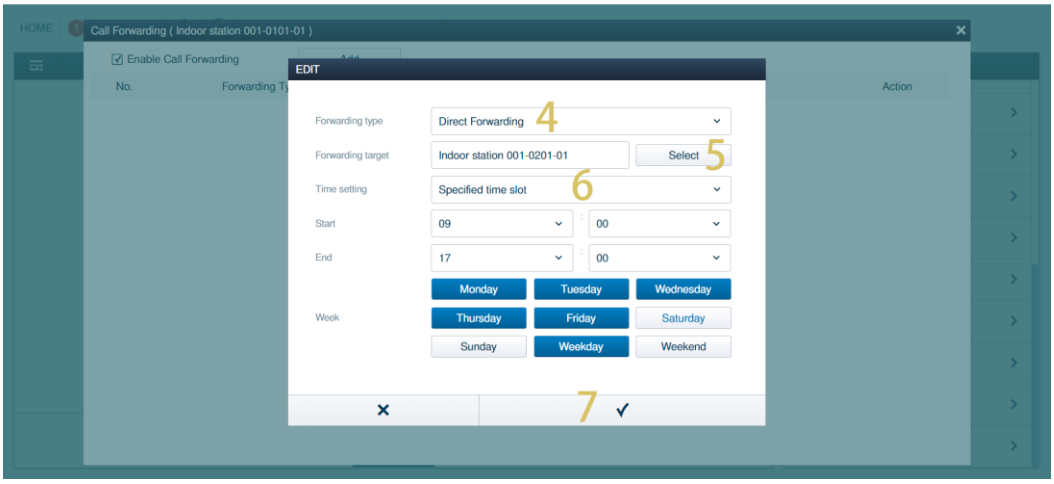
- If the effective time is set to ""Specified time slot", you need to set the start time, end time and work days.

[7] Click " √ ".

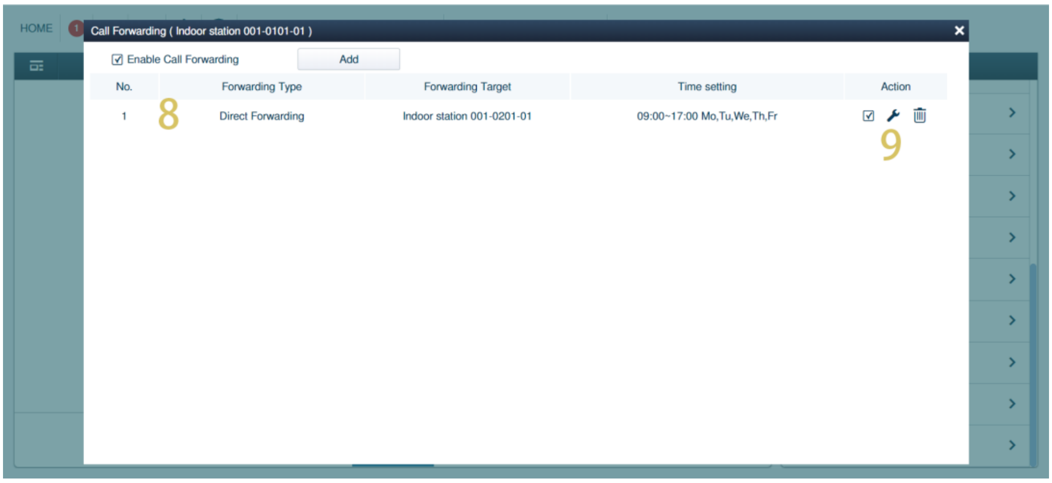
[8] The forwarding setting is displayed on the screen.

[9] Manage the forwarding setting.

- Tick/untick the checkbox to enable/disable the forwarding setting.
- Click " 🔧 " to edit the forwarding setting.
- Click " 🗑 " to remove the forwarding setting.



Forwarding type	Direct Forwarding
Forwarding target	Indoor station 001-0201-01 Select
Time setting	Specified time slot
Start	09 : 00
End	17 : 00
Week	Monday Tuesday Wednesday Thursday Friday Saturday Sunday Weekday Weekend



No.	Forwarding Type	Forwarding Target	Time setting	Action
1	Direct Forwarding	Indoor station 001-0201-01	09:00~17:00 Mo,Tu,We,Th,Fr	☑ 🔧 🗑

5.2.2 Forwarding Call for Guard Units

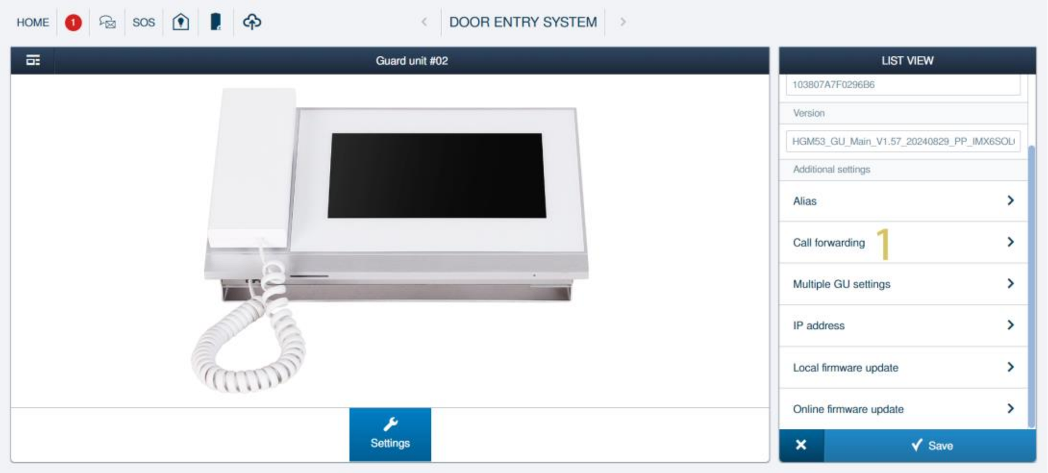
The Forwarding call feature allows the call destinated to one Guard Unit to be redirected to a determined alternative Guard Unit, directly, in specific time slots, or in case of missing answer within a selected time.

Please follow the steps below:

[1] On the designated Guard Unit screen of SmartAP, click "Call forwarding".

[2] Tick the checkbox to enable the function.

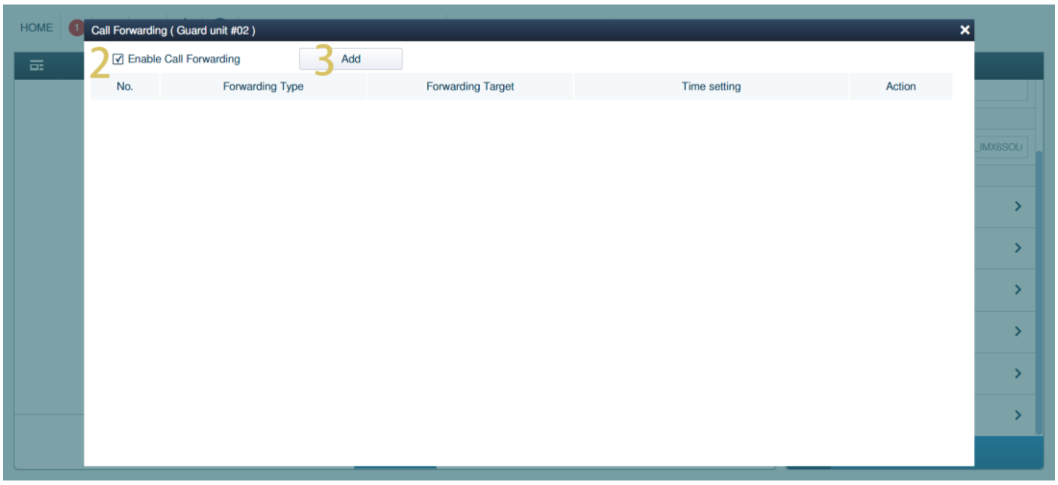
[3] Click "Add".



103807A7F0296B6

Version

HGM53_GU_Main_V1.57_20240829_PP_IMX6SOL



Call Forwarding (Guard unit #02)

☑ Enable Call Forwarding

No.	Forwarding Type	Forwarding Target	Time setting	Action

[4] Select the forwarding type. It can be set to "Direct Forwarding" or "No Answer".

- If "No Answer" is selected, you need to set "Duration", it can be set to "15","20" or "25". The call will be forwarded after the duration time specified.
- If "Direct Forwarding" is selected, the call will be redirected immediately.

[5] Click "Select" to select the target device.

[6] Set the effective time, it can be set to "Specified time slot" or "Always".

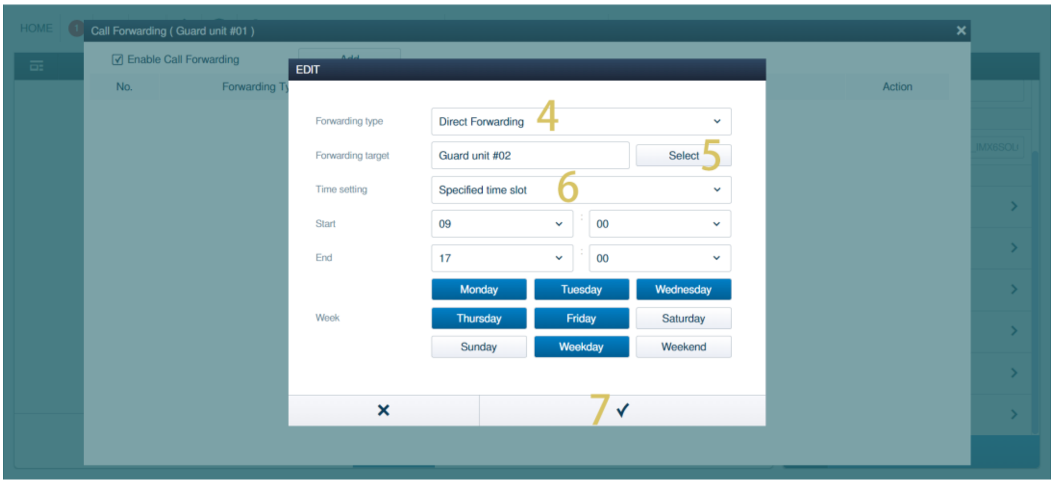
- If the effective time is set to ""Specified time slot", you need to set the start time, end time and work days.

[7] Click " √ ".

[8] The forwarding setting is displayed on the screen.

[9] Manage the forwarding setting.

- Tick/untick the checkbox to enable/disable the forwarding setting.
- Click " 🔧 " to edit the forwarding setting.
- Click " 🗑 " to remove the forwarding setting.


Call Forwarding (Guard unit #01)

☑ Enable Call Forwarding

EDIT

Forwarding type: Direct Forwarding

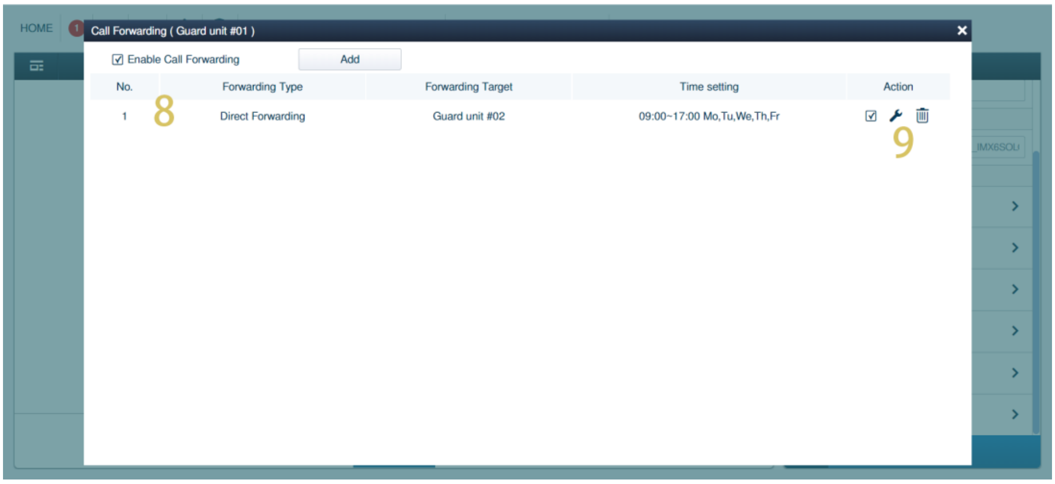
Forwarding target: Guard unit #02 Select

Time setting: Specified time slot

Start: 09 : 00

End: 17 : 00

Week: Monday Tuesday Wednesday Thursday Friday Saturday Sunday Weekday Weekend


Call Forwarding (Guard unit #01)

☑ Enable Call Forwarding Add

No.	Forwarding Type	Forwarding Target	Time setting	Action
1	Direct Forwarding	Guard unit #02	09:00~17:00 Mo,Tu,We,Th,Fr	☑ 🔧 🗑

5.3 Linking Guard Units

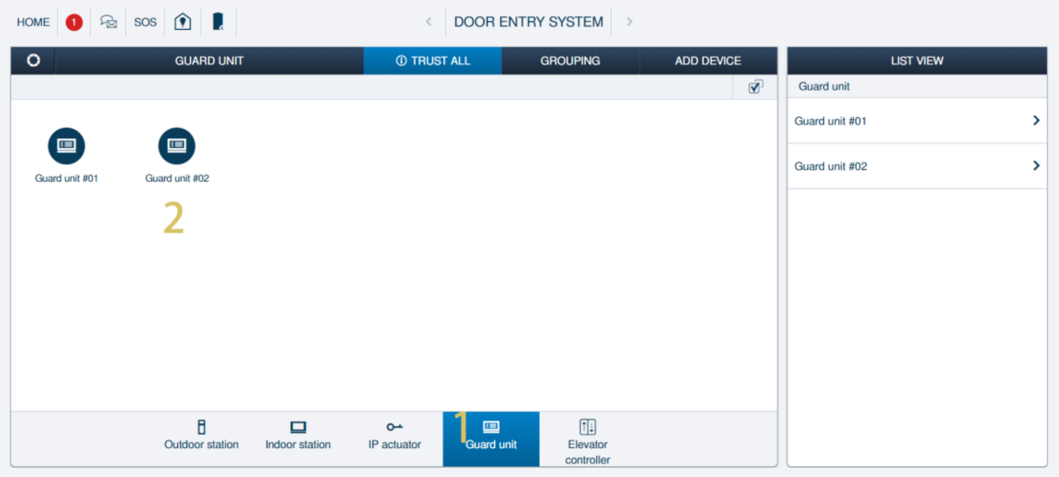
All Guard Units except Guard Unit 1 can be linked to Guard Unit 1. After the setting, these Guard Units will ring at the same time as Guard Unit 1 during an incoming call.

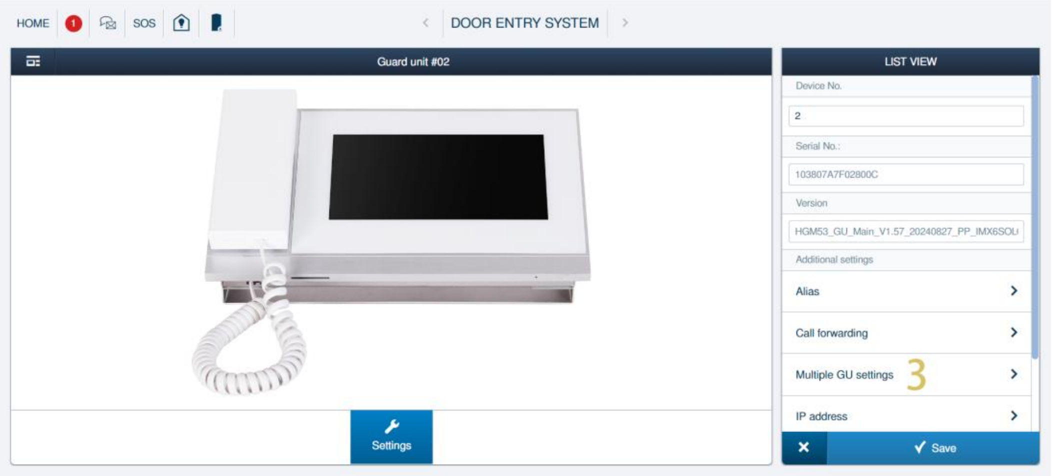
Please follow the steps below:

[1] On the "Door Entry System" screen, click "Guard Unit".

[2] Click the designated Guard Unit.

[3] On the designated Guard Unit screen, click "Multiple GU settings".





Device No.: 2

Serial No.: 103807A7F02800C

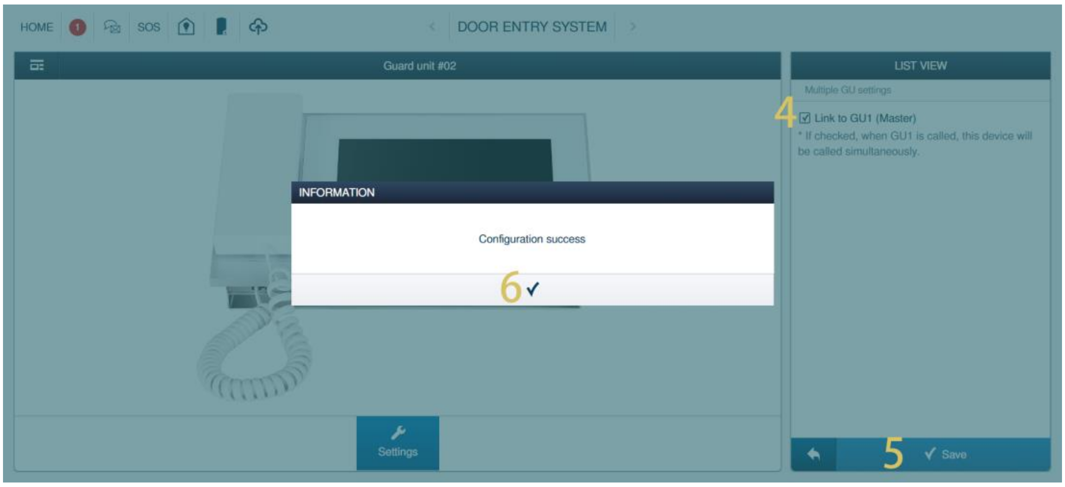
Version: HGM53_GU_Main_V1.57_20240827_PP_IMX6SOL

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

[5] Click "Save".

[6] Click " √ ".

[7] Go back to "Guard Unit" screen, click Guard Unit 1.



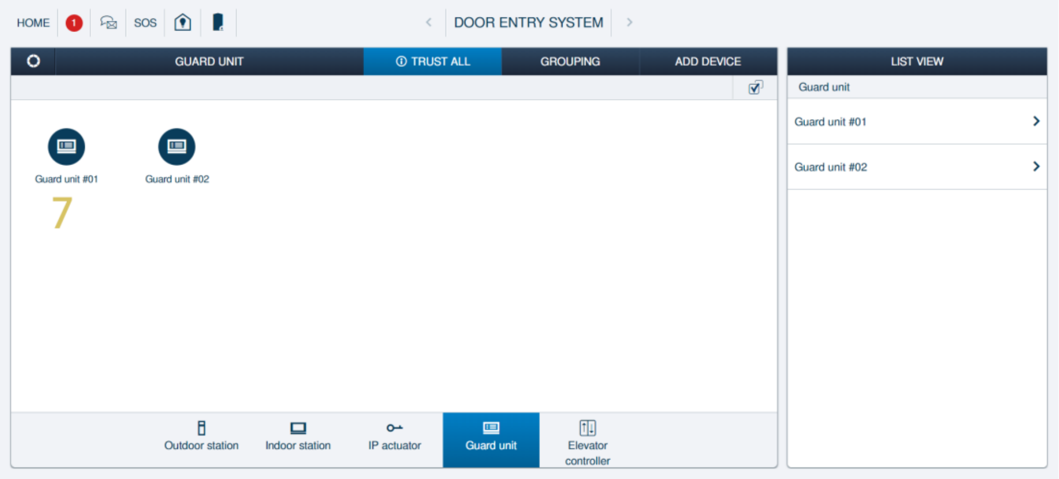
INFORMATION

Configuration success

Multiple GU settings

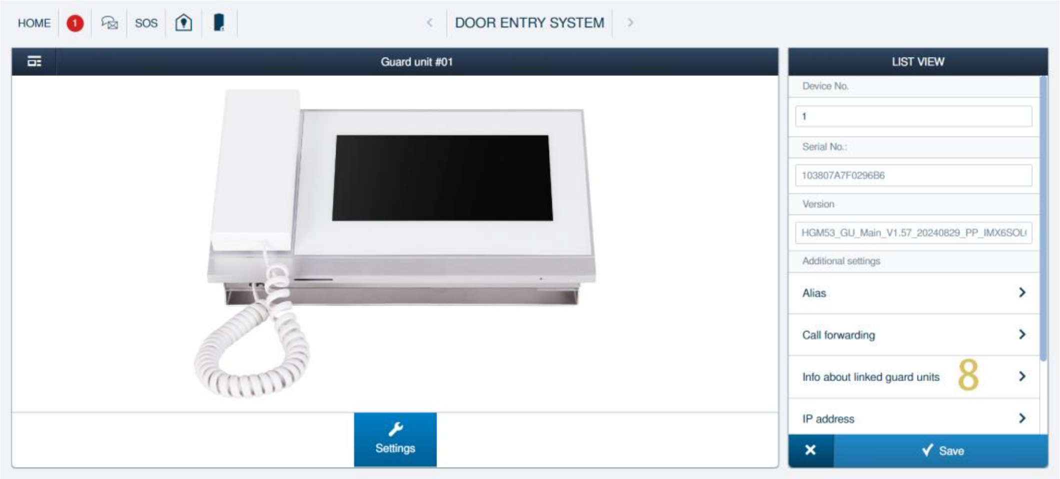
☑ Link to GU1 (Master)

* If checked, when GU1 is called, this device will be called simultaneously.



[8] On the Guard Unit 1 screen, click "Info about linked Guard Units".

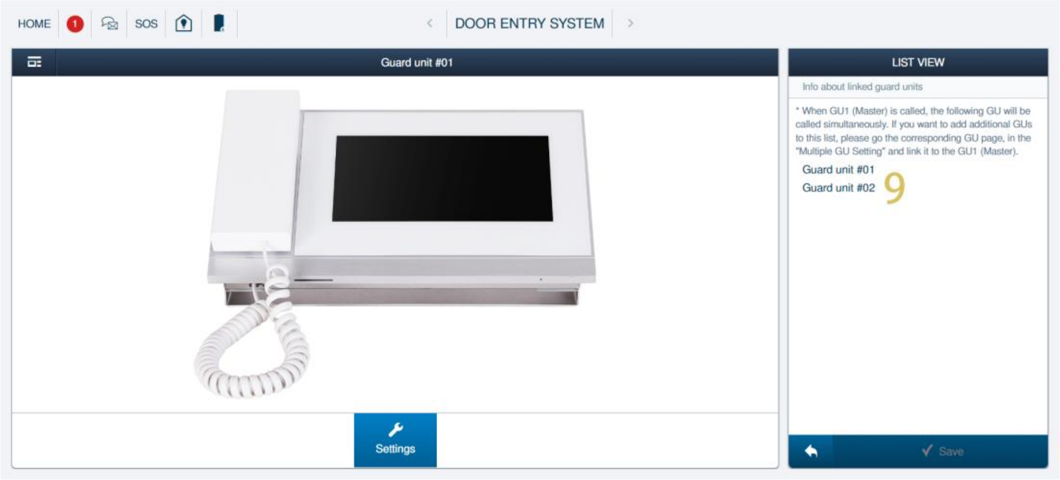
[9] The linked Guard Units will be displayed on the screen.



Device No.: 1

Serial No.: 103807A7F0296B6

Version: HGM53_GU_Main_V1.57_20240829_PP_IMX6SOL



* When GU1 (Master) is called, the following GU will be called simultaneously. If you want to add additional GUs to this list, please go the corresponding GU page, in the "Multiple GU Setting" and link it to the GU1 (Master).

Guard unit #01
Guard unit #02

6 Firmware update

6.1 Updating overview

There are 4 scenarios for updating the firmware.

No.	Using SmartAP	Connect to internet	Reference
1	No, Single Family Home mode	Yes	For more details, see chapter 6.2 “Updating the firmware - Single Family Home mode with internet“ on page 188.
2	No, Single Family Home mode	No	For more details, see chapter 6.3 “Updating the firmware - Single Family Home mode without internet“ on page 194.
3	Yes	Yes	For more details, see chapter 6.4 “Updating the firmware - SmartAP with internet“ on page 199.
4	Yes	No	For more details, see chapter 6.5 “Updating the firmware - SmartAP without internet“ on page 203.

6.2 Updating the firmware - Single Family Home mode with internet

6.2.1 Updating the firmware of the panel online

This chapter applies to IP Touch 7, IP Touch 10 and IP Touch Lite 7, not including Audio IP.

On the panel, please follow the steps below:

[1] On the "Settings" screen, tap "Software Update".

[2] The current software version will be displayed on the screen.

[3] Tick the check box to enable the download function.

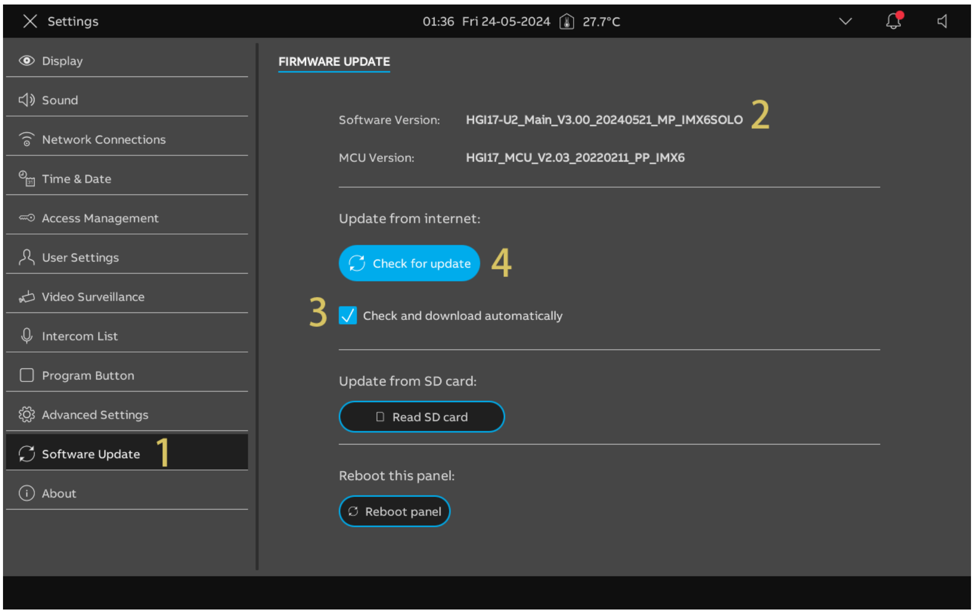
- If this function is enabled, the panel will check the new version and download the firmware automatically.
- If this function is enables, please skip the step 4-8 and continue the step 9.

[4] Tap "Check for update".

[5] The new version will be displayed on the screen.

[6] A release note for the new version will be displayed on the screen.

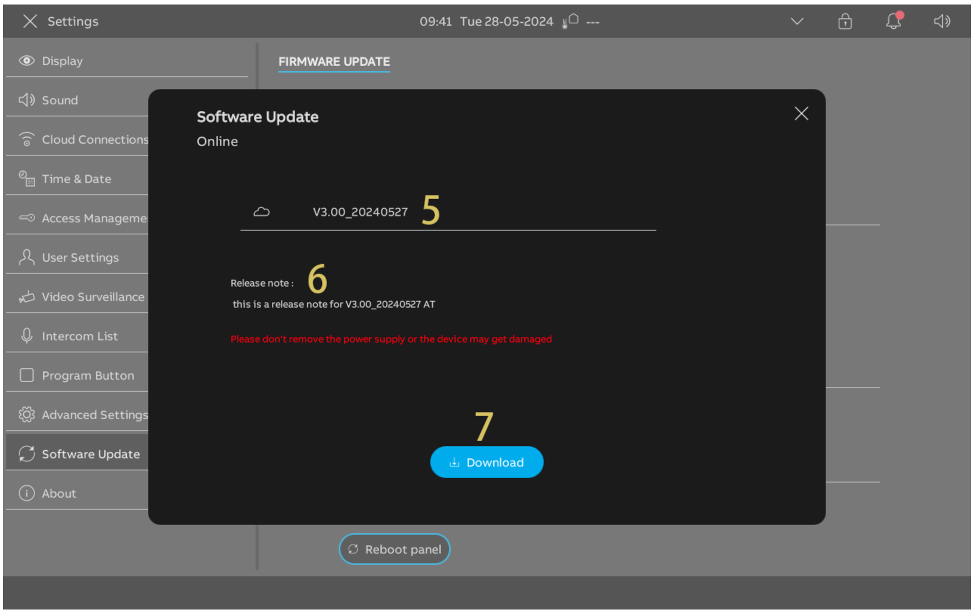
[7] Tap "Download".



Software Version: HGI17-U2_Main_V3.00_20240521_MP_IMX6SOLO

MCU Version: HGI17_MCU_V2.03_20220211_PP_IMX6

☑ Check and download automatically



Software Update

Online

V3.00_20240527

Release note :

this is a release note for V3.00_20240527 AT

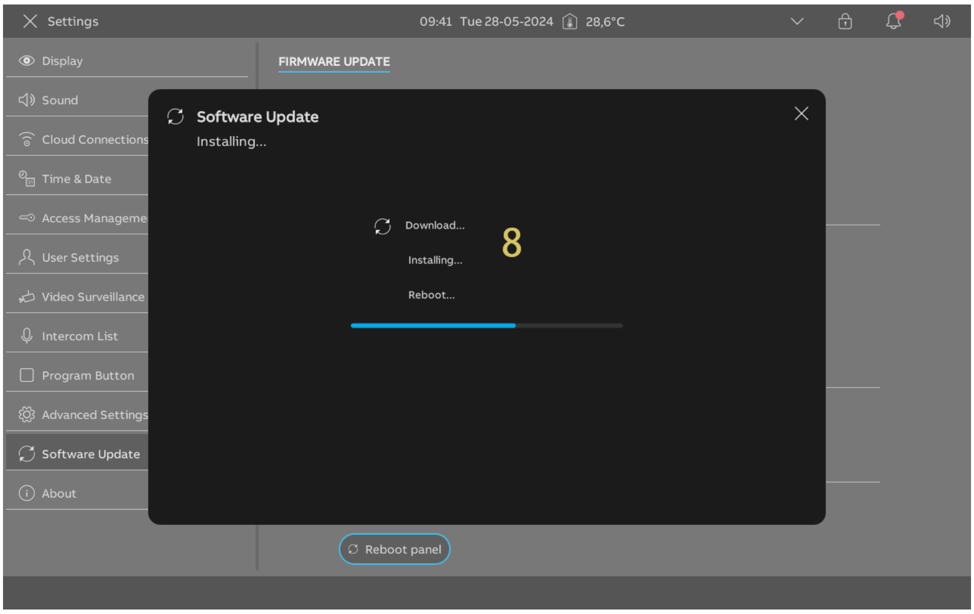
Please don't remove the power supply or the device may get damaged

[8] It will take a little while to download the new software.

[9] Tick the check box to accept the licence.

[10]Tap "OK".

- If you don’t want to update the firmware, tap "x" to exit.



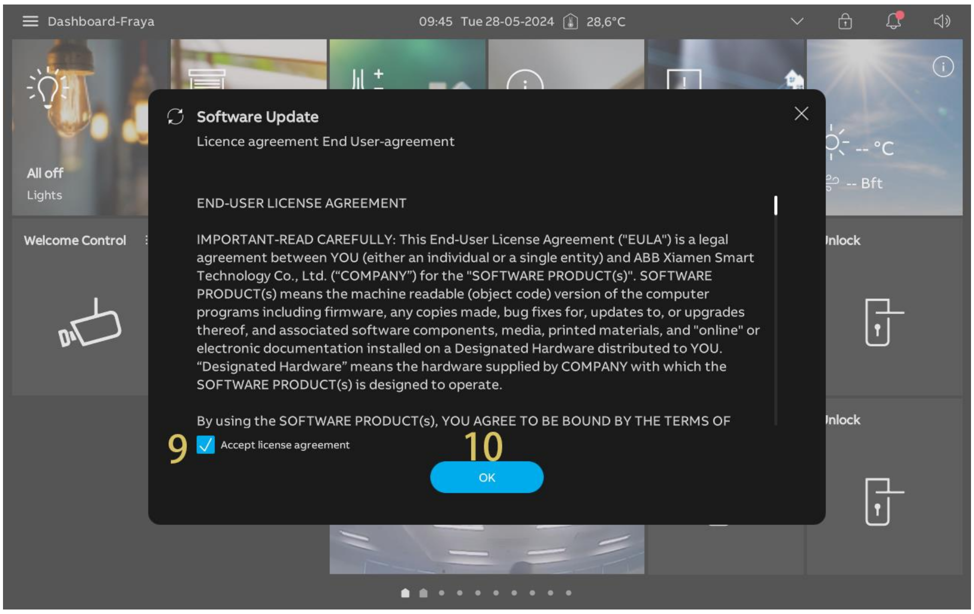
Software Update

Installing...

Download...

Installing...

Reboot...



Software Update

Licence agreement End User-agreement

END-USER LICENSE AGREEMENT

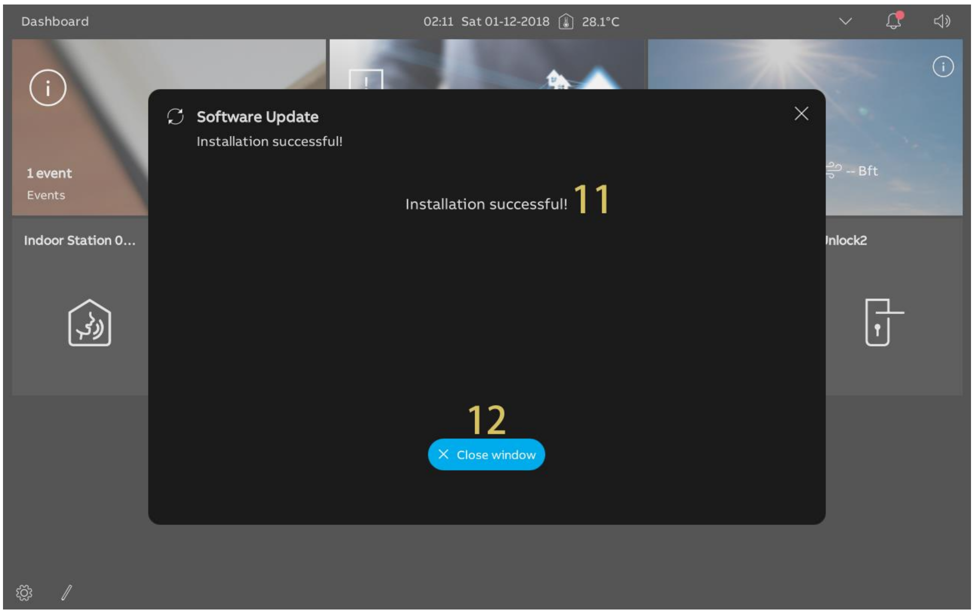
IMPORTANT-READ CAREFULLY: This End-User License Agreement ("EULA") is a legal agreement between YOU (either an individual or a single entity) and ABB Xiamen Smart Technology Co., Ltd. (“COMPANY”) for the "SOFTWARE PRODUCT(S)". SOFTWARE PRODUCT(S) means the machine readable (object code) version of the computer programs including firmware, any copies made, bug fixes for, updates to, or upgrades thereof, and associated software components, media, printed materials, and "online" or electronic documentation installed on a Designated Hardware distributed to YOU. “Designated Hardware” means the hardware supplied by COMPANY with which the SOFTWARE PRODUCT(S) is designed to operate.

By using the SOFTWARE PRODUCT(S), YOU AGREE TO BE BOUND BY THE TERMS OF

☑ Accept license agreement

[11]"Installation successful!" will be displayed on the screen if successful.

[12]Tap "Close window".



Software Update

Installation successful!

Installation successful!

6.2.2 Updating the firmware of the IP Actuator or the 2nd OS via APP

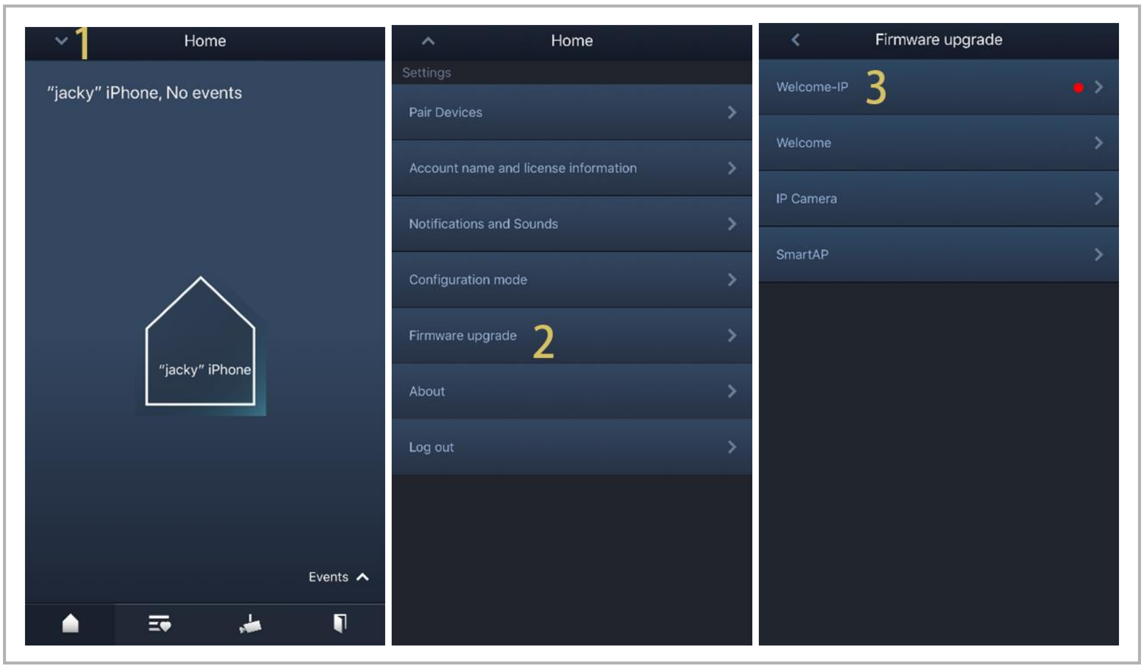
On Single Family Home mode, IP Actuator and the 2nd OS should be updated via APP. Please follow the steps below:

[1] On the APP "Home" screen of APP, tap "∨".

[2] Tap "Firmware upgrade".

[3] Click "Welcome-IP".

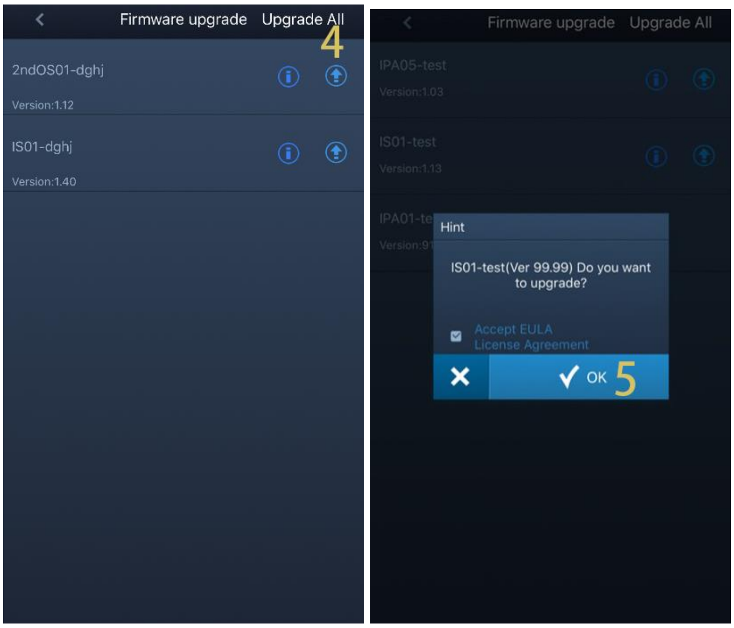
- " ● " will be displayed if there is a new version for the devices.



[4] Find the designated 2nd OS or IP Actuator, tap " ⬆ ".

- Tap " ⓘ " to view details about the new version.

[5] Tap "OK".



IS01-test(Ver 99.99) Do you want to upgrade?

6.3 Updating the firmware - Single Family Home mode without internet

6.3.1 Updating the firmware of the panel via SD card

This chapter applies to IP Touch 7 and IP Touch 10, not including IP Touch Lite 7 and Audio IP.

Please ensure that the firmware update file has been stored in the SD card and the SD card has been inserted into the panel.

Please follow the steps below:

[1] On the "Settings" screen, tap "Software Update".

[2] The current software version will be displayed on the screen.

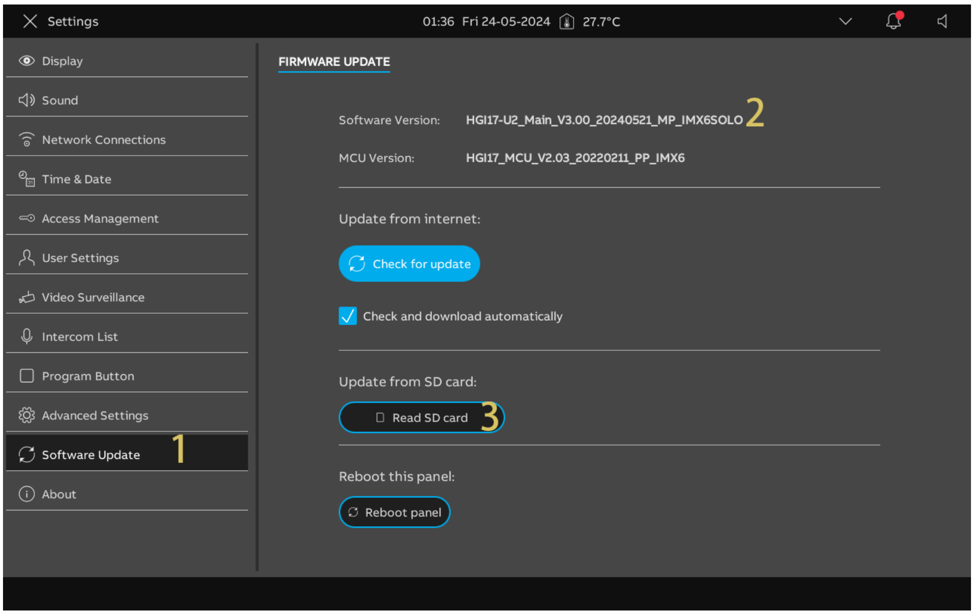
[3] Go to the "Update from SD card" section, tap "Read SD card".

[4] Select the designated update file.

[5] Tap "Install the update".

[6] A release note for the new version will be displayed on the screen.

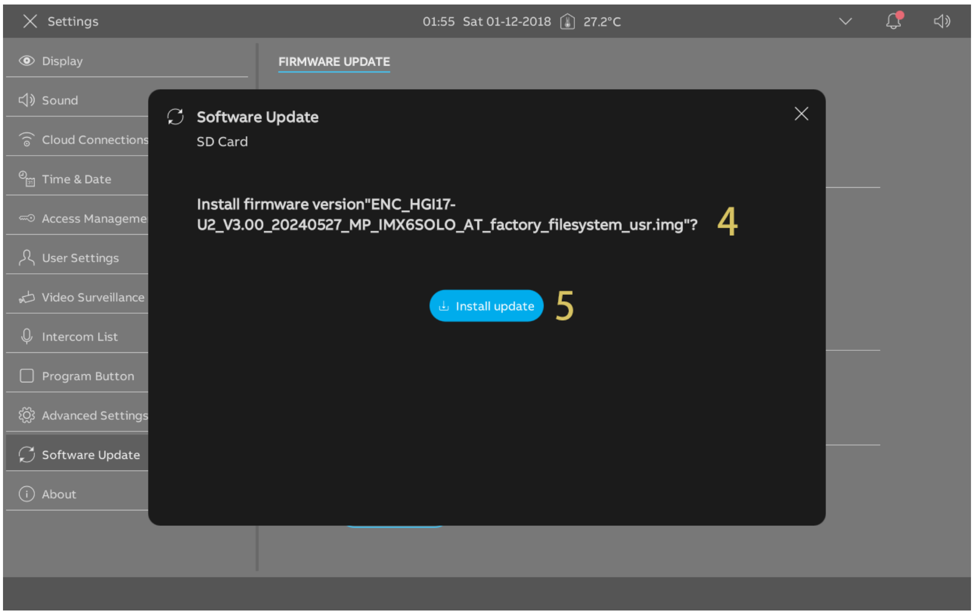
[7] Tap "Download".



Software Version: HGI17-U2_Main_V3.00_20240521_MP_IMX6SOLO

MCU Version: HGI17_MCU_V2.03_20220211_PP_IMX6

☑ Check and download automatically

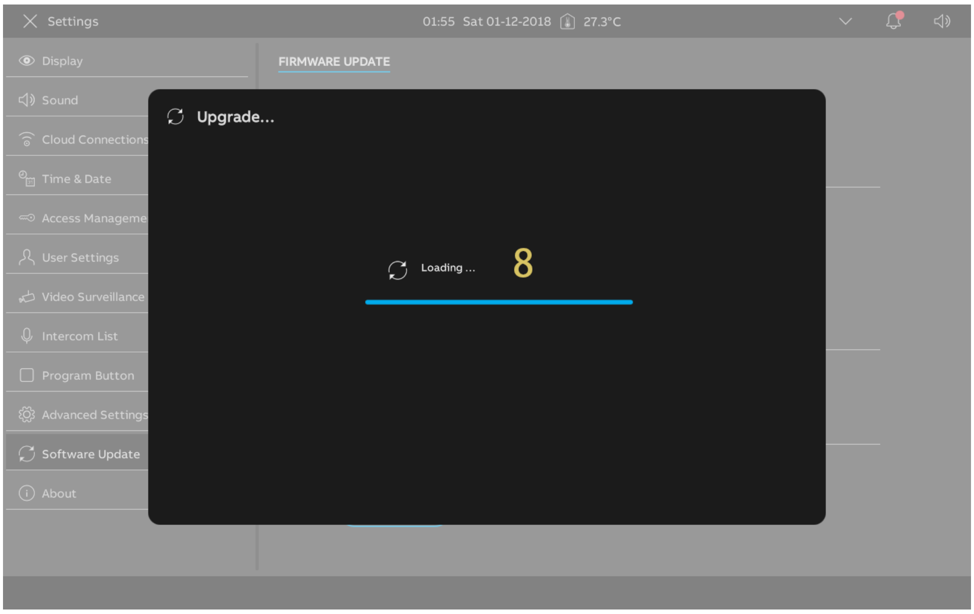


Install firmware version"ENC_HGI17-U2_V3.00_20240527_MP_IMX6SOLO_AT_factory_filesystem_usr.img"?

[8] It will take a little while to prepare the installation.

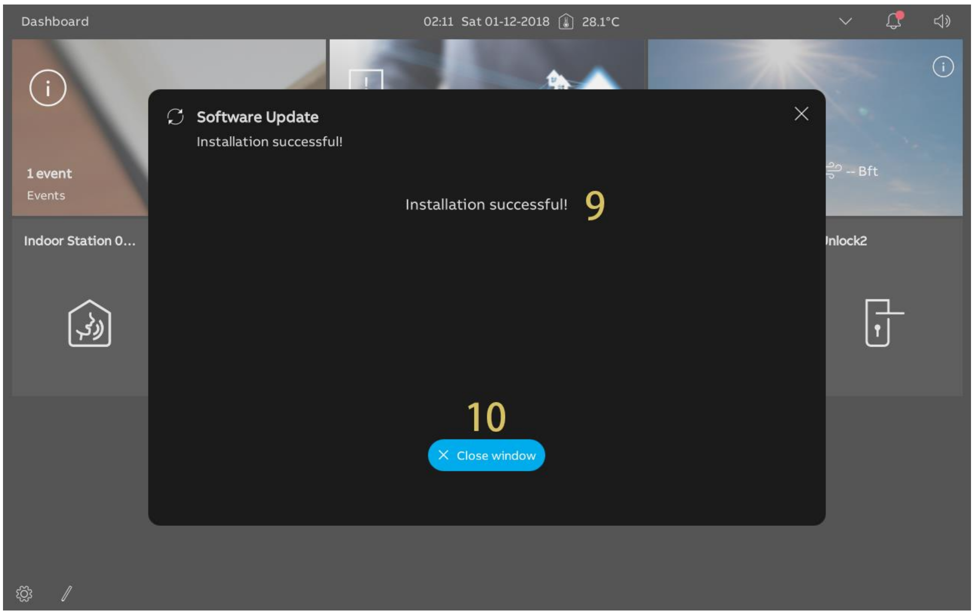
[9] "Installation successful!" will be displayed on the screen if successful.

[10]Tap "Close window".



Upgrade...

Loading ...



Software Update

Installation successful!

Installation successful!

6.3.2 Updating the firmware of the IP Actuator or the 2nd OS via SD card

The following operations take the 2nd OS as an example.

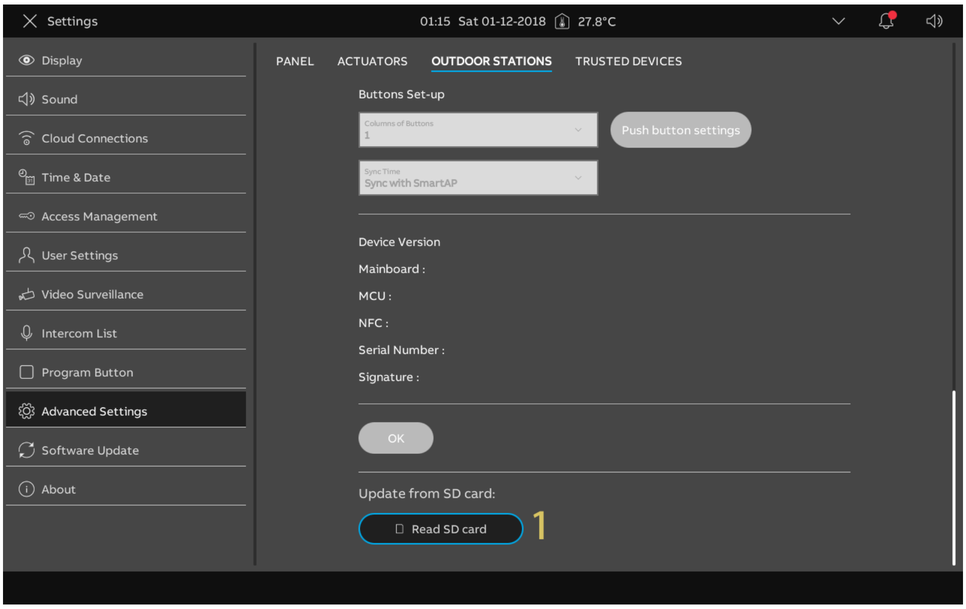
Please follow the steps below:

[1] On the "Outdoor Stations" screen of the panel, tap "Read SD card".

[2] Select the designated Outdoor Station.

[3] Select the updating file from SD card.

[4] Tap "Save & Close".



Buttons Set-up

Columns of Buttons: 1

Sync Time: Sync with SmartAP

Device Version

Mainboard :

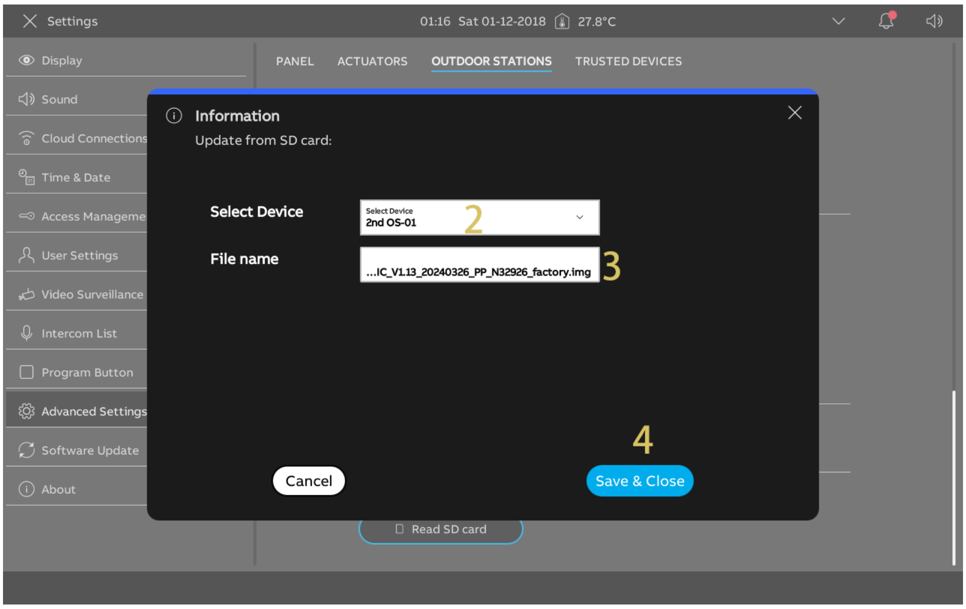
MCU :

NFC :

Serial Number :

Signature :

Update from SD card:



Information

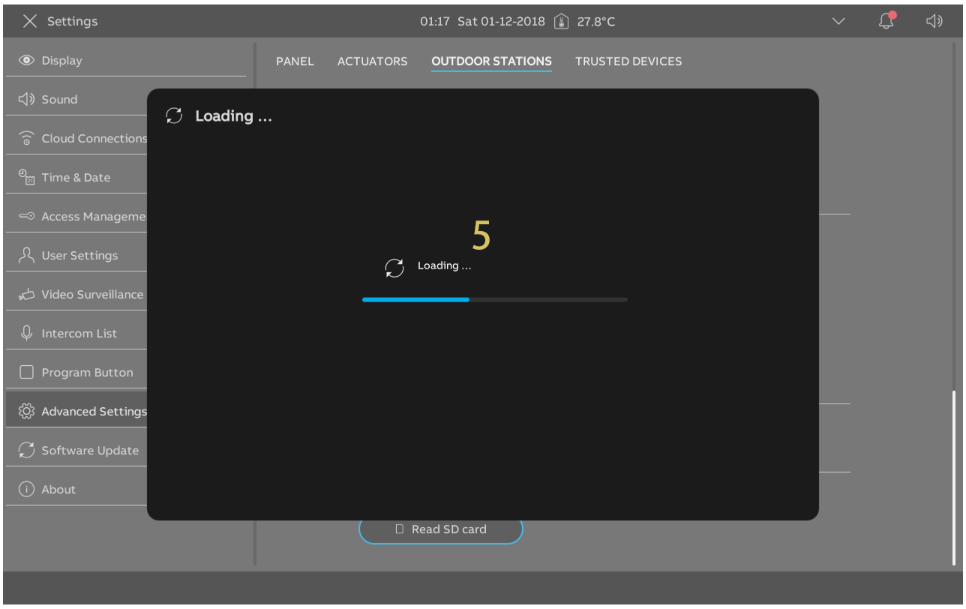
Update from SD card:

Select Device: 2nd OS-01

File name: ...IC_V1.13_20240326_PP_N32926_factory.img

[5] "Loading…" will be displayed to indicate that the upgrade is in progress.

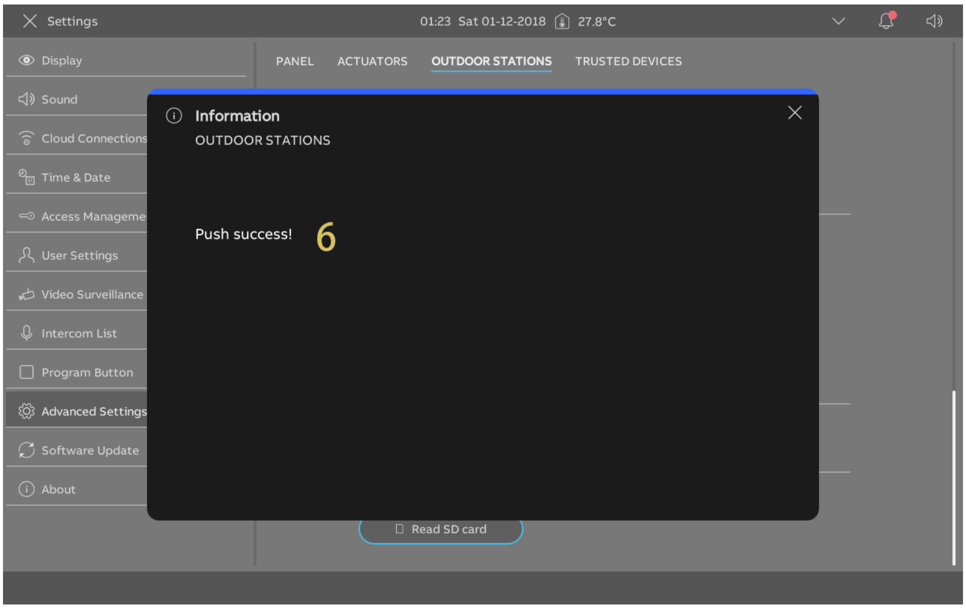
[6] "Push success!" will be displayed if the upgrade is successful.



Loading ...

5

Loading ...



Information

OUTDOOR STATIONS

Push success! 6

6.4 Updating the firmware - SmartAP with internet

6.4.1 Updating the firmware of SmartAP online

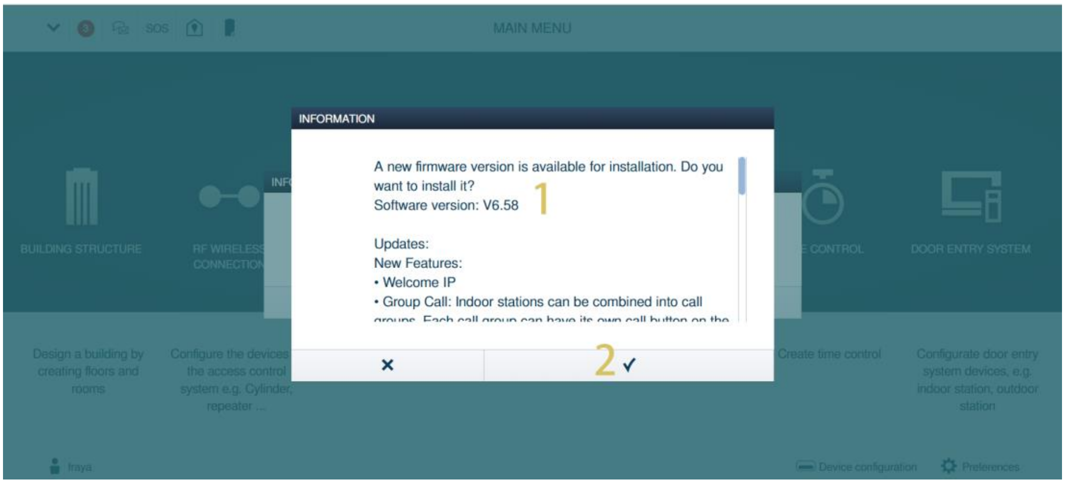
If SmartAP can connect to the internet, a pop-up window will appear automatically when there is a new firmware.

Please follow the steps below:

[1] The latest version will be displayed.

[2] Click " √ ".

[3] Download the latest firmware.

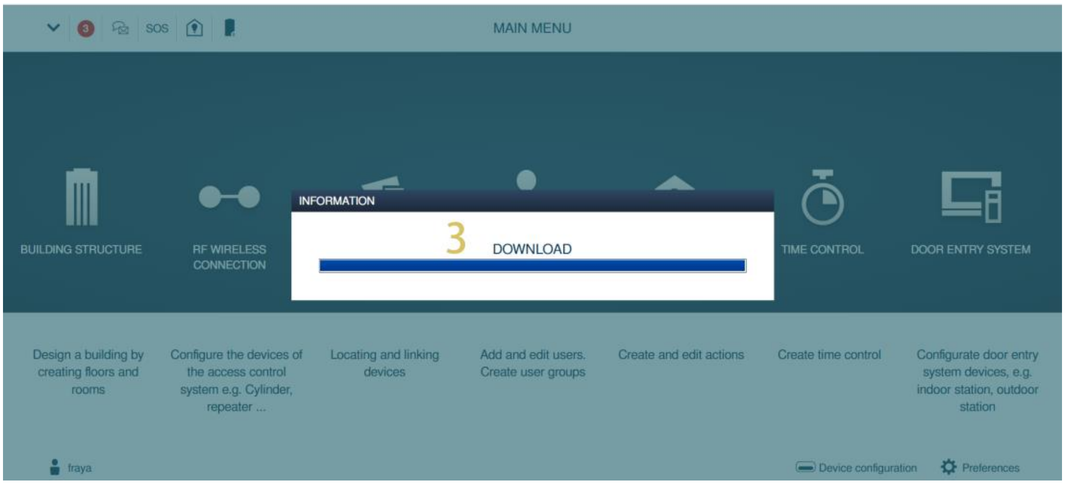


INFORMATION

A new firmware version is available for installation. Do you want to install it?
Software version: V6.58

Updates:
New Features:
• Welcome IP
• Group Call: Indoor stations can be combined into call groups. Each call group can have its own call button on the

MAIN MENU
SOS
1
2
×
✓
BUILDING STRUCTURE
RF WIRELESS CONNECTION
CONTROL
DOOR ENTRY SYSTEM
Design a building by creating floors and rooms
Configure the devices of the access control system e.g. Cylinder, repeater ...
Create time control
Configurate door entry system devices, e.g. indoor station, outdoor station
fraya
Device configuration
Preferences



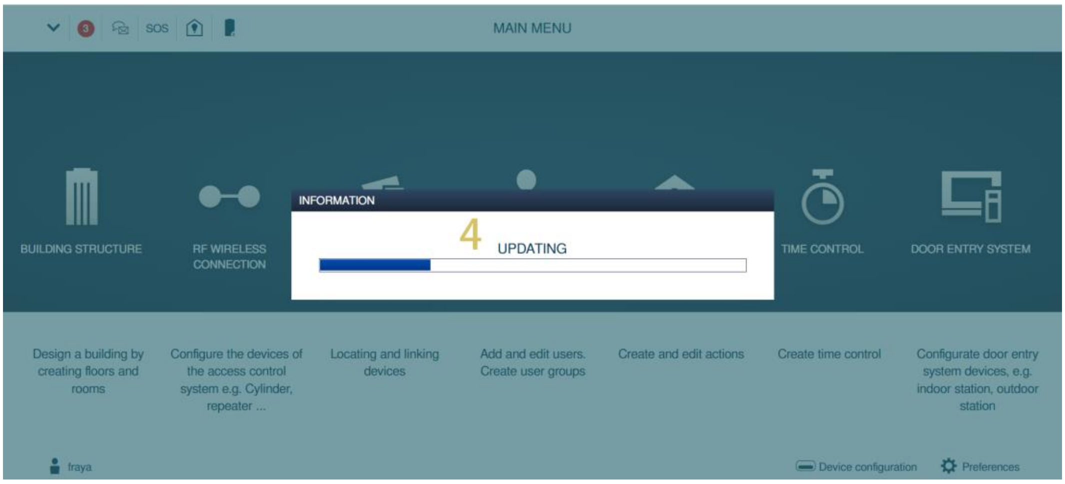
INFORMATION

DOWNLOAD

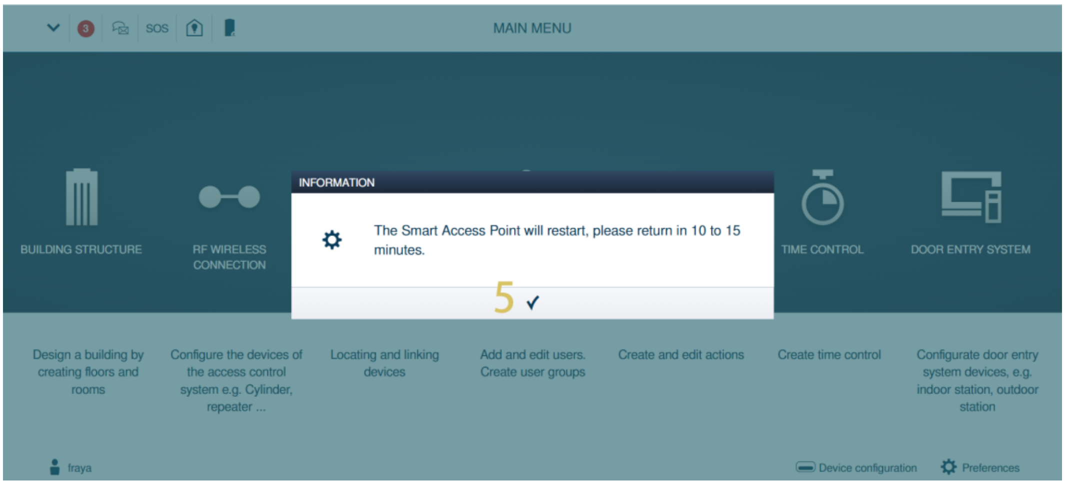
MAIN MENU
SOS
3
BUILDING STRUCTURE
RF WIRELESS CONNECTION
TIME CONTROL
DOOR ENTRY SYSTEM
Design a building by creating floors and rooms
Configure the devices of the access control system e.g. Cylinder, repeater ...
Locating and linking devices
Add and edit users. Create user groups
Create and edit actions
Create time control
Configurate door entry system devices, e.g. indoor station, outdoor station
fraya
Device configuration
Preferences

[4] Updating the firmware.

[5] Click " √ " to restart SmartAP.



MAIN MENU
SOS
BUILDING STRUCTURE
RF WIRELESS CONNECTION
TIME CONTROL
DOOR ENTRY SYSTEM
INFORMATION
4
UPDATING
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
fraya
Device configuration
Preferences



INFORMATION

The Smart Access Point will restart, please return in 10 to 15 minutes.

MAIN MENU
SOS
BUILDING STRUCTURE
RF WIRELESS CONNECTION
TIME CONTROL
DOOR ENTRY SYSTEM
5
✓
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
fraya
Device configuration
Preferences

6.4.2 Updating the firmware of other devices online

This chapter applies to all devices of Welcome IP system except SmartAP.

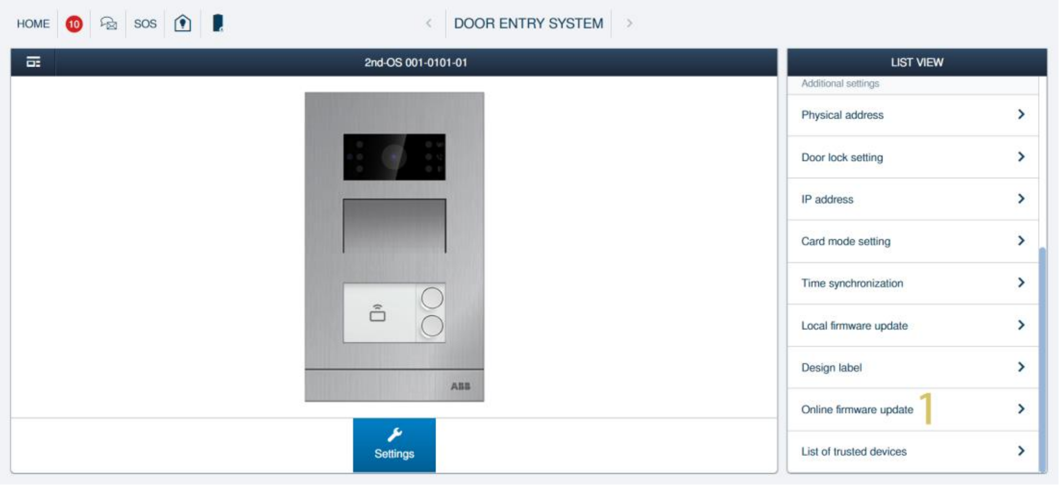
The following operations take the 2nd OS as an example.

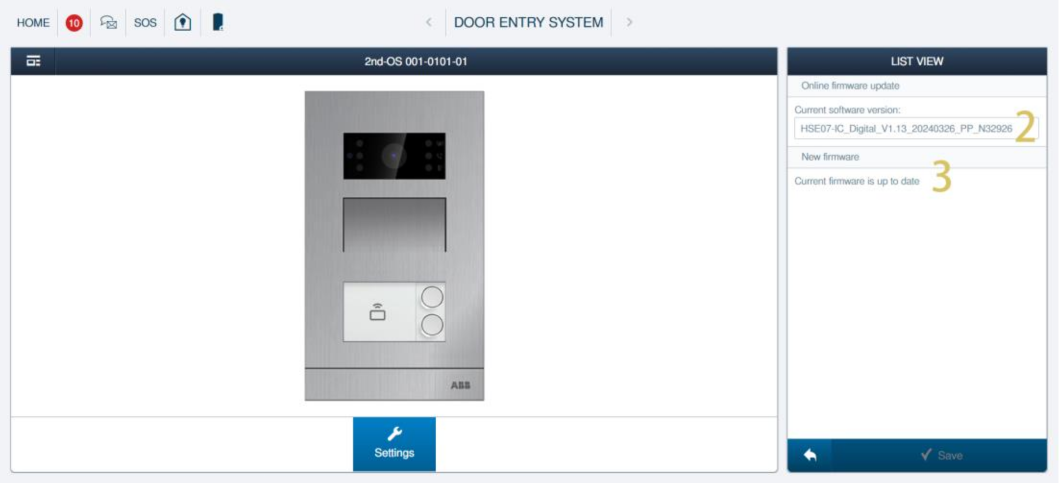
Please follow the steps below:

[1] On the designated device screen, click "Online firmware update".

[2] Current firmware version will be displayed.

[3] "Current firmware is up to date" will be displayed if no newer version is available.





Current software version:

HSE07-IC_Digital_V1.13_20240326_PP_N32926

Current firmware is up to date

6.4.3 Updating the public devices online in batches

Note

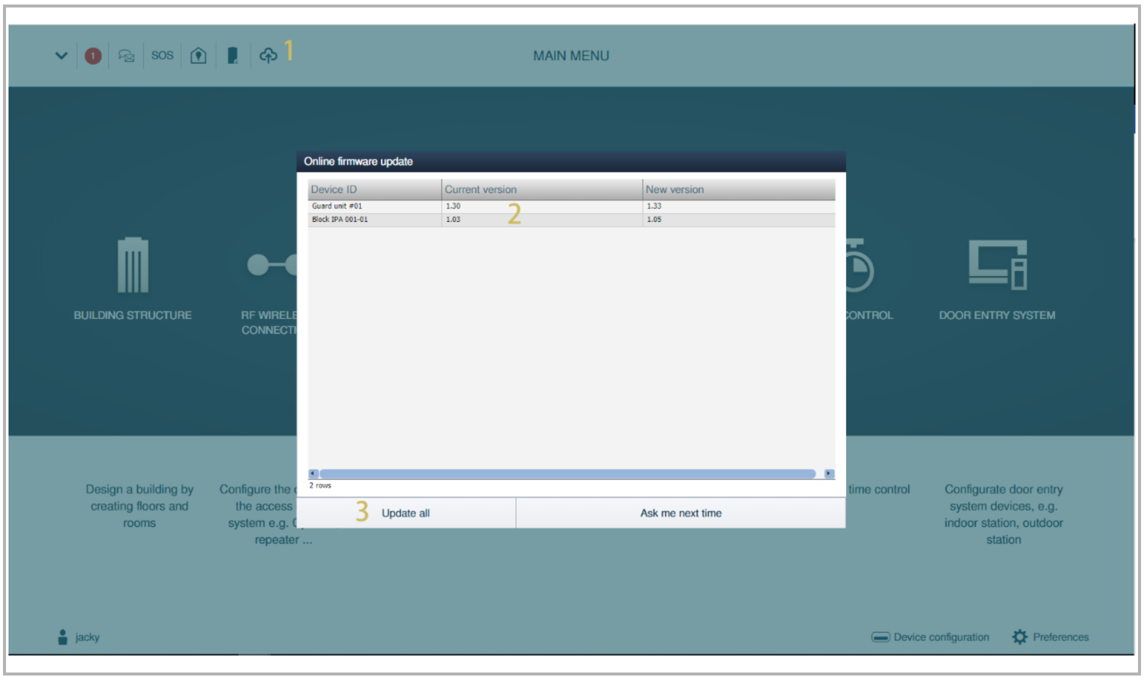
Only the devices which are placed on the public areas (e.g. Guard unit, building IPA, network IPA etc.) can be updated via this method.

Please follow the steps below:

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

[2] The devices to be updated are displayed on the screen.

[3] Click "Update all" to update all the devices in batches.



Online firmware update

Device ID	Current version	New version
Guard unit #01	1.30	1.33
Block IPA 001-01	1.03	1.05

2 rows

SOS
1
MAIN MENU
2
BUILDING STRUCTURE
RF WIRELE
CONNECTI
CONTROL
DOOR ENTRY SYSTEM
Design a building by creating floors and rooms
Configure the the access system e.g. repeater ...
time control
Configurate door entry system devices, e.g. indoor station, outdoor station
3
Update all
Ask me next time
jacky
Device configuration
Preferences

6.5 Updating the firmware - SmartAP without internet

6.5.1 Updating the firmware of SmartAP locally

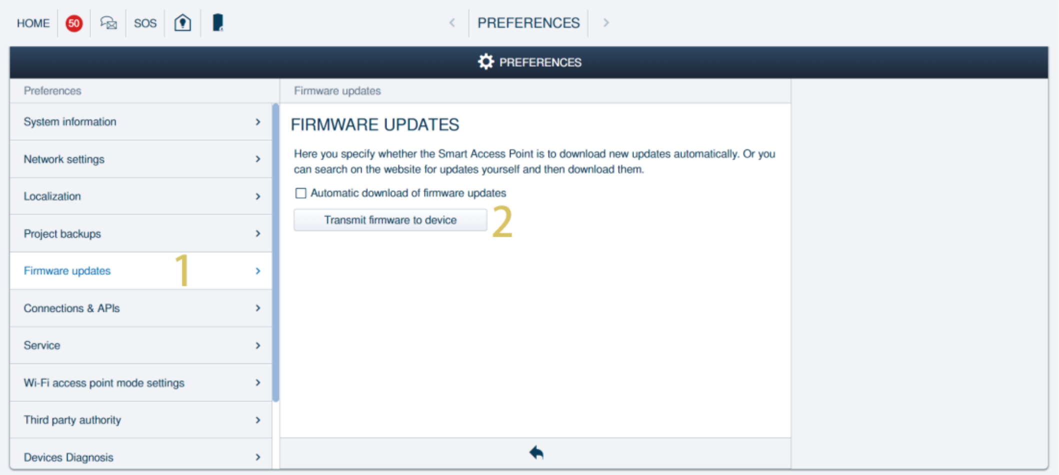
Please follow the steps below:

[1] On the "Preferences" screen of SmartAP, click "Firmware updates".

[2] Click "Transmit firmware to devices".

[3] Click "Browse" to add the new firmware.

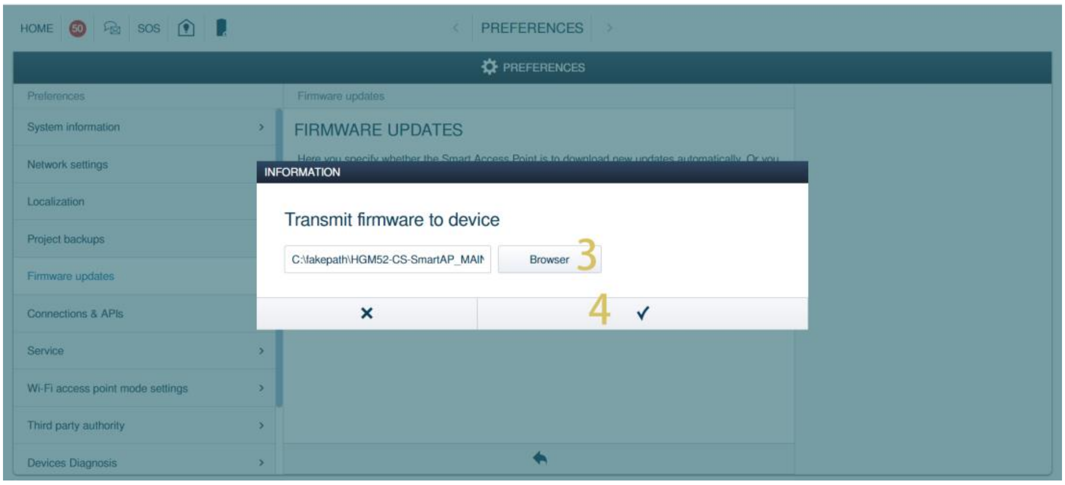
[4] Click " √ ".



FIRMWARE UPDATES

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.

□ Automatic download of firmware updates



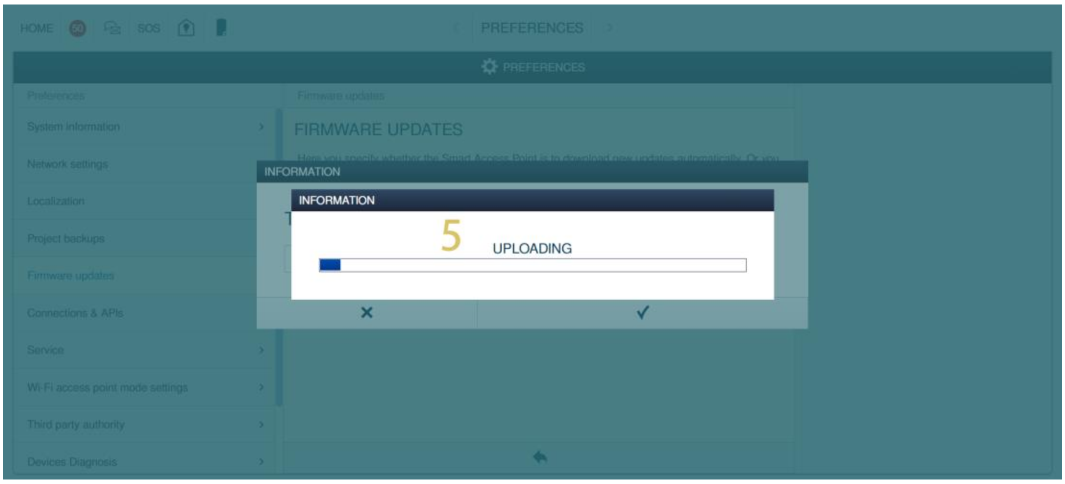
Transmit firmware to device

C:\fakepath\HGM52-CS-SmartAP_MAIN

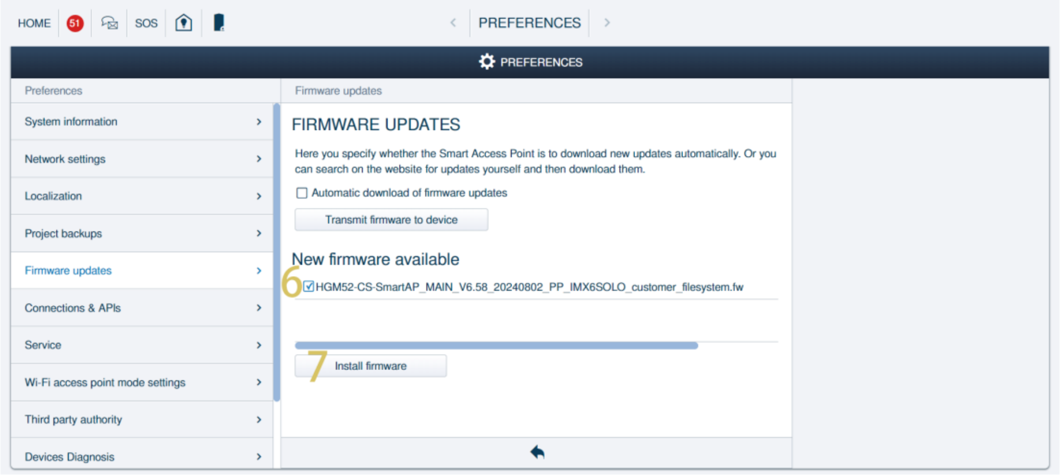
[5] Updating the firmware.

[6] Tick the check box to select the designated firmware.

[7] Click "Install firmware".



UPLOADING



FIRMWARE UPDATES

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.

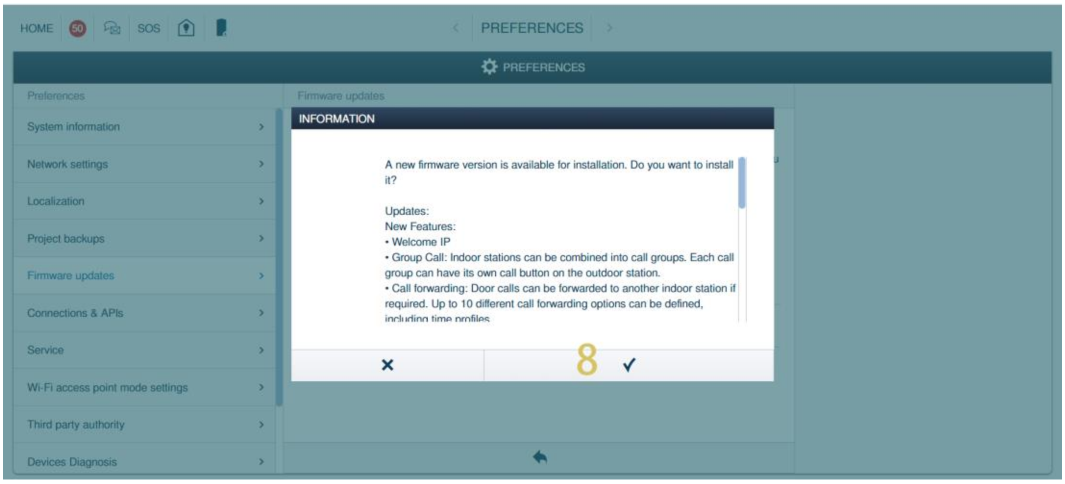
☐ Automatic download of firmware updates

New firmware available

☑ HGM52-CS-SmartAP_MAIN_V6.58_20240802_PP_IMX6SOLO_customer_filesystem.fw

[8] New features will be displayed on the screen, click " √ ".

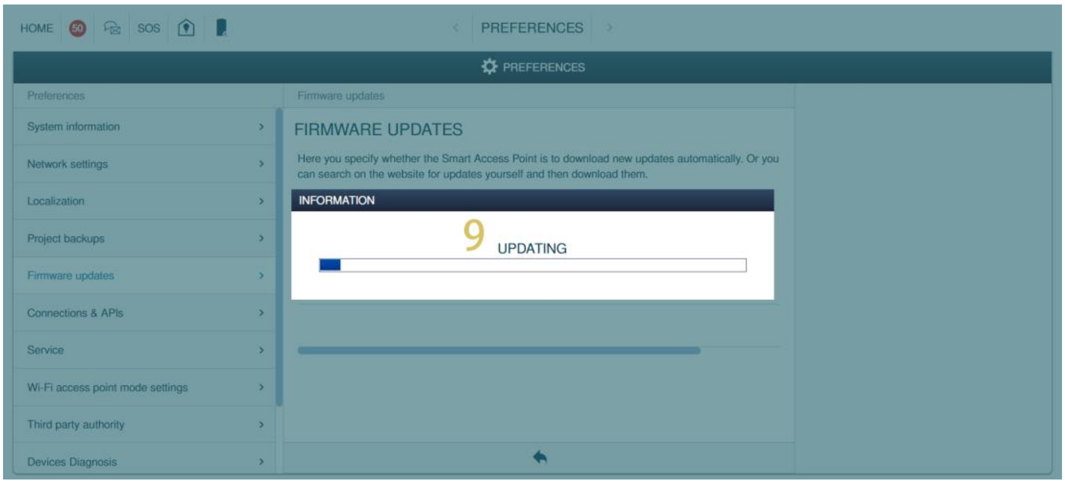
[9] Updating the firmware.



INFORMATION

A new firmware version is available for installation. Do you want to install it?

Updates:
New Features:
• Welcome IP
• Group Call: Indoor stations can be combined into call groups. Each call group can have its own call button on the outdoor station.
• Call forwarding: Door calls can be forwarded to another indoor station if required. Up to 10 different call forwarding options can be defined, including time profiles



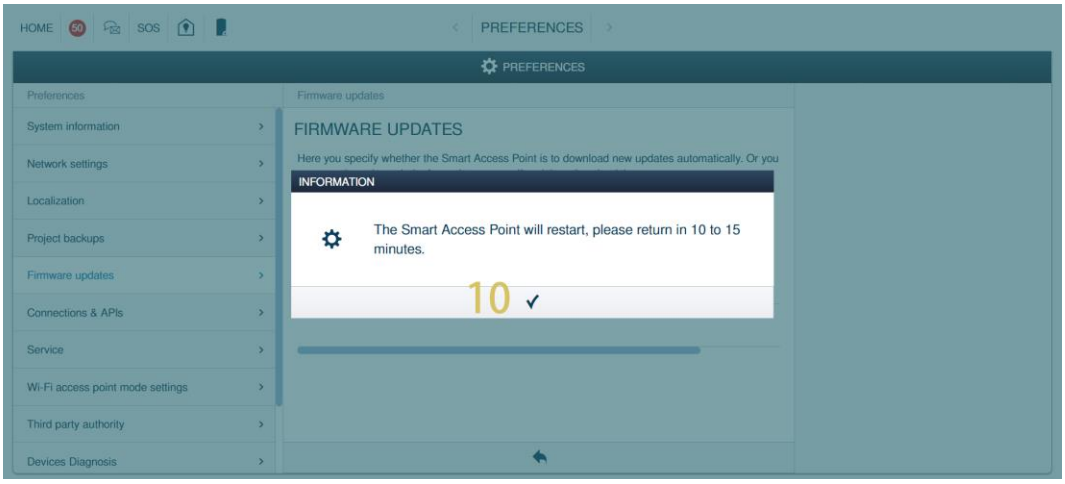
FIRMWARE UPDATES

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.

INFORMATION

UPDATING

[10]Click " √ " to restart SmartAP.



Here you specify whether the Smart Access Point is to download new updates automatically. Or you

The Smart Access Point will restart, please return in 10 to 15 minutes.

6.5.2 Updating the firmware of other devices locally one by one

This chapter applies to all devices of Welcome IP system except SmartAP.

The following operations take the 2nd OS as an example.

Please follow the steps below:

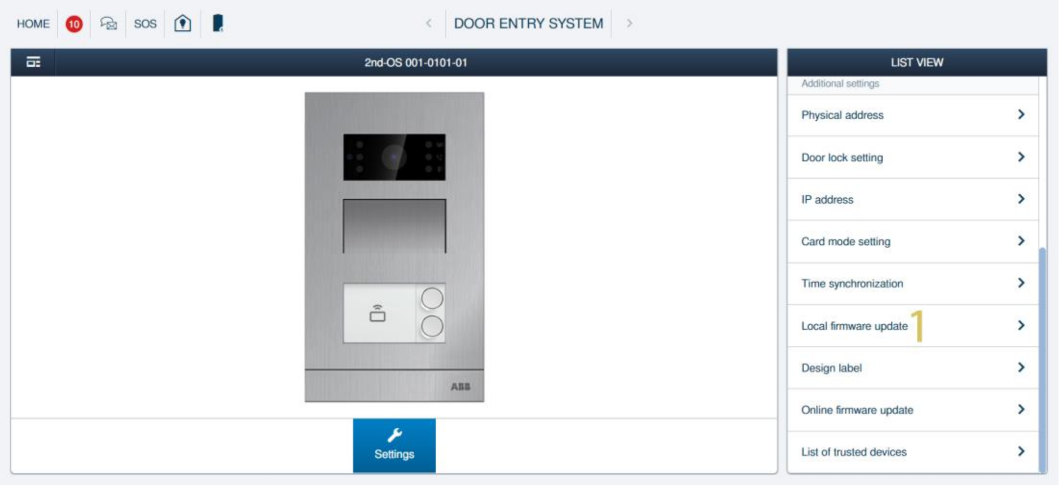
[1] On the designated device screen, click "Local firmware update".

[2] Click "Browser" to select the update file (.img).

[3] Click "Browser" to select the signature file (.sig).

[4] Click "Save".

[5] Click "I agree" to accept the end user license agreement.



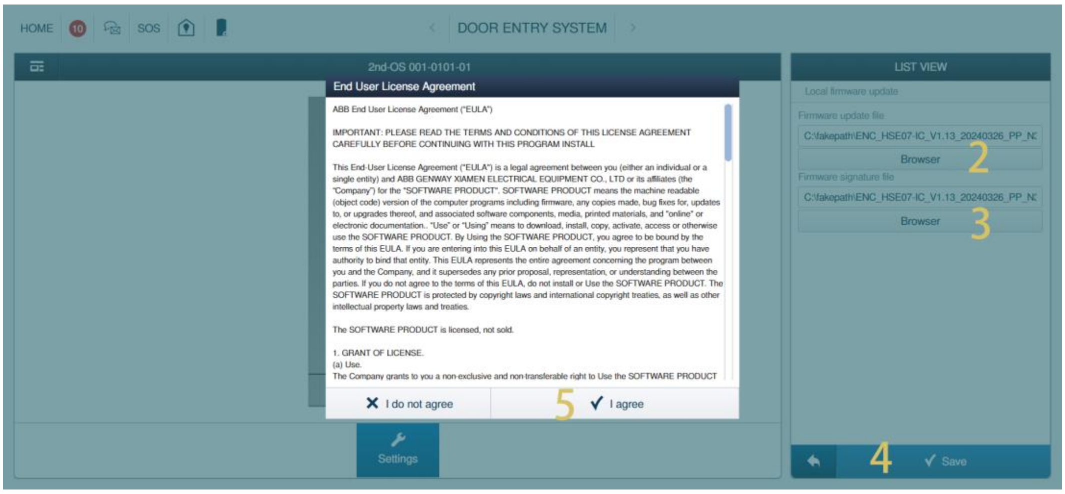


ABB End User License Agreement ("EULA")

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE CONTINUING WITH THIS PROGRAM INSTALL

This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and ABB GENWAY XIAMEN ELECTRICAL EQUIPMENT CO., LTD or its affiliates (the "Company") for the "SOFTWARE PRODUCT". SOFTWARE PRODUCT means the machine readable (object code) version of the computer programs including firmware, any copies made, bug fixes for, updates to, or upgrades thereof, and associated software components, media, printed materials, and "online" or electronic documentation.. "Use" or "Using" means to download, install, copy, activate, access or otherwise use the SOFTWARE PRODUCT. By Using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you are entering into this EULA on behalf of an entity, you represent that you have authority to bind that entity. This EULA represents the entire agreement concerning the program between you and the Company, and it supersedes any prior proposal, representation, or understanding between the parties. If you do not agree to the terms of this EULA, do not install or Use the SOFTWARE PRODUCT. The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties.

The SOFTWARE PRODUCT is licensed, not sold.

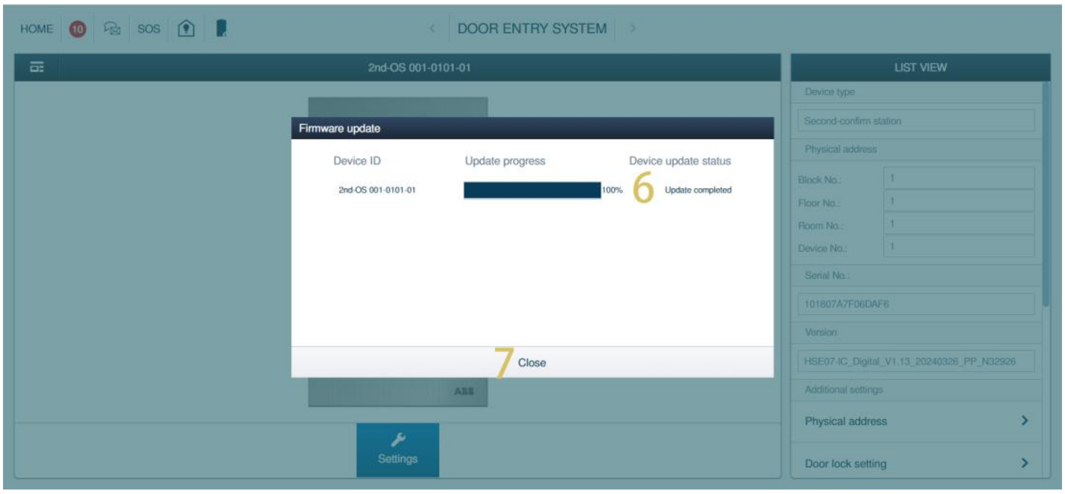
1. GRANT OF LICENSE.
(a) Use.
The Company grants to you a non-exclusive and non-transferable right to Use the SOFTWARE PRODUCT

Firmware update file: C:\fakepath\ENC_HSE07-IC_V1.13_20240326_PP_N

Firmware signature file: C:\fakepath\ENC_HSE07-IC_V1.13_20240326_PP_N

[6] Update status will be displayed.

[7] Click "Close" when the update is completed.



Device ID	Update progress	Device update status
2nd-OS 001-0101-01	100%	Update completed

Device type: Second-confirm station

Physical address

Block No.: 1

Floor No.: 1

Room No.: 1

Device No.: 1

Serial No.: 101807A7F06DAF6

Version: HSE07-IC_Digital_V1.13_20240326_PP_N32926

Additional settings

6.5.3 Updating the firmware of other devices locally in batches

This chapter applies to all devices of Welcome IP system except SmartAP.

The following operations take the OS as an example.

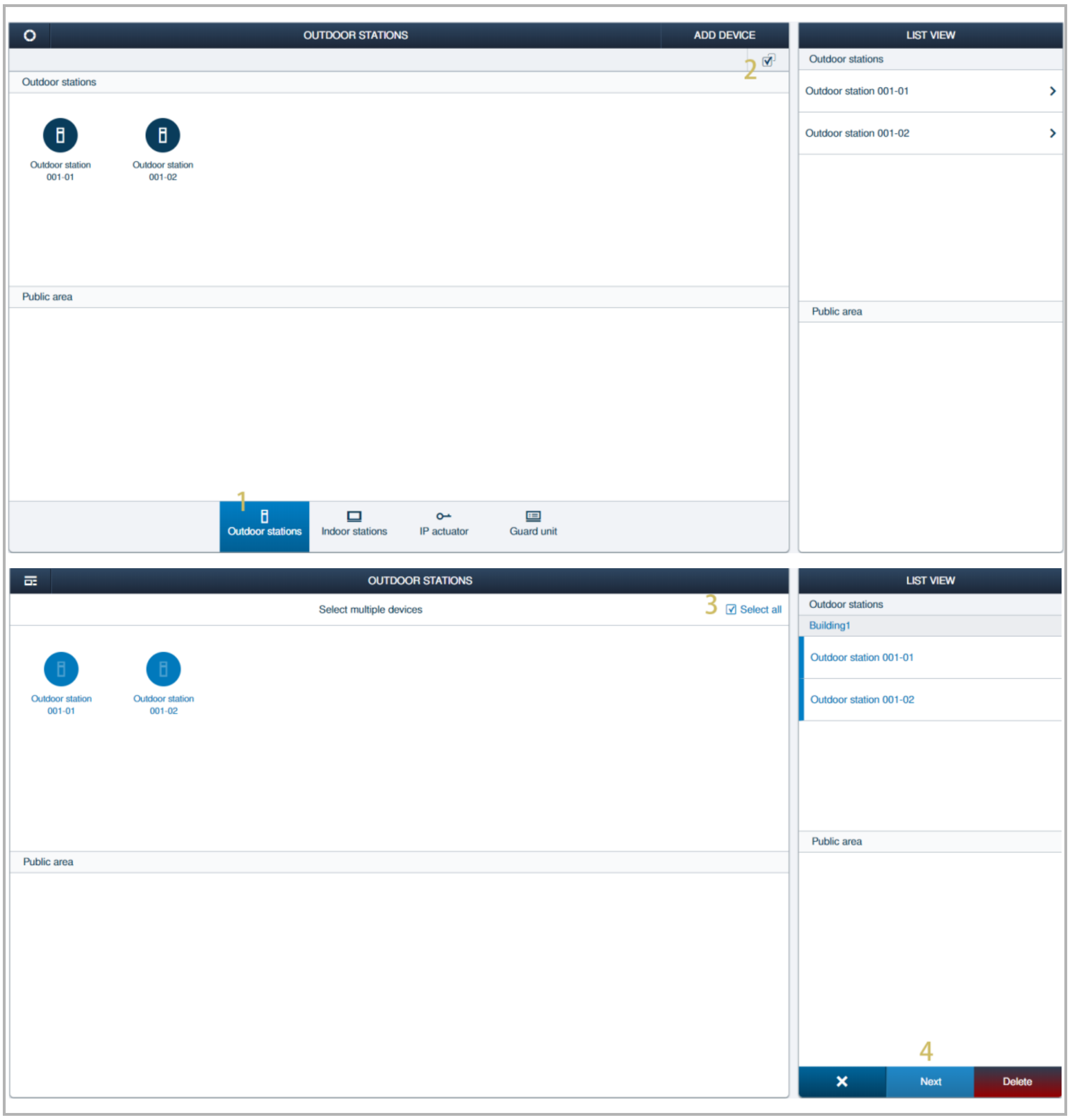
Please follow the steps below:

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

[2] Click " ☑ ".

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

[4] Click "Next".

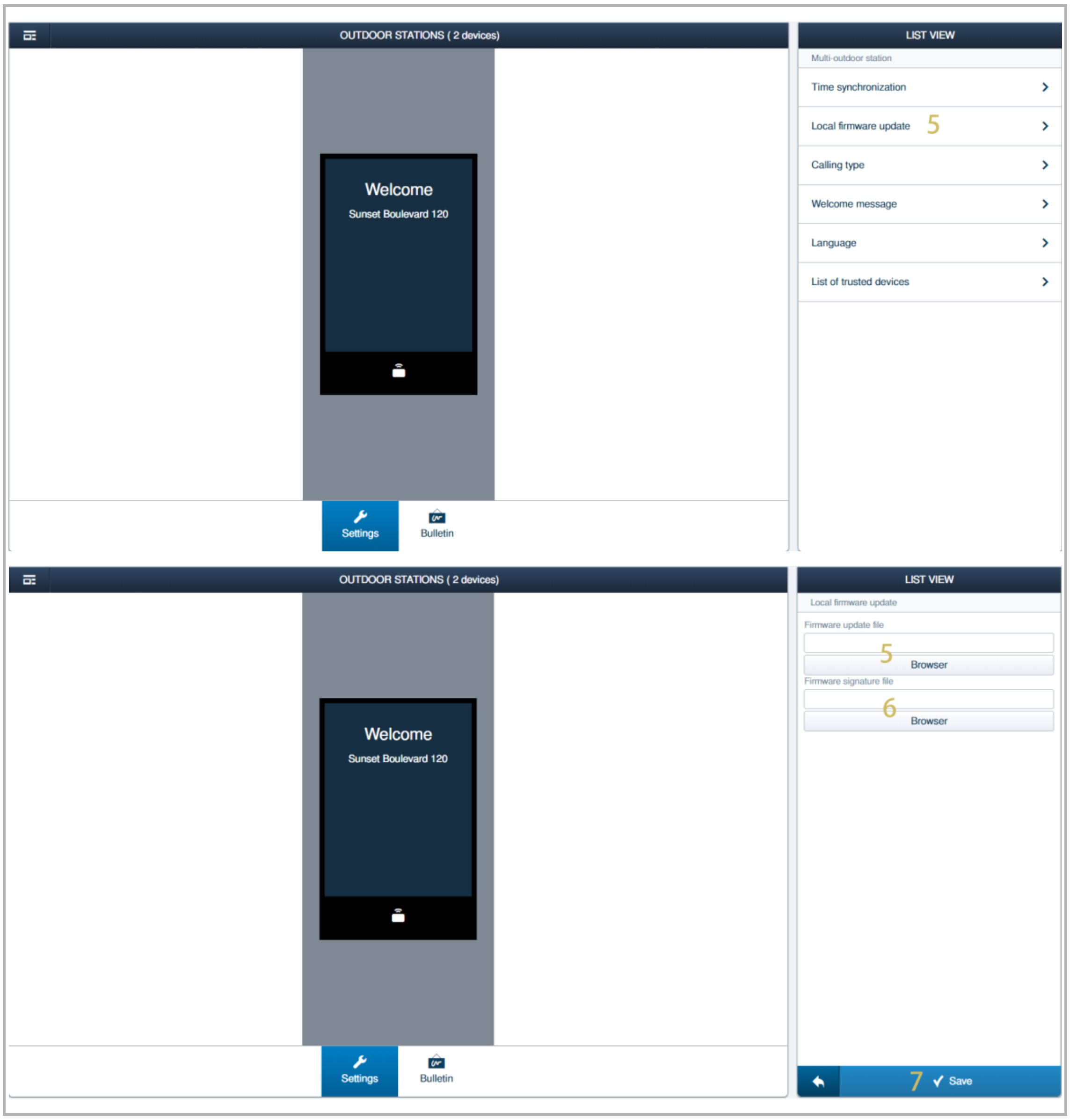


[5] Click "Local firmware update".

[6] Upload the firmware.

[7] Upload the signature.

[8] Click " √ " to save.



7 Smart Home Integration

For more details about KNX settings, please see the “10.1 KNX settings” chapter of IP touch 7 & 10 product manual.

For more details about free@home settings, please see the “10.2 free@home settings” chapter of IP touch 7 & 10 product manual.

You can access IP touch 7 & 10 product manual via the link: https://search.abb.com/library/Download.aspx?DocumentID=2TMD042400D0019&LanguageCode=en&DocumentPartId=&Action=Launch.

8 API

8.1 API overview

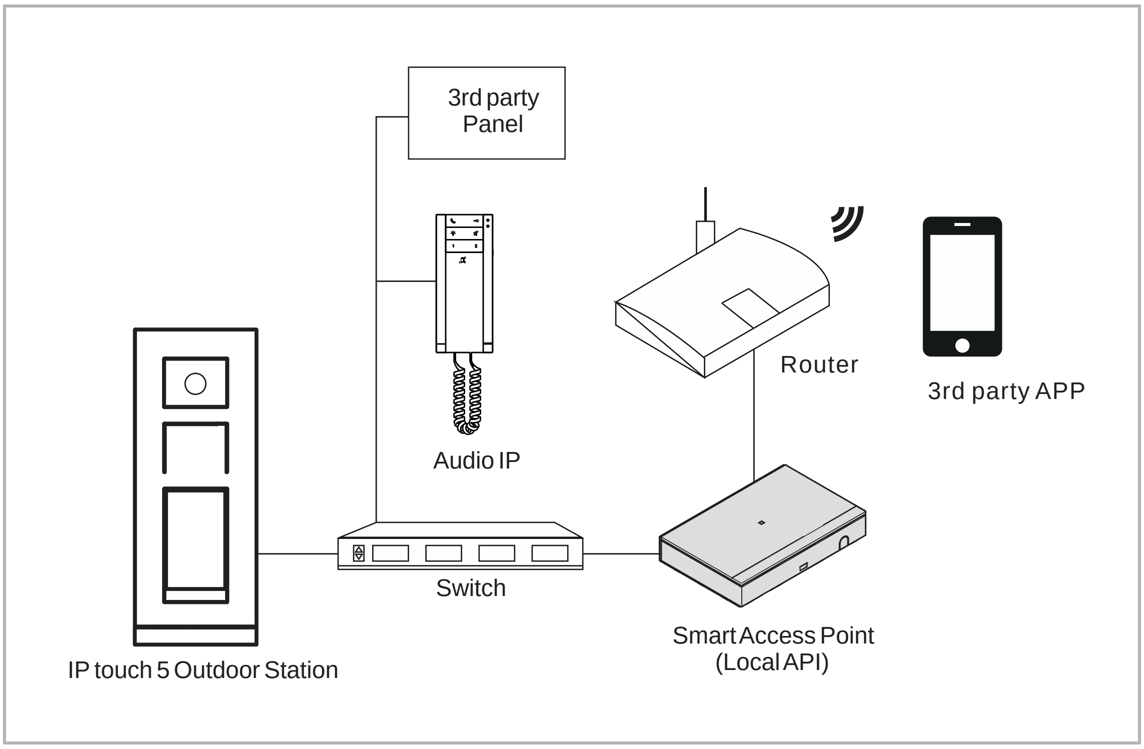
The API provides access to a Welcome IP & AccessControl door entry system, enabling control and monitoring functions.

This API facilitates querying information about the current configuration of the door entry system, including devices and their status. It provides endpoints with the ability to query and modify the current status of devices and receive updates on changes.

Access to the Welcome IP & AccessControl local API is controlled by the user management of the intelligent access point. For this reason, each request must be submitted with valid credentials. The smart access point assigns each user account a generic username that is independent of the account name. The username generated for a specific user account can be found in the Smart Access Point. The credentials are transmitted in accordance with RFC7617 using HTTP Basic Access Authentication.

8.2 Topology

The topology is as follows (example only):



8.3 Precondition

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

8.4 Enabling local API

Please follow the steps below:

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

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

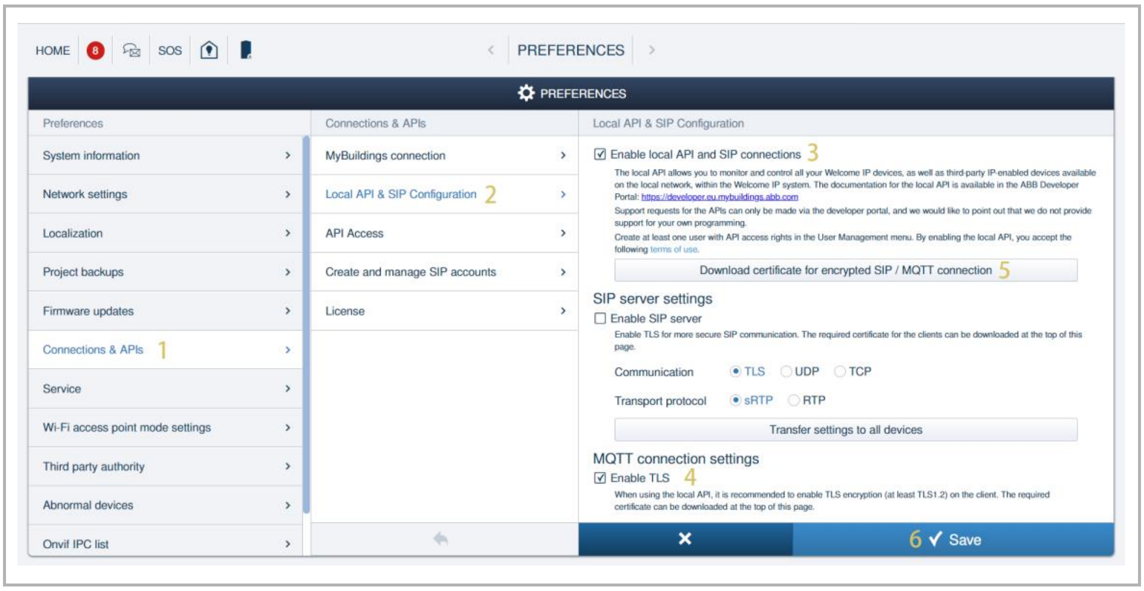
[3] Tick the check box to enable the local API function.

[4] It is recommended to tick the check box to enable TLS encryption.

[5] If "Enable TLS" is activated, please download the certificate for encryption.

[6] Click "Save".

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



☑ Enable local API and SIP connections 3

The local API allows you to monitor and control all your Welcome IP devices, as well as third-party IP-enabled devices available on the local network, within the Welcome IP system. The documentation for the local API is available in the ABB Developer Portal: https://developer.eu.mybuildings.abb.com

Support requests for the APIs can only be made via the developer portal, and we would like to point out that we do not provide support for your own programming.

Create at least one user with API access rights in the User Management menu. By enabling the local API, you accept the following terms of use.

Download certificate for encrypted SIP / MQTT connection 5

SIP server settings

□ Enable SIP server

Enable TLS for more secure SIP communication. The required certificate for the clients can be downloaded at the top of this page.

Communication ● TLS ○ UDP ○ TCP

Transport protocol ● sRTP ○ RTP

Transfer settings to all devices

MQTT connection settings

☑ Enable TLS 4

When using the local API, it is recommended to enable TLS encryption (at least TLS1.2) on the client. The required certificate can be downloaded at the top of this page.

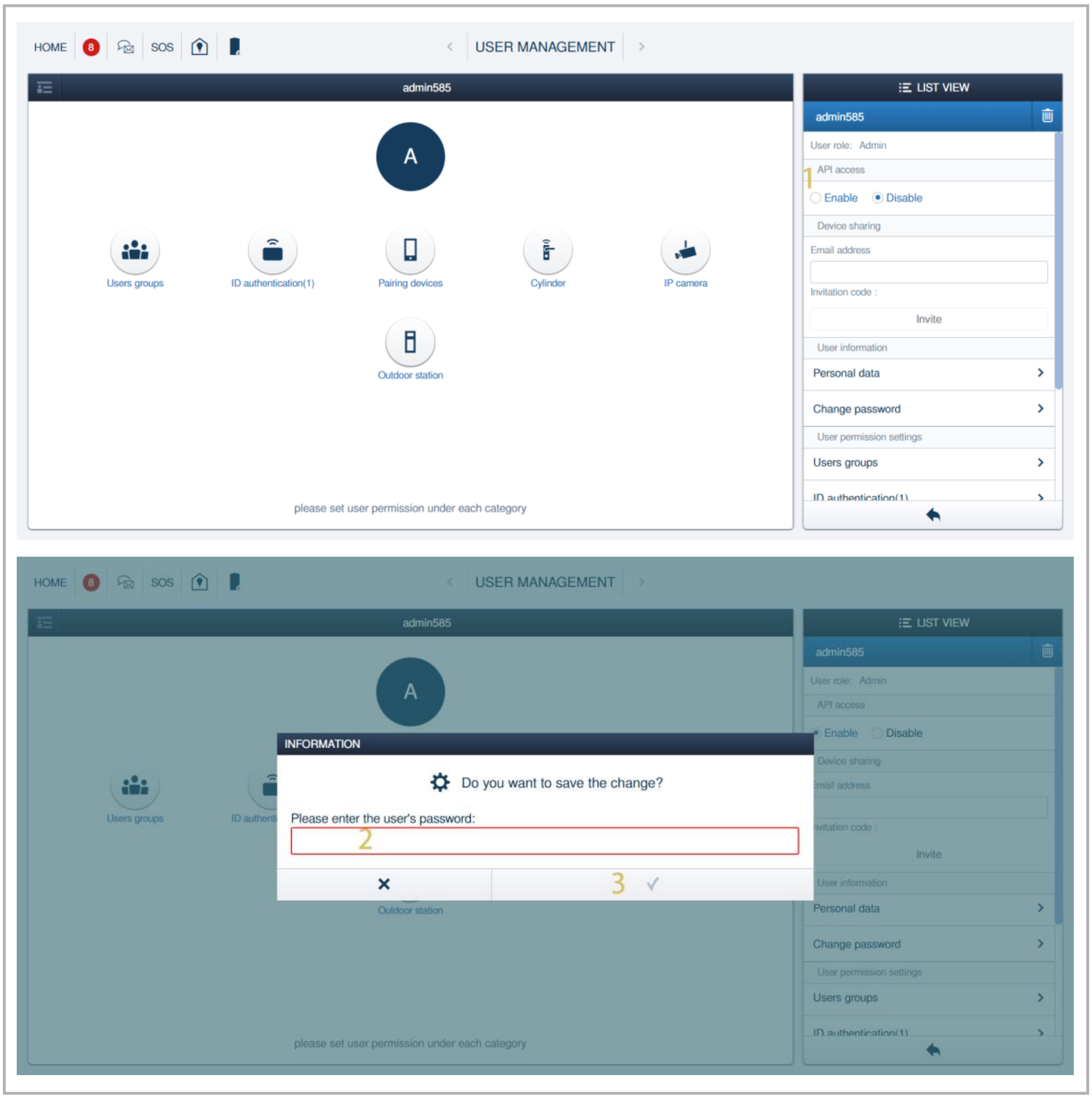
8.5 Creating a local API user

Please follow the steps below:

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

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

[3] Click "√".

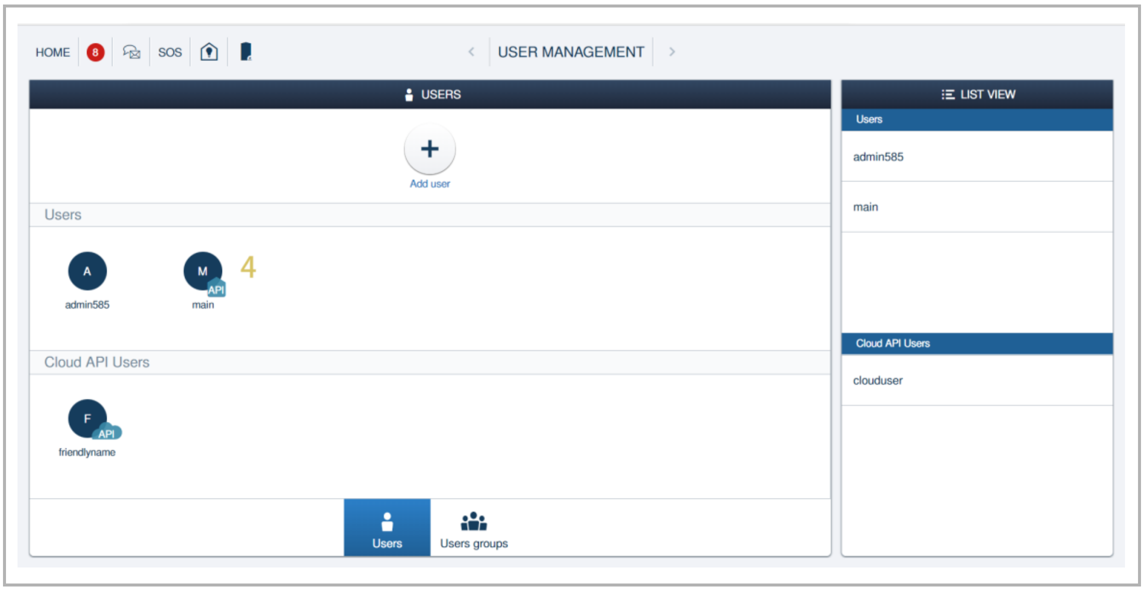


please set user permission under each category

Do you want to save the change?

Please enter the user's password:

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



9 SIP

9.1 SIP overview

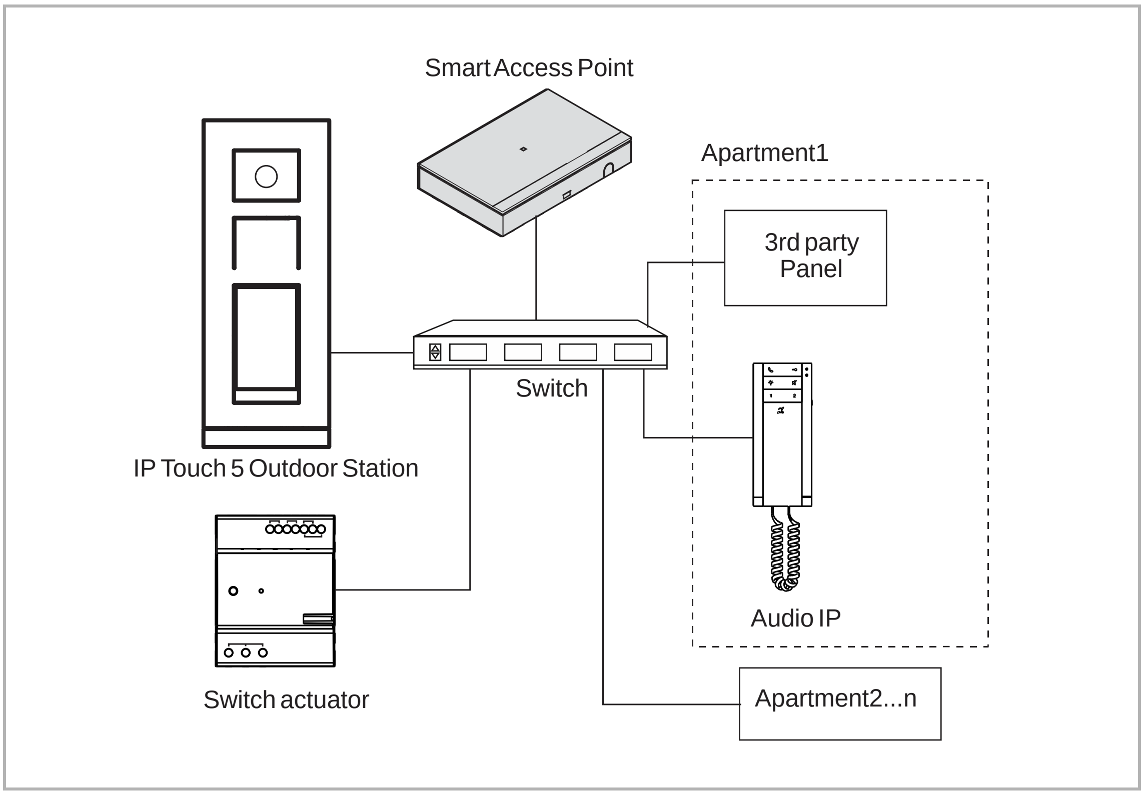
Session Initiation Protocol (SIP) integration refers to the process of implementing SIP technology in communications systems to enable and enhance Voice over Internet Protocol (VoIP) capabilities. SIP is a signalling protocol used to initiate, maintain and terminate real-time sessions, primarily involving video, voice, messaging and other communications services over IP networks.

SIP integration involves setting up SIP servers, gateways and session border controllers, among other components, to manage and route communications between users, devices and the network.

Welcome IP natively supports SIP. This allows organisations and home users to integrate Welcome IP with any third-party telephony application. They can act as either servers or clients within the network.

9.2 Topology

The topology is as follows (just an example):



The above topology supports 2 scenarios.

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

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

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

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

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

[2] Configuring Smart Access Point as SIP server.

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

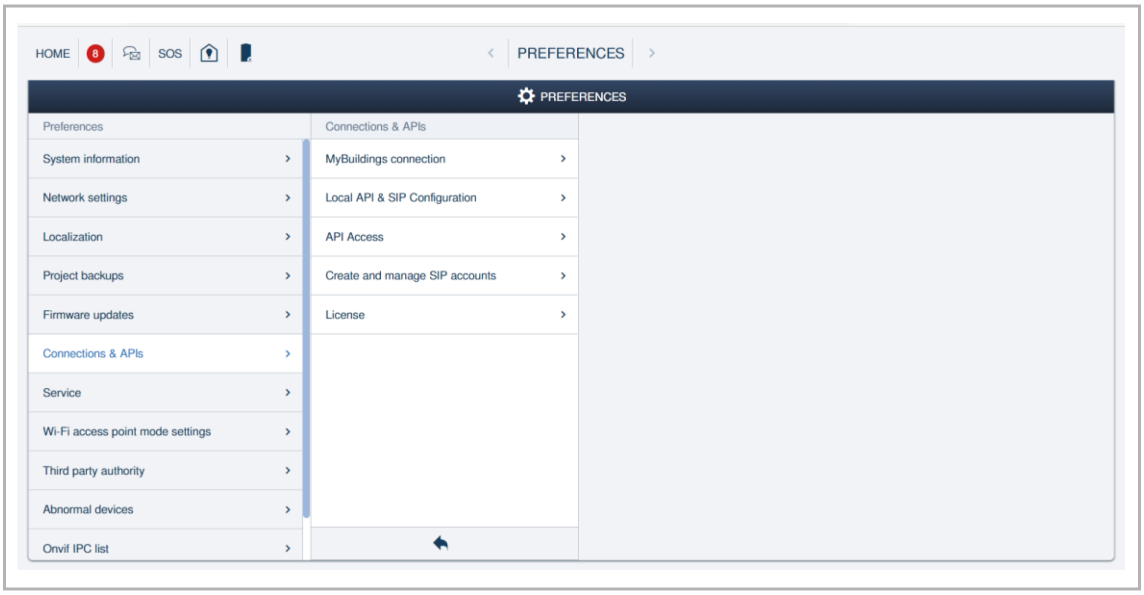
[4] Configuring the 3rd party panel.

[5] Configuring IP touch 5 outdoor station.

[6] Configuring Audio IP.

9.3 Accessing "SIP" screen on the SmartAP

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



9.4 Configuring the SmartAP as SIP server

In scenarios where a smart access point (AP) acts as a SIP server, the device plays multiple roles within the network infrastructure. Essentially, it acts as both a connectivity point for Wi-Fi devices and a central hub for managing SIP-based communications. Here's a brief description of its functions in this dual role:

Connectivity provider: The Smart AP provides wireless network access to connected devices, just like a traditional access point.

SIP Registrar: It registers SIP clients, authenticates devices and users when they log on to the network, and maintains a directory of these clients to facilitate communication.

SIP Proxy and Router: The Smart AP routes SIP calls and messages between registered clients within the network and can also manage traffic between these clients and external SIP networks. This includes call setup, management and teardown.

This setup reduces the need for separate hardware and simplifies the network architecture, making it more cost-effective and easier to manage, while still supporting a wide range of communications protocols and services.

Please follow the steps below:

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

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

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

[4] Select the communication protocol.

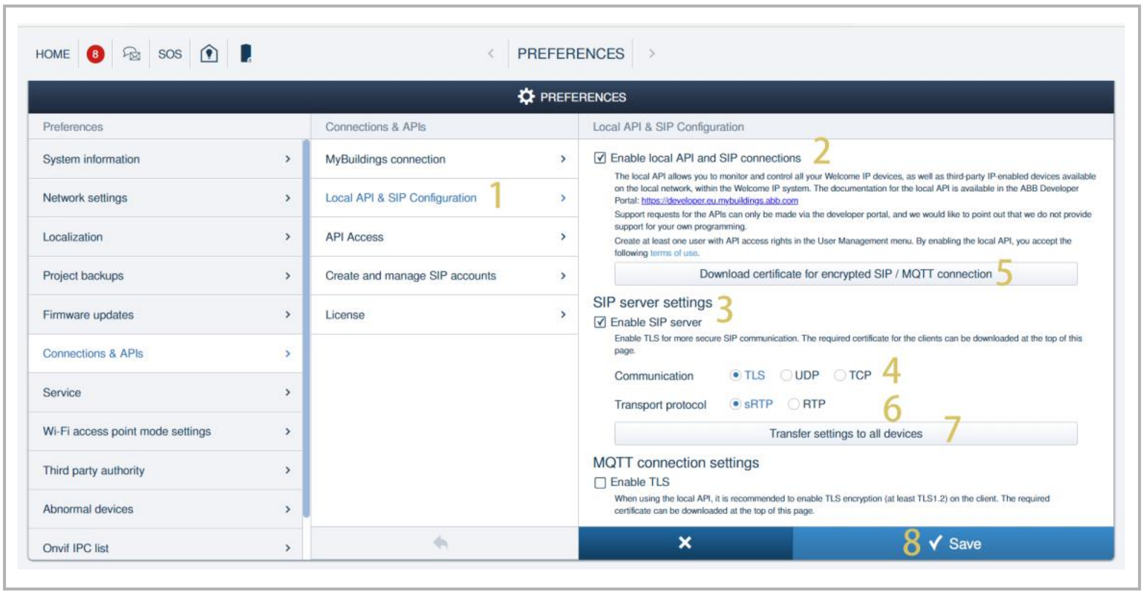
[5] If the communication protocol is set to "TLS", a certificate should be downloaded before use.

[6] Select a transport protocol.

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

It is recommended to carry out this operation when SIP settings are changed or if any devices are not working normally.

[8] Click "Save".



☑ Enable local API and SIP connections

The local API allows you to monitor and control all your Welcome IP devices, as well as third-party IP-enabled devices available on the local network, within the Welcome IP system. The documentation for the local API is available in the ABB Developer Portal: https://developer.eu.mybuildings.abb.com

Support requests for the APIs can only be made via the developer portal, and we would like to point out that we do not provide support for your own programming.

Create at least one user with API access rights in the User Management menu. By enabling the local API, you accept the following terms of use.

SIP server settings

☑ Enable SIP server

Enable TLS for more secure SIP communication. The required certificate for the clients can be downloaded at the top of this page.

Communication ● TLS ○ UDP ○ TCP

Transport protocol ● sRTP ○ RTP

MQTT connection settings

□ Enable TLS

When using the local API, it is recommended to enable TLS encryption (at least TLS1.2) on the client. The required certificate can be downloaded at the top of this page.

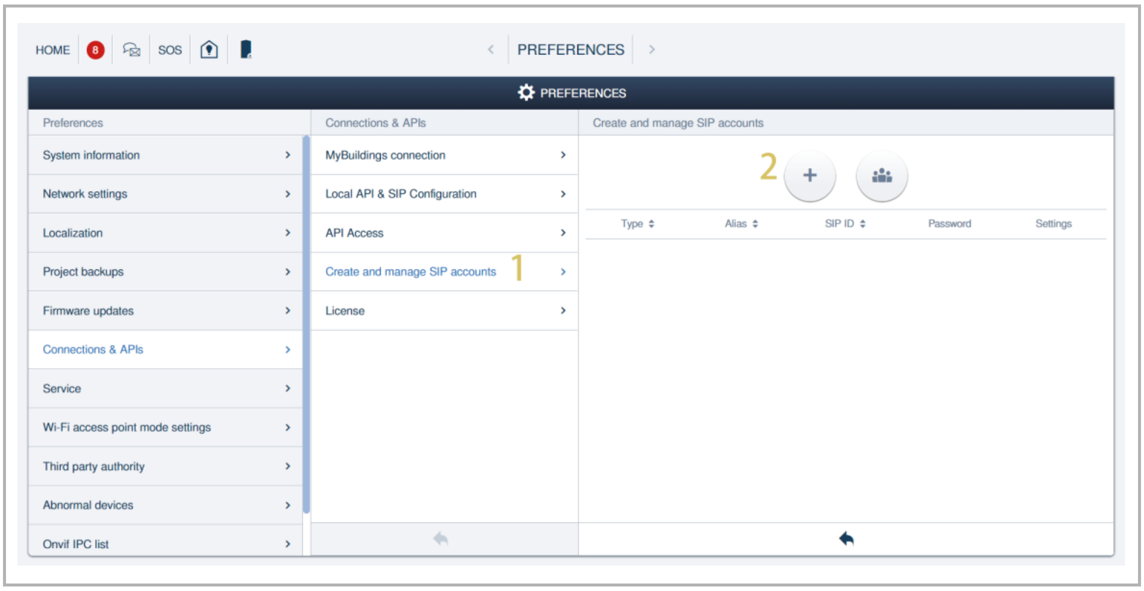
9.5 Creating a SIP account for each 3rd party panel

1. Create the SIP accounts one by one

Please follow the steps below:

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

[2] Click "+".



[3] The 3rd party panel will be set to "Indoor station" automatically and cannot be modified.

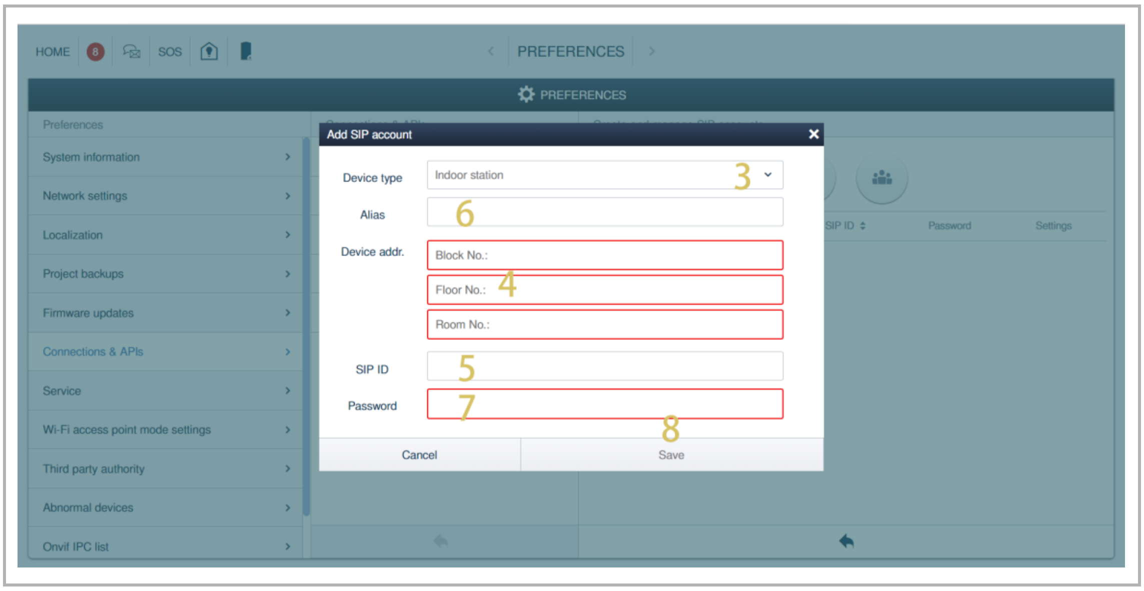
[4] Enter the device address (contains block no., floor no. and room no.).

[5] The ID will be generated automatically according to the rule and cannot be modified.

[6] The alias will be generated automatically according to the rule and can be modified.

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

[8] Click "Save".



Add SIP account

Device type: Indoor station

Alias

Device addr.: Block No.: / Floor No.: / Room No.:

SIP ID

Password

2. Creating SIP accounts in batches

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

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

Please follow the steps below:

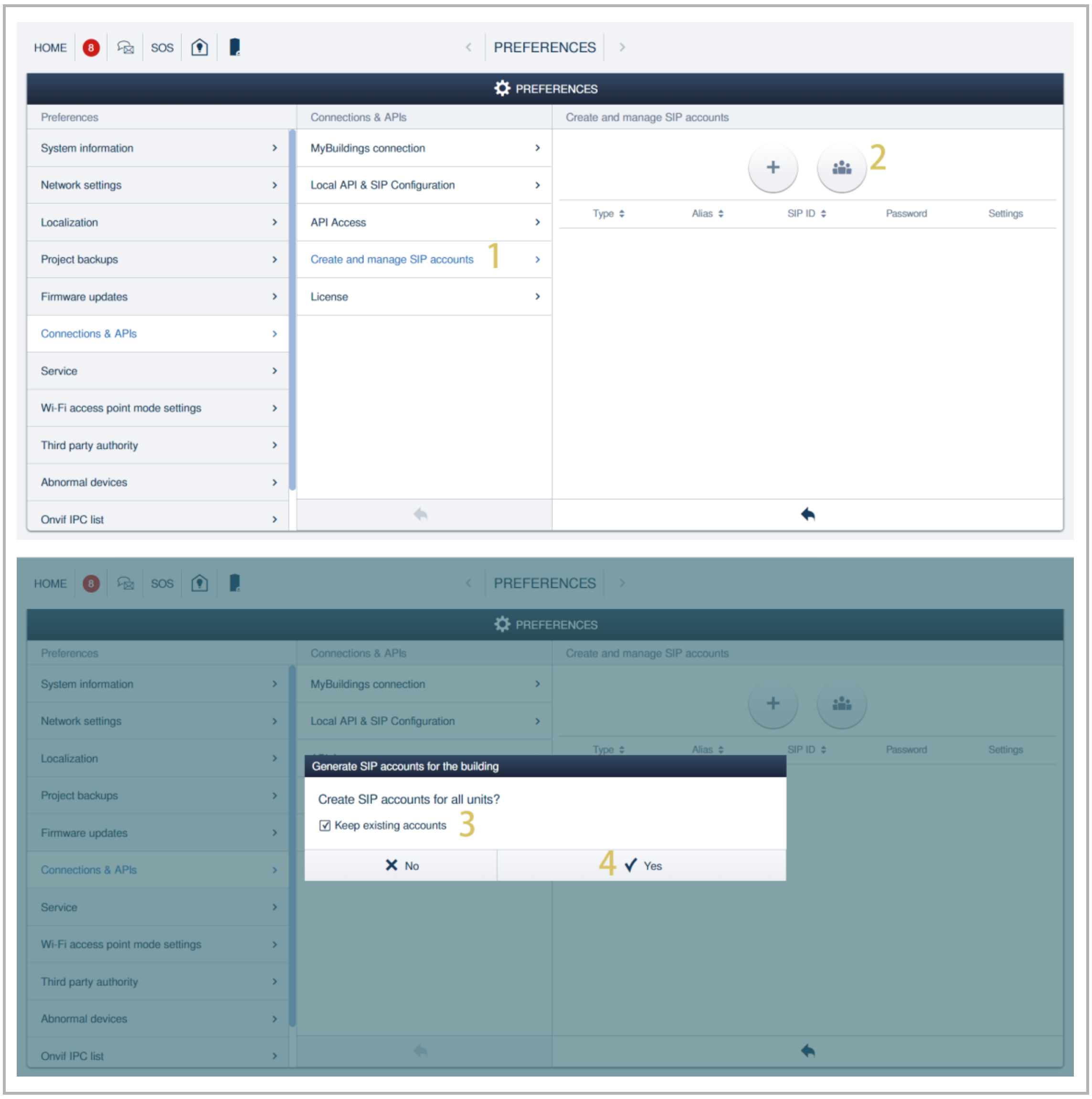
[1] On the "Connections & APIs" screen, click "Create and manage SIP accounts".

[2] Click " 👥 ".

[3] If the existing account needs to be kept, tick the checkbox, otherwise all existing accounts will be cleared and new accounts will be created.

[4] Click "Yes".

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



Generate SIP accounts for the building

Create SIP accounts for all units?

☑ Keep existing accounts

✕ No ✓ Yes

9.6 Configuring the 3rd party panel

(The addresses are given as an example only, please check the values with your real installation)

Please follow the steps below:

[1] Enter the SIP account.

[2] Enter the SIP password.

[3] Enter the server address 10.0.0.1.

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

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

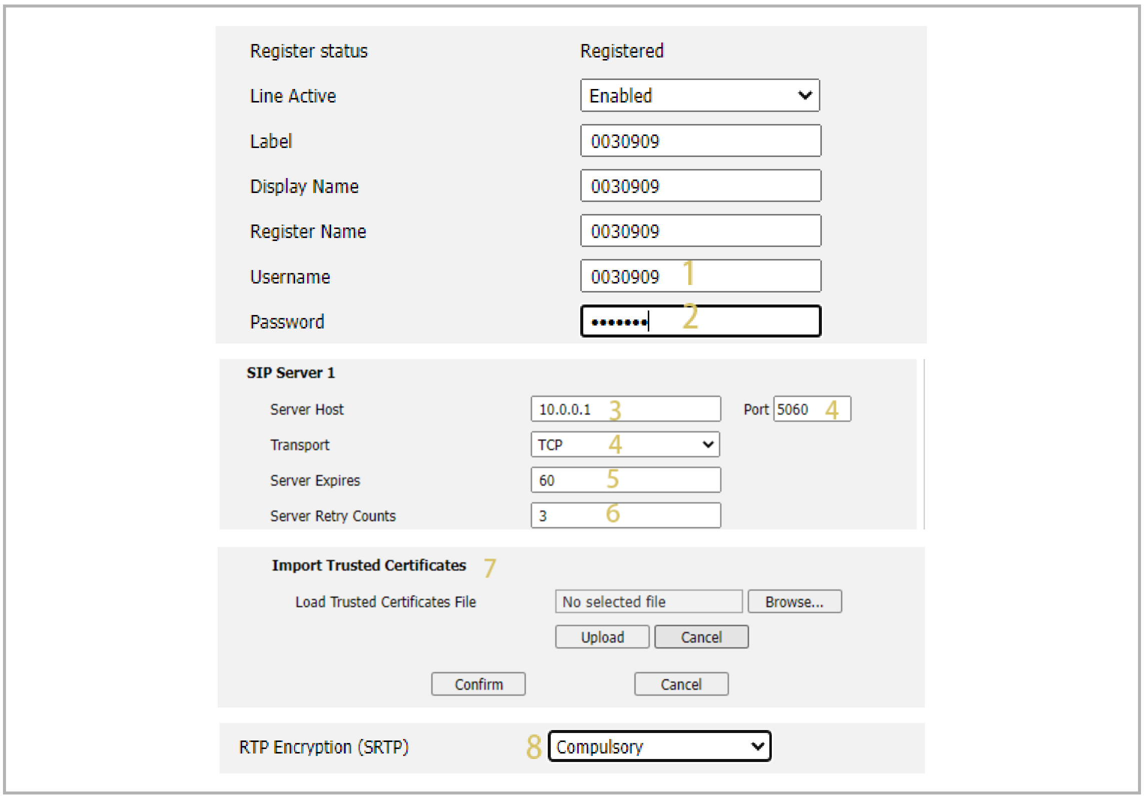
[5] Enter the server expire time (60...120 seconds).

[6] Enter the server retry counts.

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

[8] Set the media stream transport protocol.

- Compulsory = SRTP
- Disabled = RTP



Register status	Registered
Line Active	Enabled
Label	0030909
Display Name	0030909
Register Name	0030909
Username	0030909
Password	•••••••

SIP Server 1

Server Host	10.0.0.1	Port 5060
Transport	TCP	
Server Expires	60	
Server Retry Counts	3	

Import Trusted Certificates

Load Trusted Certificates File: No selected file

RTP Encryption (SRTP): Compulsory

9.7 Configuring IP touch 5 OS

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

9.7.1 SIP client settings

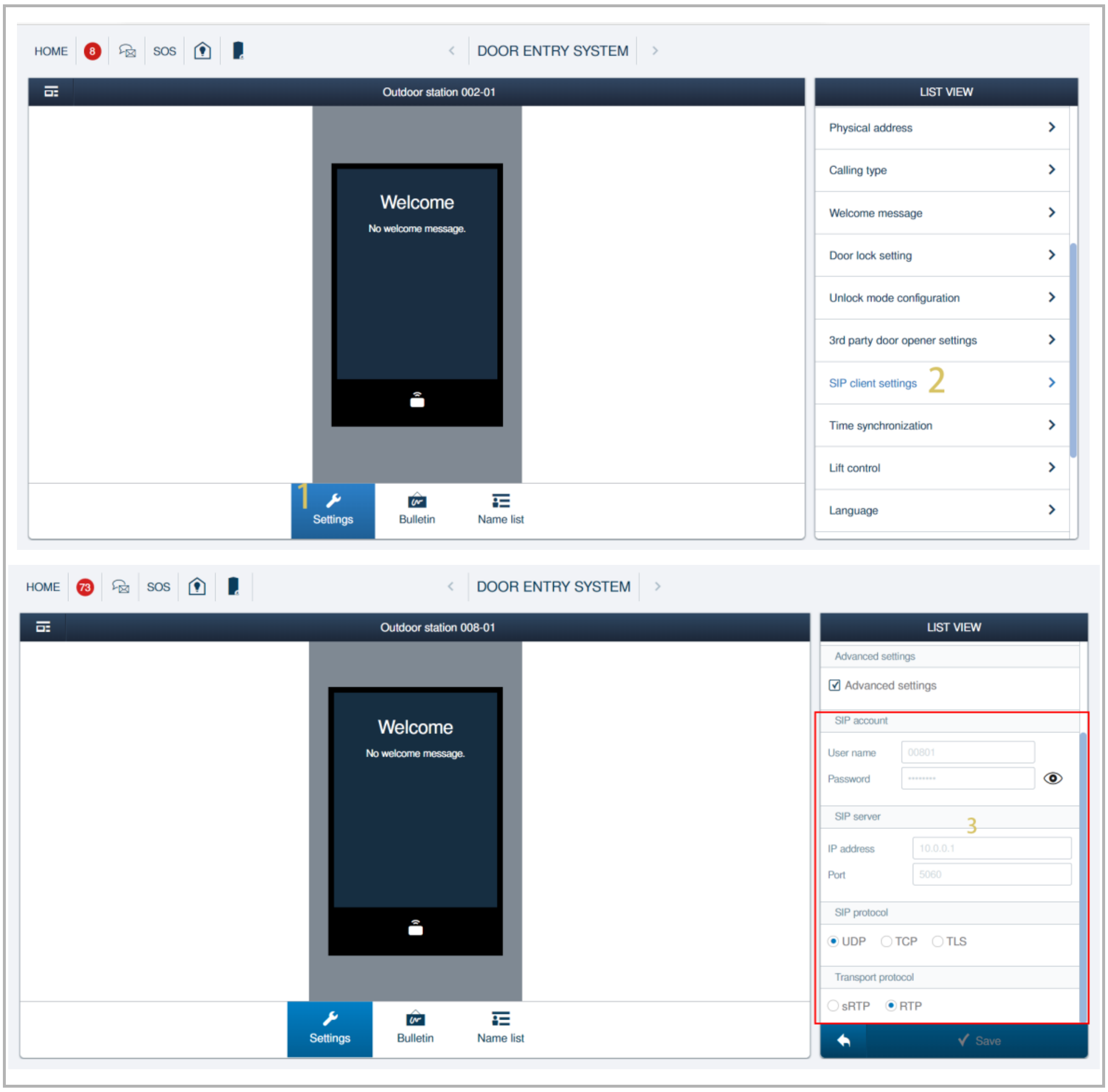
Please follow the steps below:

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

[2] Click "SIP client settings".

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

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



Advanced settings

☑ Advanced settings

SIP account

User name: 00801

Password: ·········

SIP server

IP address: 10.0.0.1

Port: 5060

SIP protocol

● UDP ○ TCP ○ TLS

Transport protocol

○ sRTP ● RTP

9.7.2 3rd party door opener settings

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

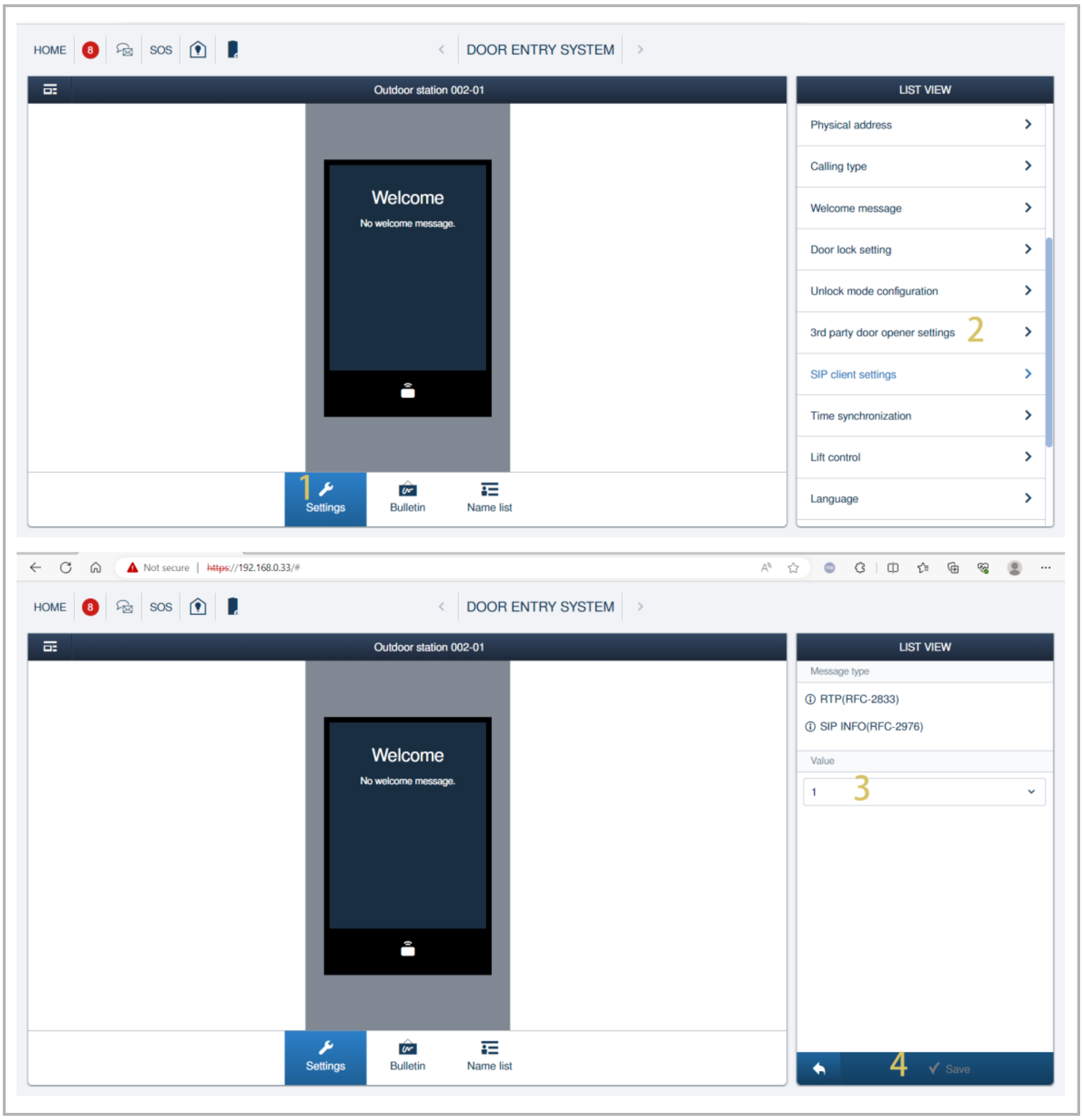
Please follow the steps below:

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

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

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

[4] Click "Save".



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

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

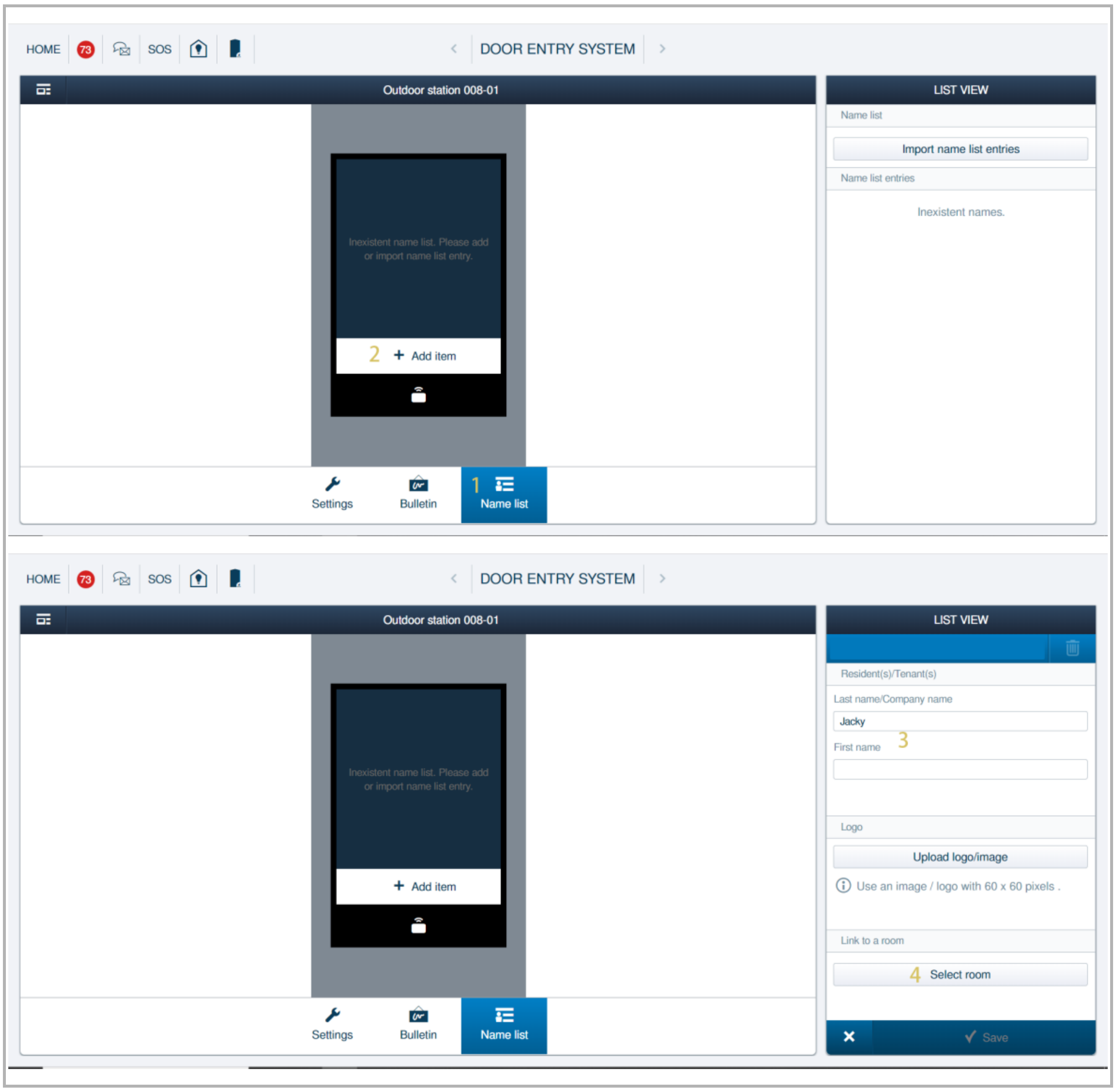
Please follow the steps to add the 3rd party panel to the name list:

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

[2] Click "+ Add item".

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

[4] Click "Select room".



Inexistent name list. Please add or import name list entry.

Inexistent names.

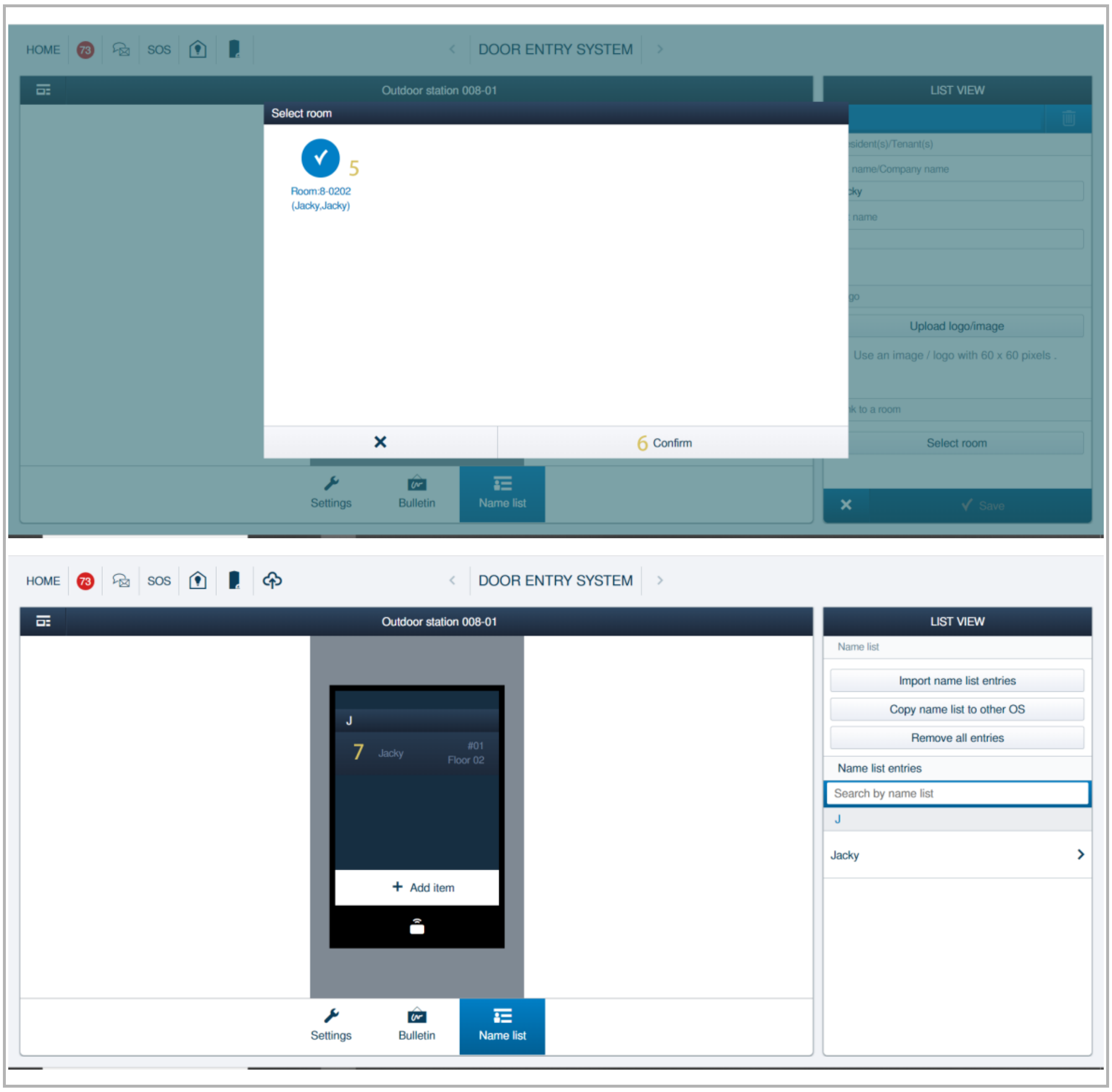
Last name/Company name: Jacky

Use an image / logo with 60 x 60 pixels .

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

[6] Click "Confirm".

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



9.7.4 Adding the 3rd party panels to the name list in batches

If there are multiple 3rd party panels that need to be added to the name list, it is recommended to use the import function.

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

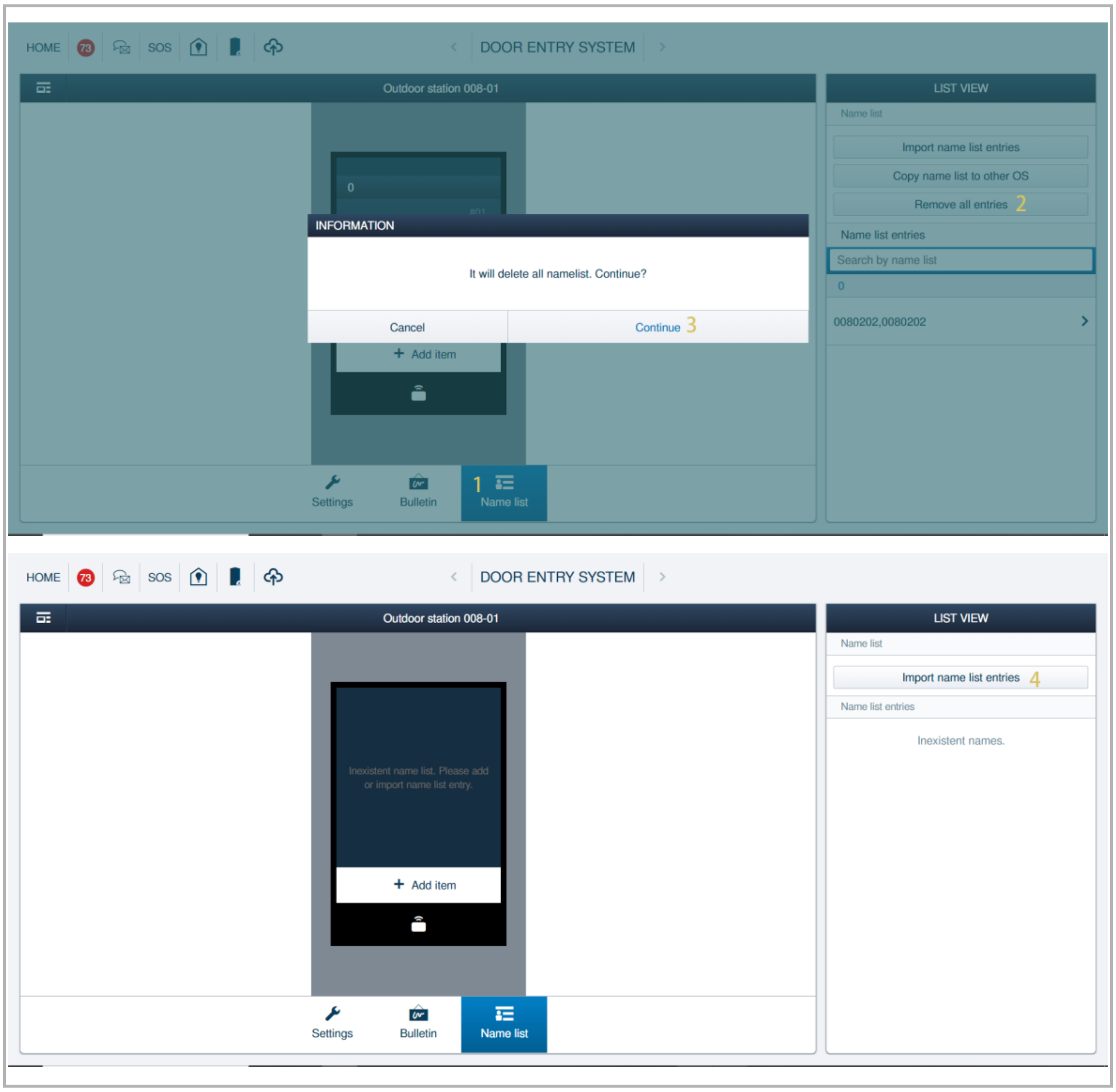
It is recommended to remove all entries before importing.

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

[2] Click "Remove all entries".

[3] Click "Continue".

[4] Click "Import name list entries".



INFORMATION

It will delete all namelist. Continue?

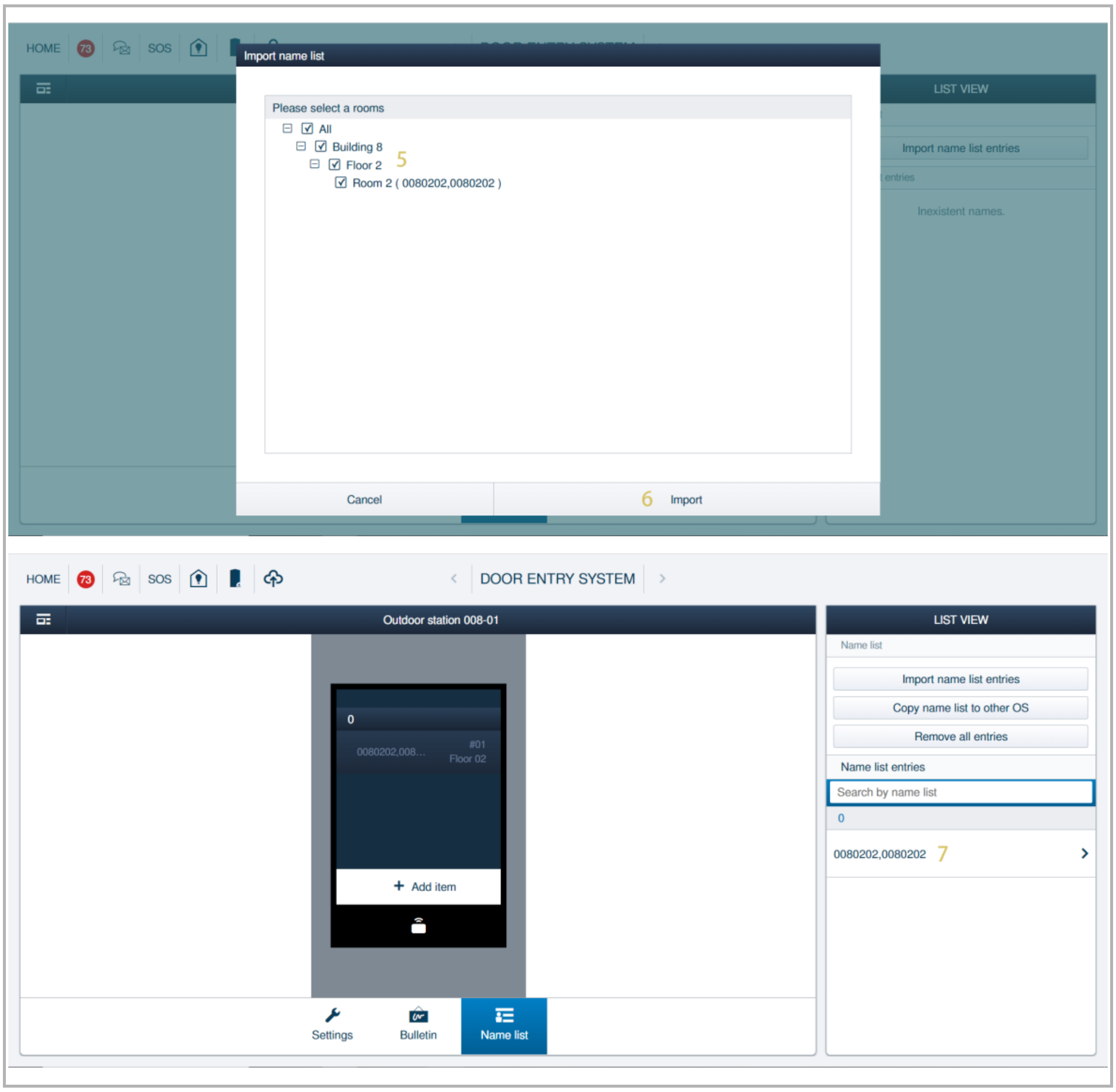
Inexistent name list. Please add or import name list entry.

Inexistent names.

[5] Select the designated rooms.

[6] Click "Import".

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



9.8 Configuring Audio IP

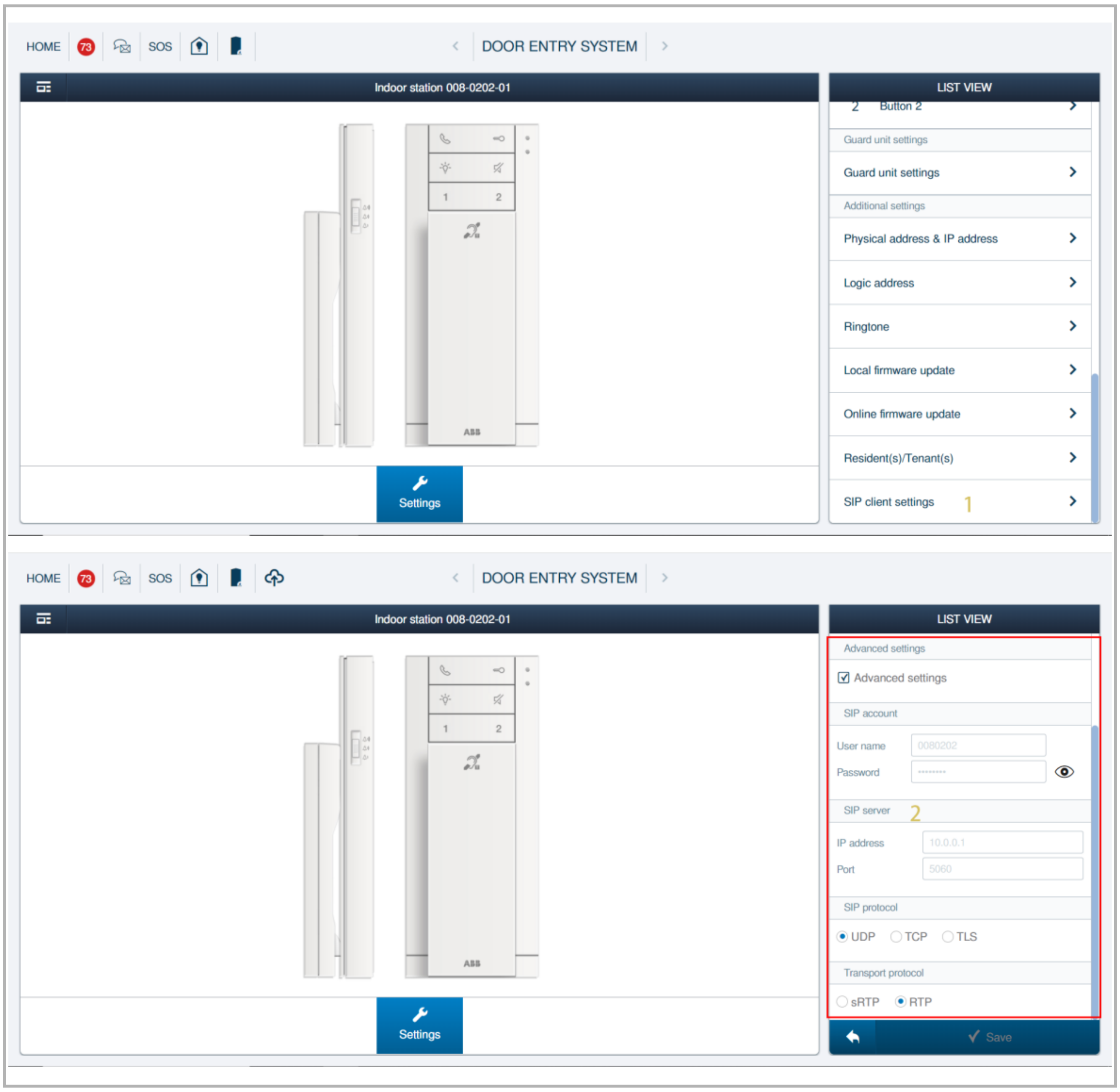
Audio IP needs to be configured before using the SIP function.

Please follow the steps below:

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

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

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



☑ Advanced settings

SIP account

User name: 0080202

Password: ********

SIP server

IP address: 10.0.0.1

Port: 5060

SIP protocol

● UDP ○ TCP ○ TLS

Transport protocol

○ sRTP ● RTP

10 Appendix

10.1 Initial setup of the SmartAP

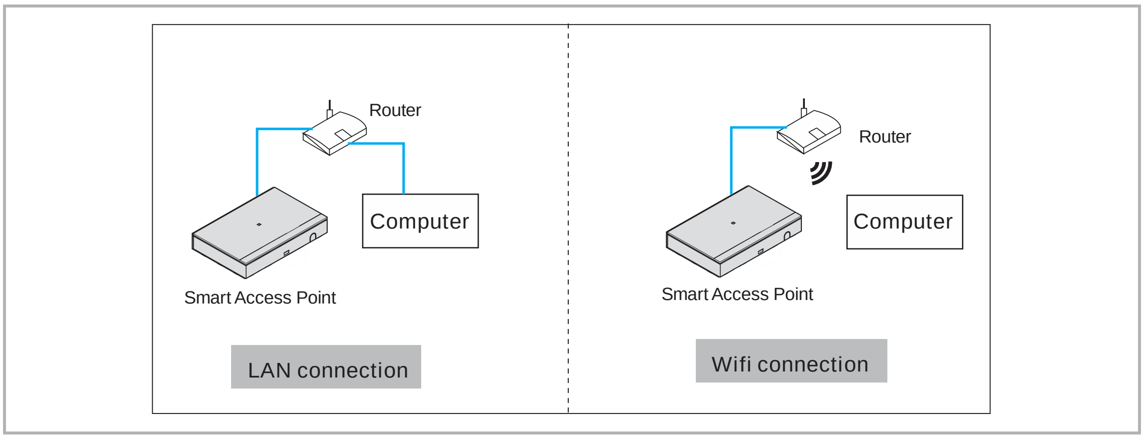
10.1.1 Accessing the web-based user interface

There are 3 options to access the web-based user interface of the SmartAP.

1. By using the Windows UPnP service

Precondition

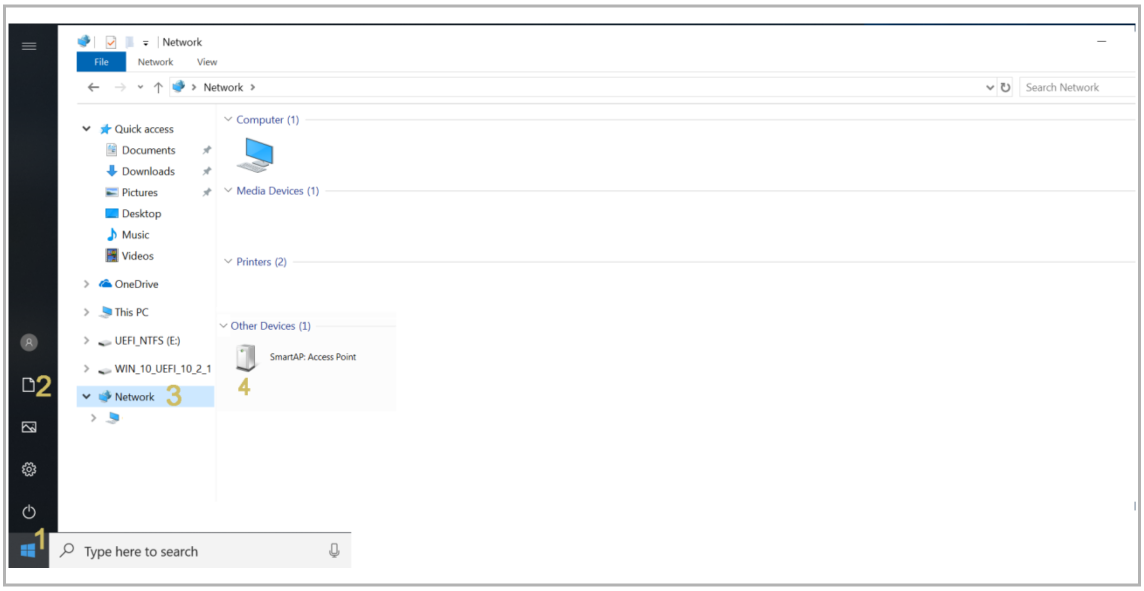
- There is a DHCP server on the network, e.g. integrated DHCP is used in the router.
- The SmartAP is connected to the router by a LAN cable.
- The computer is connected to the router by LAN connection or WiFi connection.
- The SmartAP is powered on and ready for operation.



Accessing SmartAP (Window 10 system as an example)

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

[2] Double click the SmartAP icon.

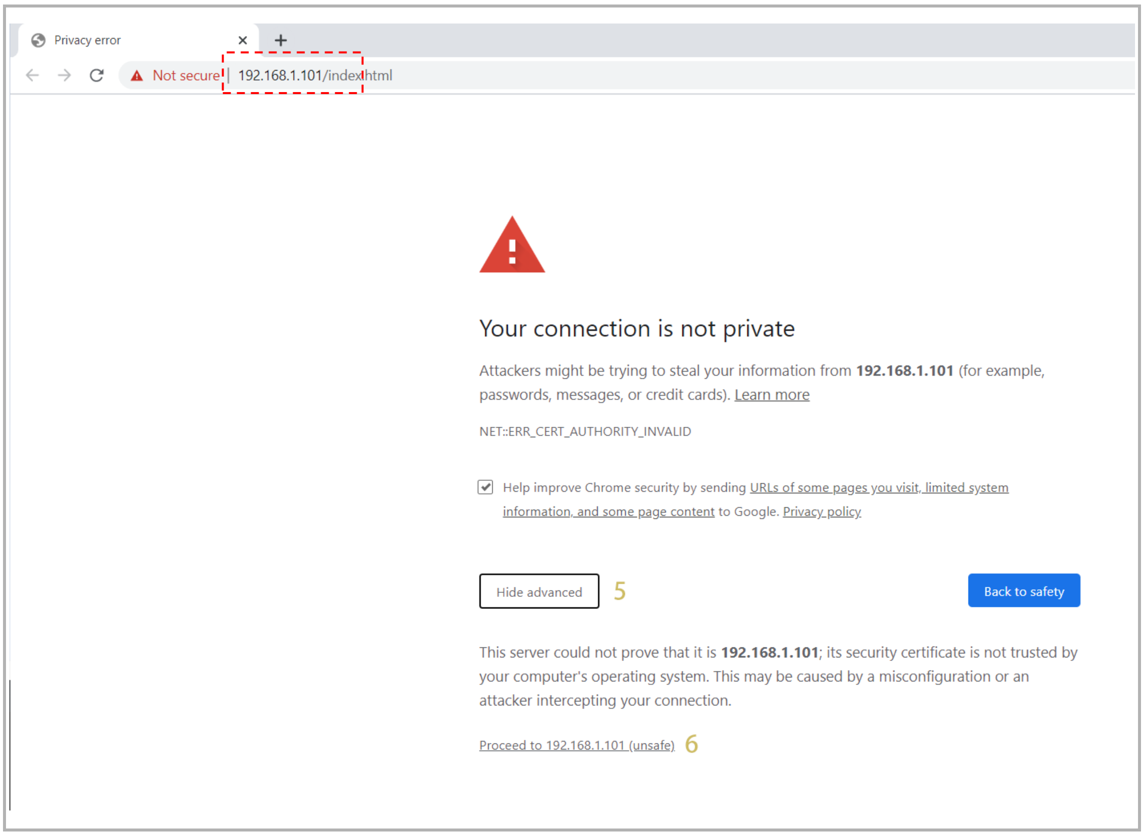


Note

If the SmartAP icon is not displayed, please check the Windows firewall or ask for help from your IT engineers.

[3] Switch to Security Login

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



Your connection is not private

Attackers might be trying to steal your information from **192.168.1.101** (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

This server could not prove that it is **192.168.1.101**; 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.

2. By entering the IP address

Precondition

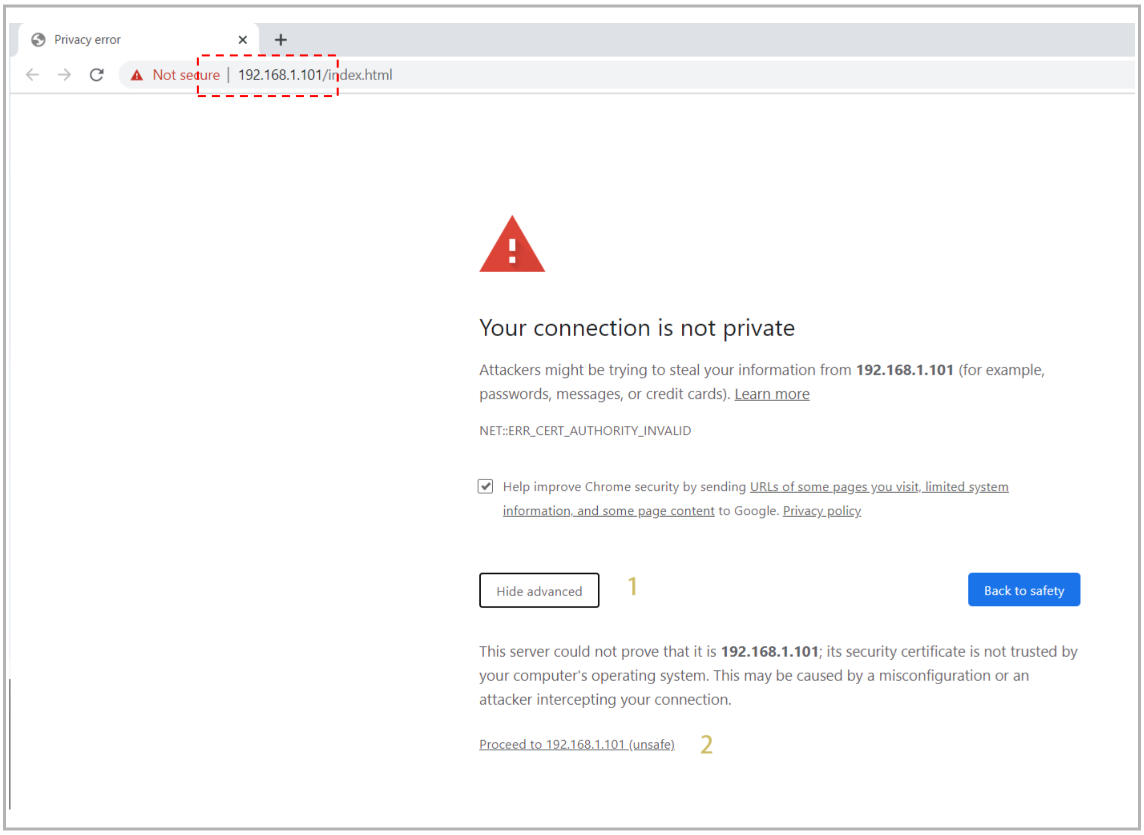
You can check the IP address of SmartAP on the router configuration website. Each router usually has its own management web interface where you can obtain the information. Please check your router’s handbook.

Accessing SmartAP (Window 10 system as an example)

[1] Enter the IP address of SmartAP (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 SmartAP. (Google Chrome, for example)



Your connection is not private

Attackers might be trying to steal your information from **192.168.1.101** (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

This server could not prove that it is **192.168.1.101**; 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.

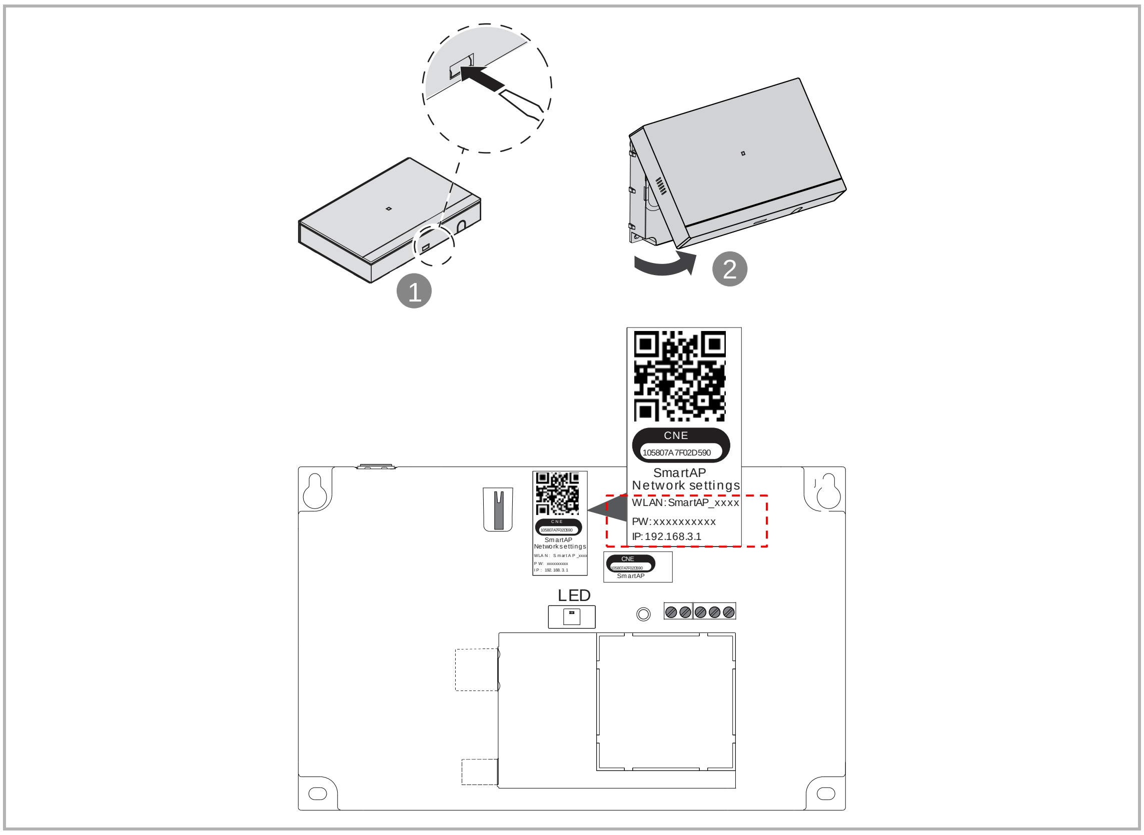
Proceed to 192.168.1.101 (unsafe)

3. By using the WiFi Access Point hotspot

Precondition

- Ensure network settings are obtained from the SmartAP
  - WLAN name (SSID)
  - Password
  - IP address

Please open the front shell of SmartAP 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)

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

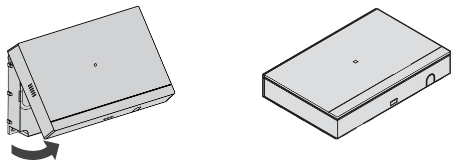
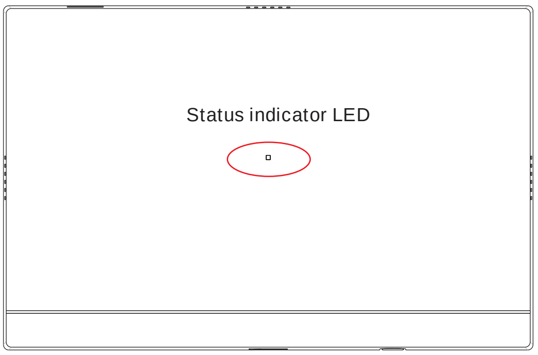


Figure A   Figure B

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



Note

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

Accessing SmartAP (Window 10 system as an example)

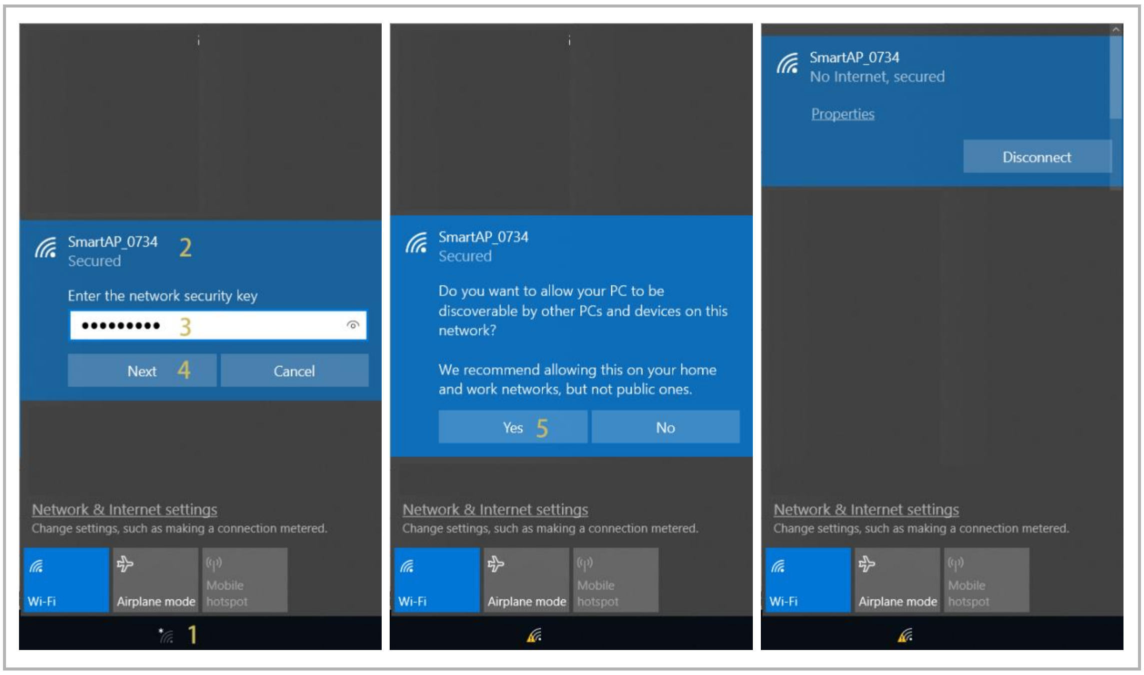
[1] Click "Internet access" icon.

[2] Click the WLAN name (SSID) of SmartAP.

[3] Enter the password.

[4] Click "Next".

[5] Click "Yes" to connect your computer to the WiFi hotspot of SmartAP.



SmartAP_0734
Secured

Enter the network security key

●●●●●●●●●

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.

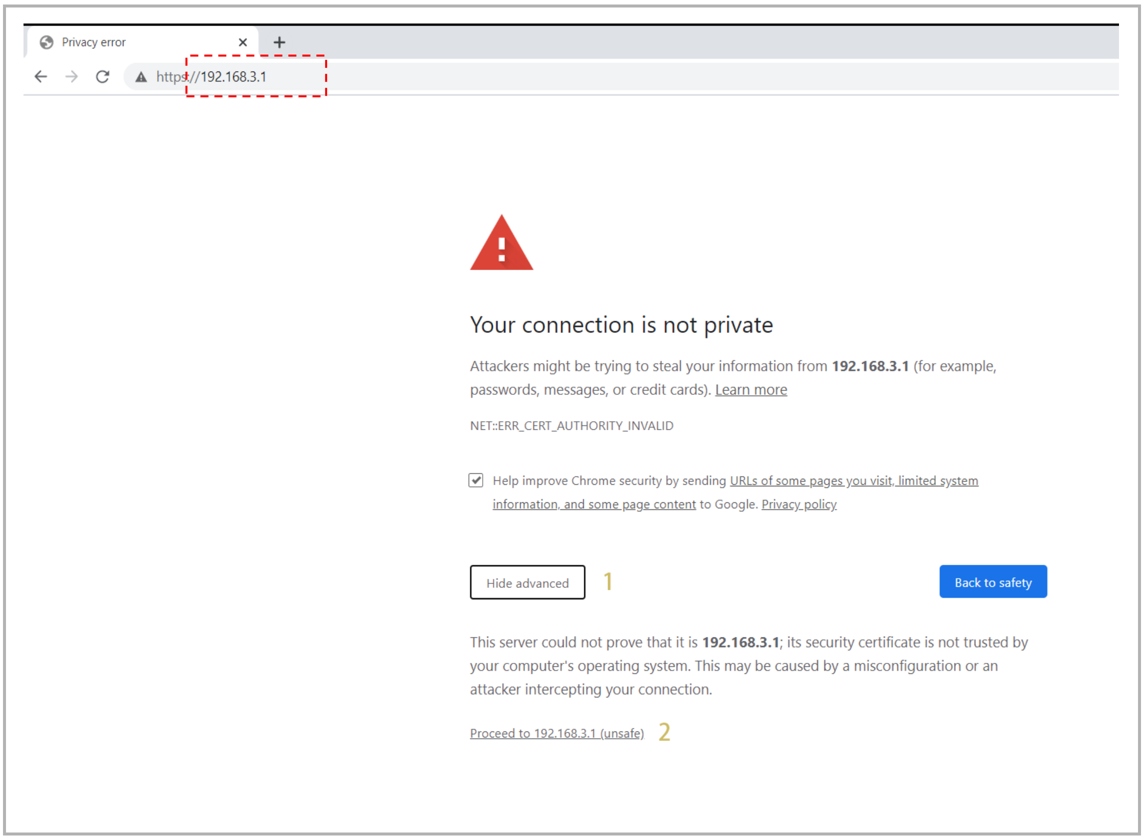
SmartAP_0734
No Internet, secured

Network & Internet settings
Change settings, such as making a connection metered.

[6] Enter "192.168.3.1" on the website to access SmartAP.

[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 SmartAP. (Google Chrome, for example)



Your connection is not private

Attackers might be trying to steal your information from **192.168.3.1** (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

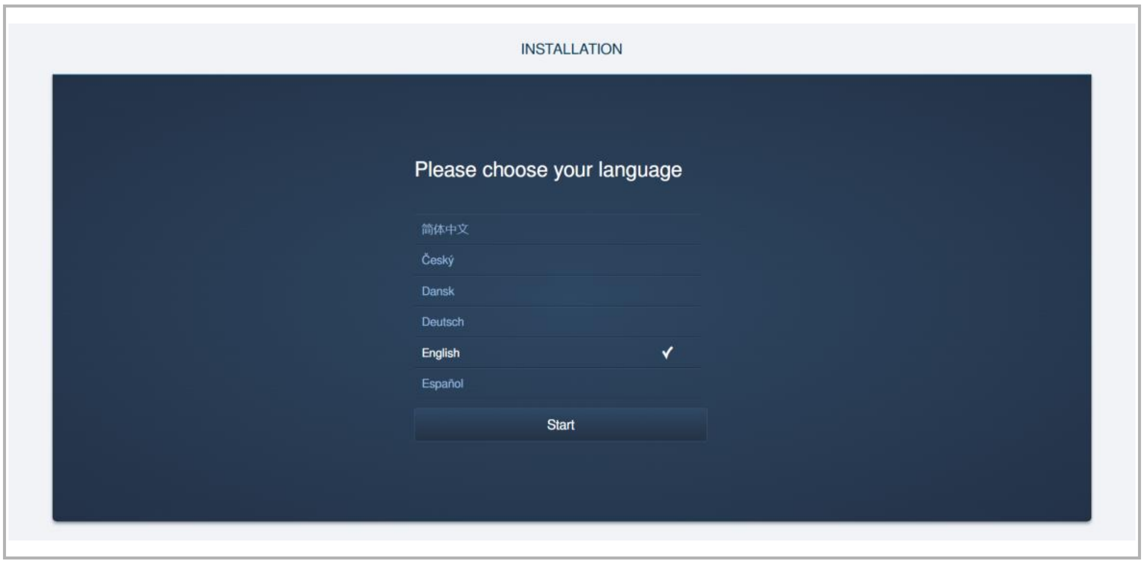
This server could not prove that it is **192.168.3.1**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

10.1.2 Initial setup

You need to do the initial setup the first time the SmartAP is powered on or the SmartAP is reset to the factory defaults.

Follow the steps below on the web-based user interface of the SmartAP.

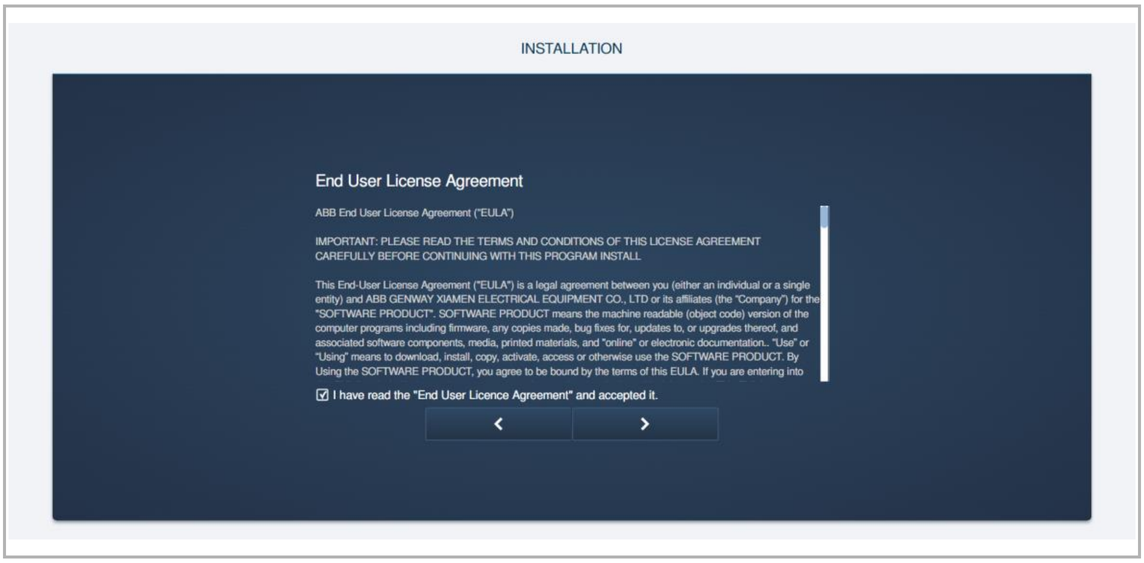
1. Select the language



Please choose your language

2. Accepting EULA

Tick the checkbox to accept the licence. Then click ">" to continue.



End User License Agreement

ABB End User License Agreement ("EULA")

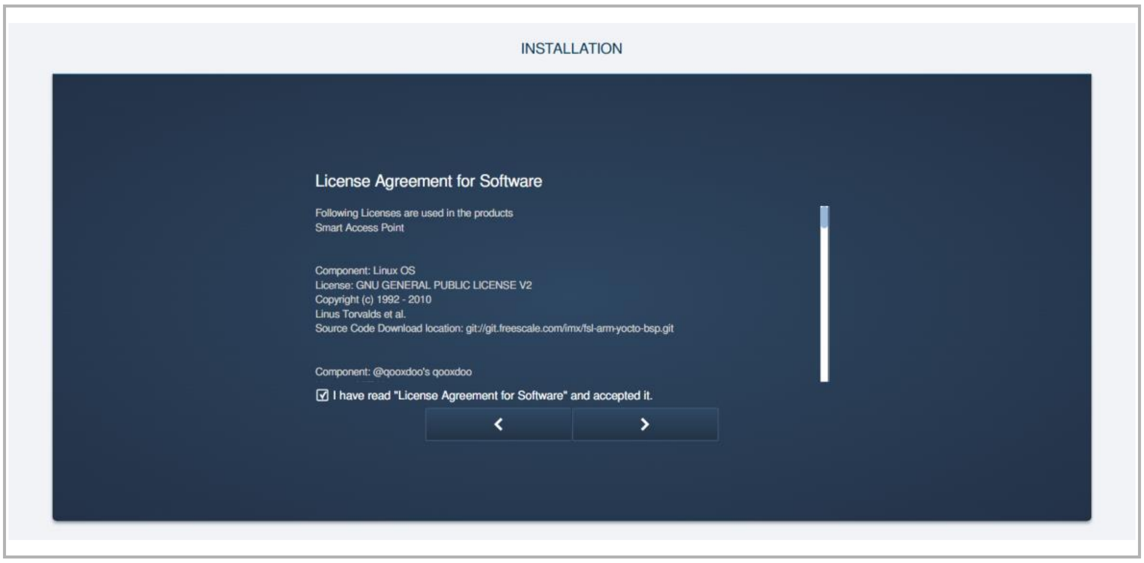
IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE CONTINUING WITH THIS PROGRAM INSTALL

This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and ABB GENWAY XIAMEN ELECTRICAL EQUIPMENT CO., LTD or its affiliates (the "Company") for the "SOFTWARE PRODUCT". SOFTWARE PRODUCT means the machine readable (object code) version of the computer programs including firmware, any copies made, bug fixes for, updates to, or upgrades thereof, and associated software components, media, printed materials, and "online" or electronic documentation.. "Use" or "Using" means to download, install, copy, activate, access or otherwise use the SOFTWARE PRODUCT. By Using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you are entering into

☑ I have read the "End User Licence Agreement" and accepted it.

3. Accepting the licence for software.

Tick the checkbox to accept the licence. Then click ">" to continue.



INSTALLATION

License Agreement for Software

Following Licenses are used in the products
Smart Access Point

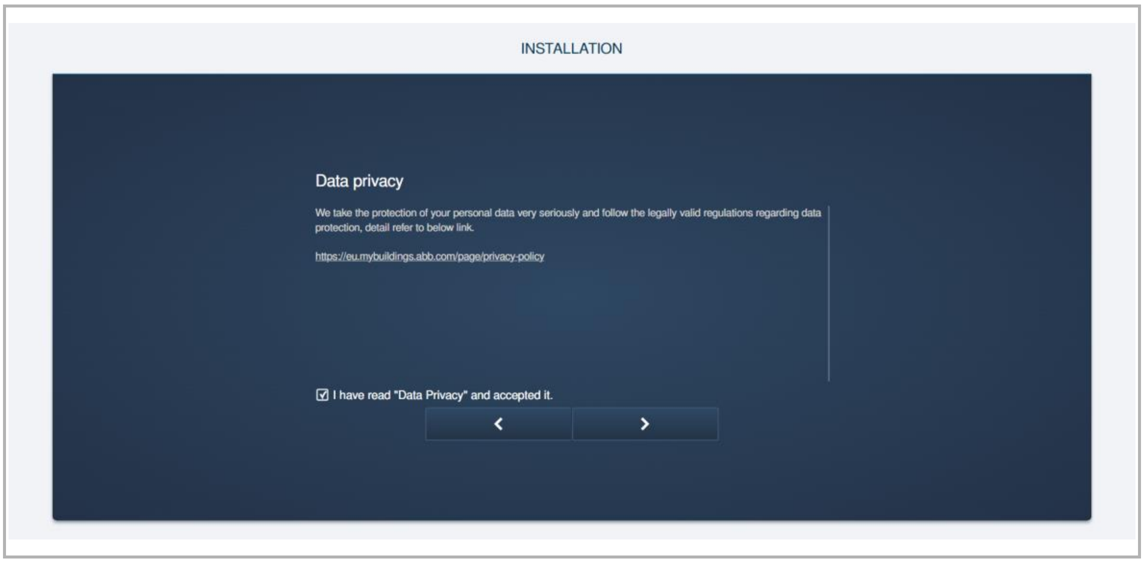
Component: Linux OS
License: GNU GENERAL PUBLIC LICENSE V2
Copyright (c) 1992 - 2010
Linus Torvalds et al.
Source Code Download location: git://git.freescale.com/imx/fsl-arm-yocto-bsp.git

Component: @qooxdoo's qooxdoo

☑ I have read "License Agreement for Software" and accepted it.

4. Accepting data privacy

Tick the checkbox to accept the licence. Then click ">" to continue.



INSTALLATION

Data privacy

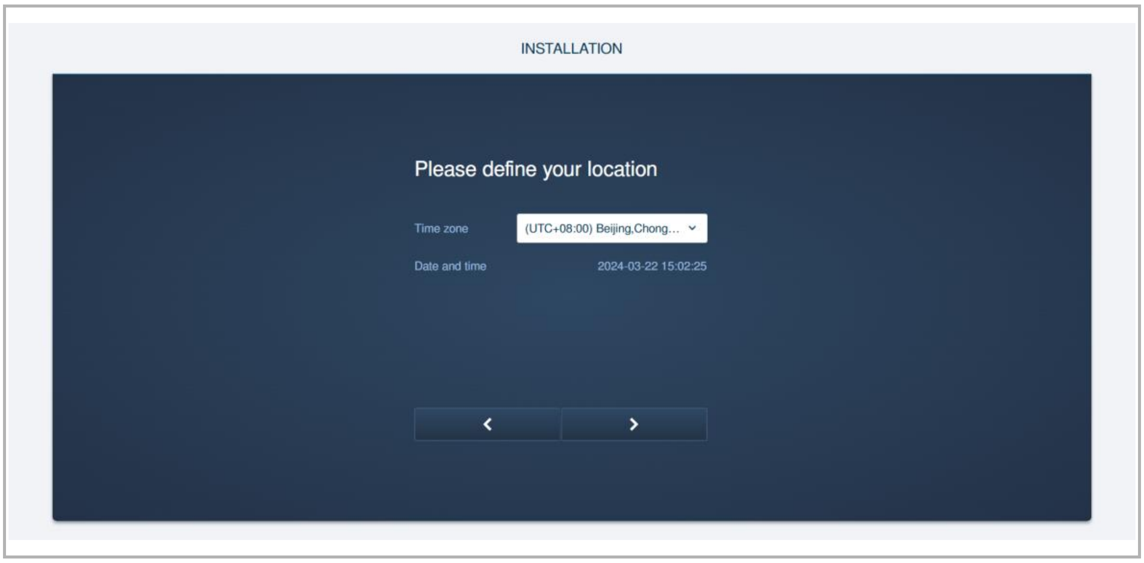
We take the protection of your personal data very seriously and follow the legally valid regulations regarding data protection, detail refer to below link.

https://eu.mybuildings.abb.com/page/privacy-policy

☑ I have read "Data Privacy" and accepted it.

5. Configuring the location

Select the time zone from the drop-down list.



INSTALLATION

Please define your location

Time zone: (UTC+08:00) Beijing,Chong...

Date and time: 2024-03-22 15:02:25

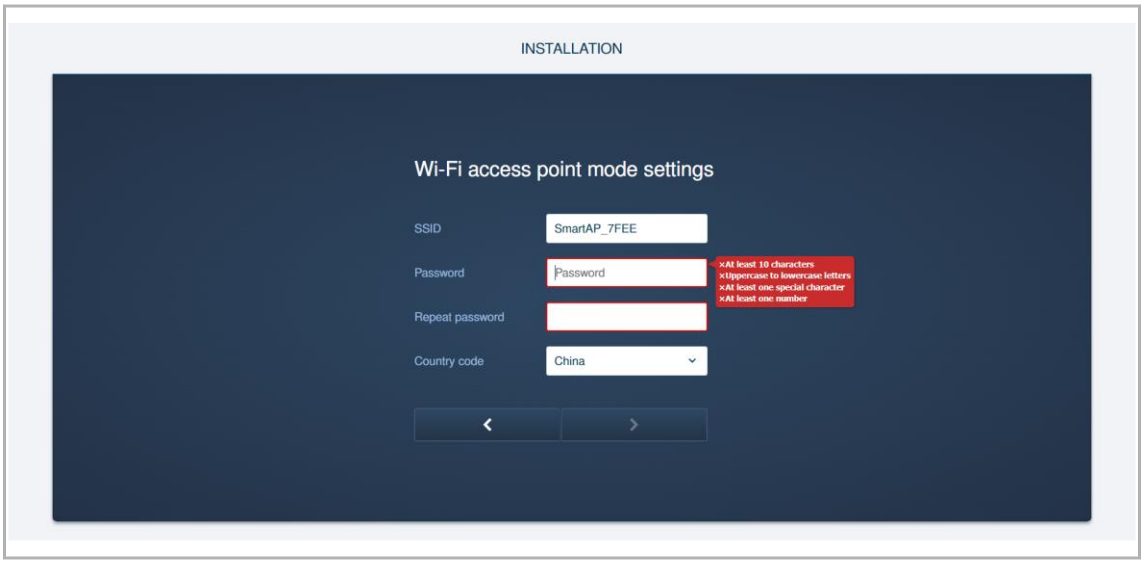
6. Configuring WiFi access point mode settings and the country code

It is compulsory to change the password in the initial setup. The password rule is displayed in a pop-up 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.



INSTALLATION

Wi-Fi access point mode settings

SSID: SmartAP_7FEE

Password: Password

×At least 10 characters
×Uppercase to lowercase letters
×At least one special character
×At least one number

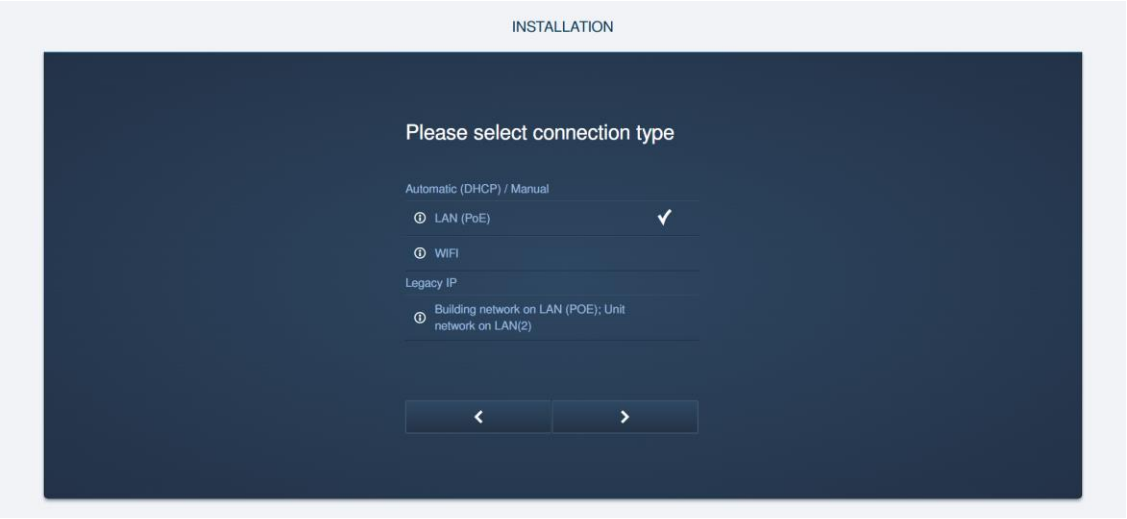
Repeat password:

Country code: China

7. Selecting the connection type

There are 3 options to set the connection type for the SmartAP.

- Tap " ⓘ " to view the topology for reference.



INSTALLATION

Please select connection type

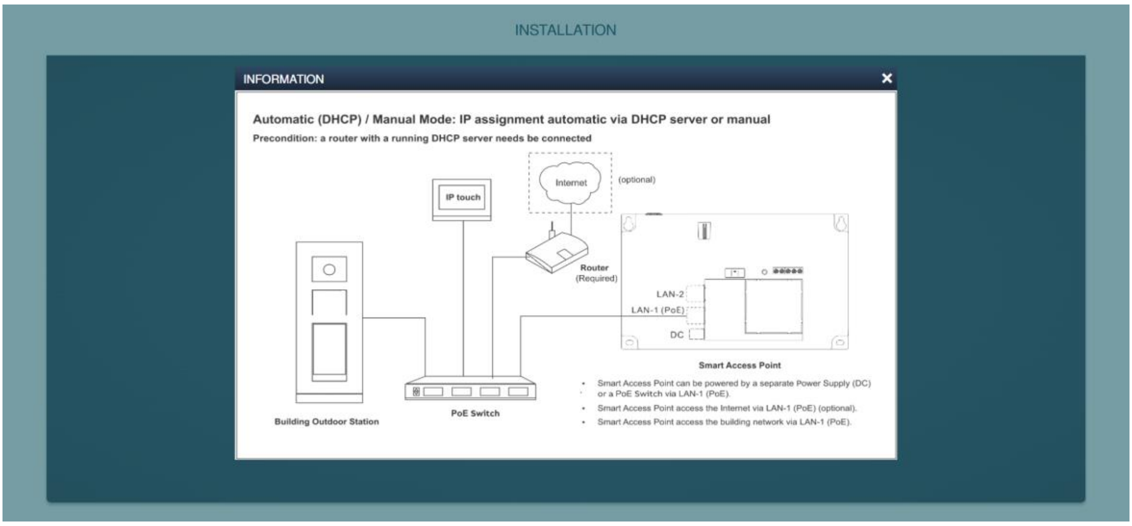
Automatic (DHCP) / Manual

ⓘ LAN (PoE) ✓

ⓘ WIFI

Legacy IP

ⓘ Building network on LAN (POE); Unit network on LAN(2)



INSTALLATION

INFORMATION ✕

Automatic (DHCP) / Manual Mode: IP assignment automatic via DHCP server or manual

Precondition: a router with a running DHCP server needs be connected

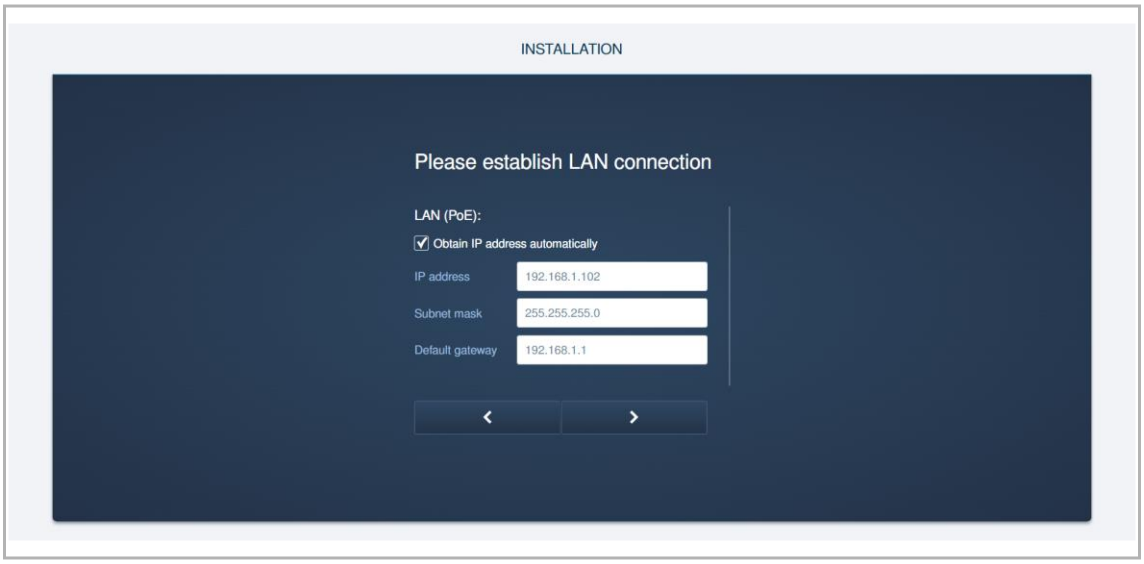
- Smart Access Point can be powered by a separate Power Supply (DC) or a PoE Switch via LAN-1 (PoE).
- Smart Access Point access the Internet via LAN-1 (PoE) (optional).
- Smart Access Point access the building network via LAN-1 (PoE).

Establish LAN connection

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

By activating the "Obtain IP address automatically" check box, 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.



INSTALLATION

Please establish LAN connection

LAN (PoE):

☑ Obtain IP address automatically

IP address: 192.168.1.102

Subnet mask: 255.255.255.0

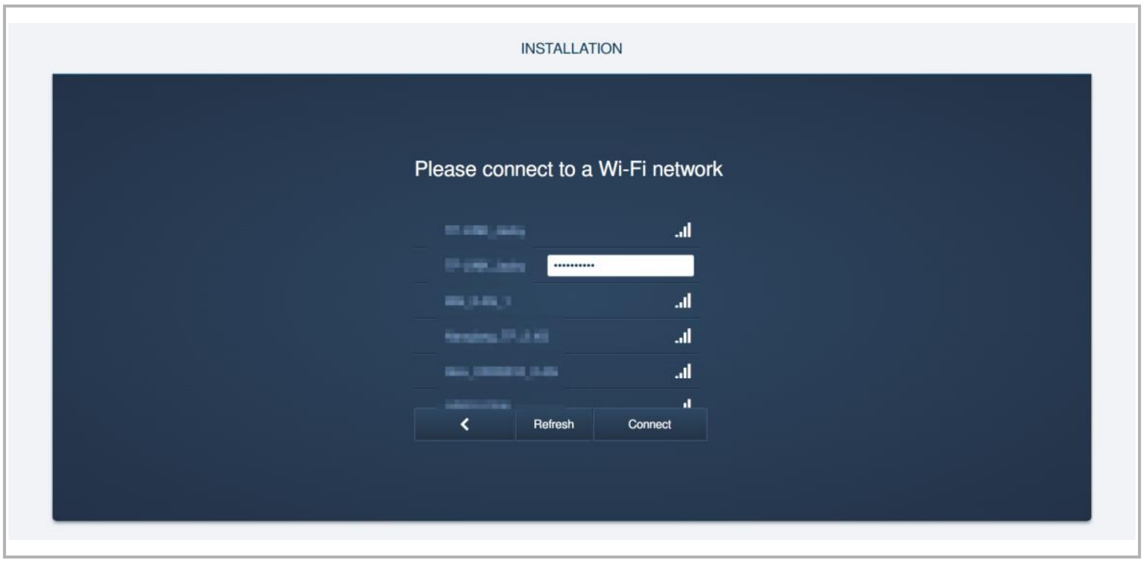
Default gateway: 192.168.1.1

Connect to a WiFi Network

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

All available nearby WiFi networks will be displayed in 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.



INSTALLATION

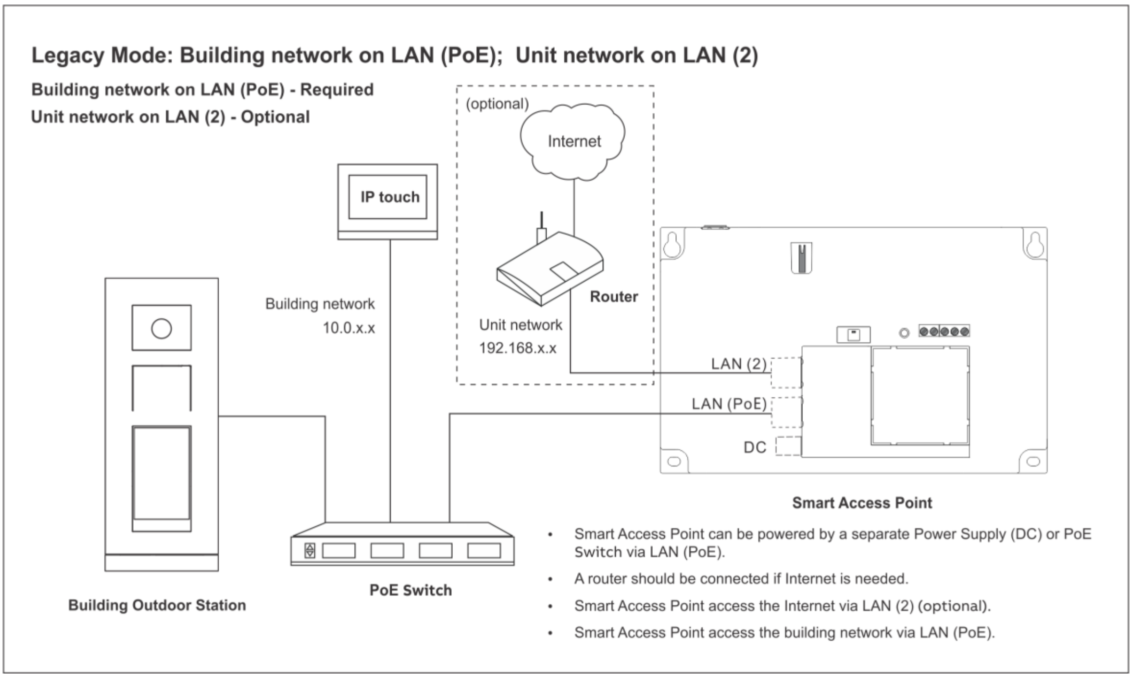
Please connect to a Wi-Fi network

••••••••••

Legacy IP network

If "Legacy IP" is selected, the default topology is used as follow.

- LAN (PoE) will be set to 10.0.x.x, LAN (2) will be connected to the router to obtain the IP address.

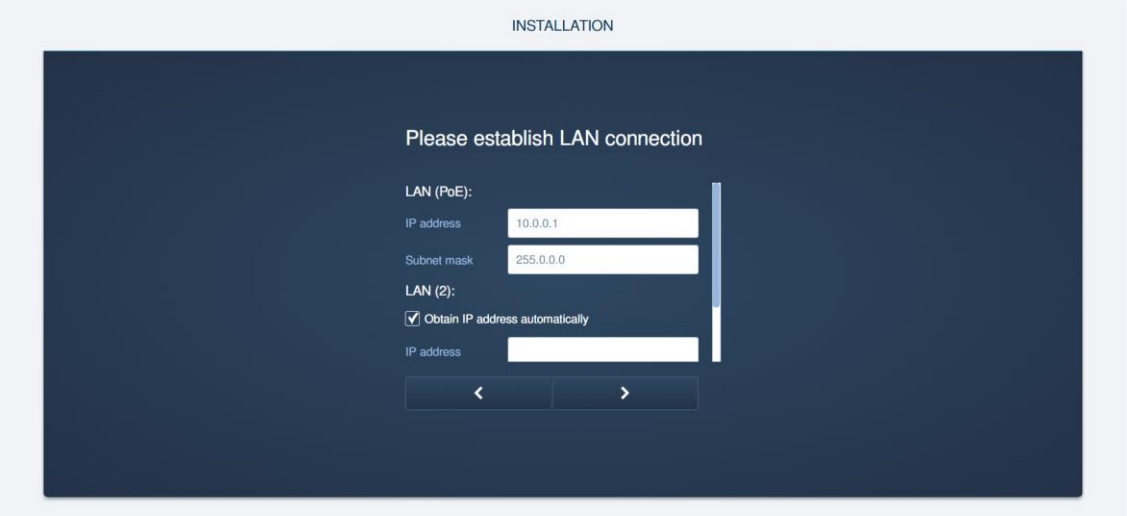


Legacy Mode: Building network on LAN (PoE); Unit network on LAN (2)

Building network on LAN (PoE) - Required

Unit network on LAN (2) - Optional

- Smart Access Point can be powered by a separate Power Supply (DC) or PoE Switch via LAN (PoE).
- A router should be connected if Internet is needed.
- Smart Access Point access the Internet via LAN (2) (optional).
- Smart Access Point access the building network via LAN (PoE).



INSTALLATION

Please establish LAN connection

LAN (PoE):

IP address: 10.0.0.1

Subnet mask: 255.0.0.0

LAN (2):

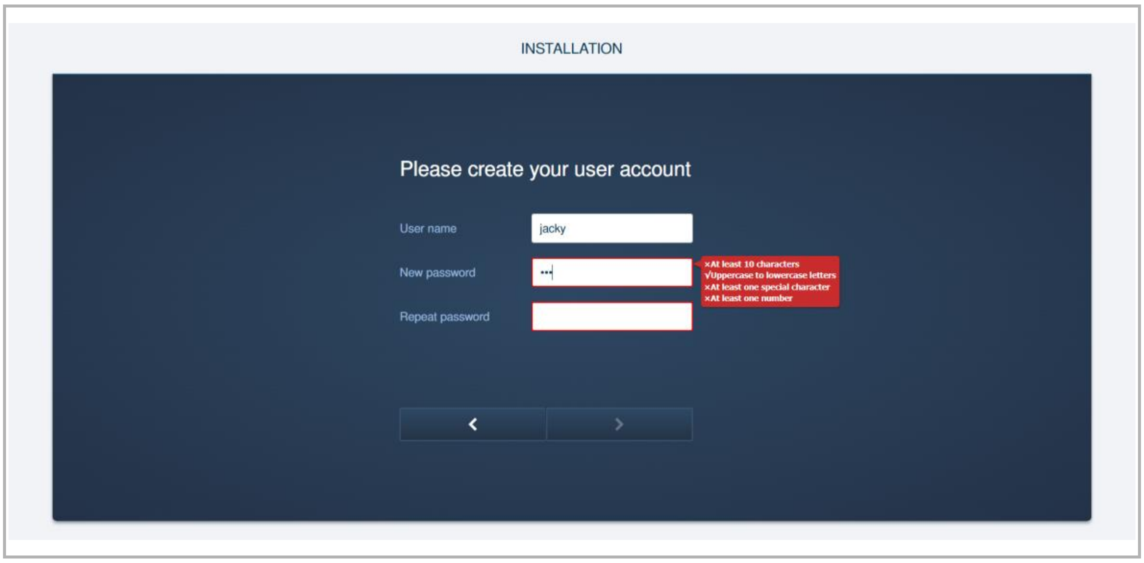
☑ Obtain IP address automatically

IP address:

8. Creating 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.



INSTALLATION

Please create your user account

User name: jacky

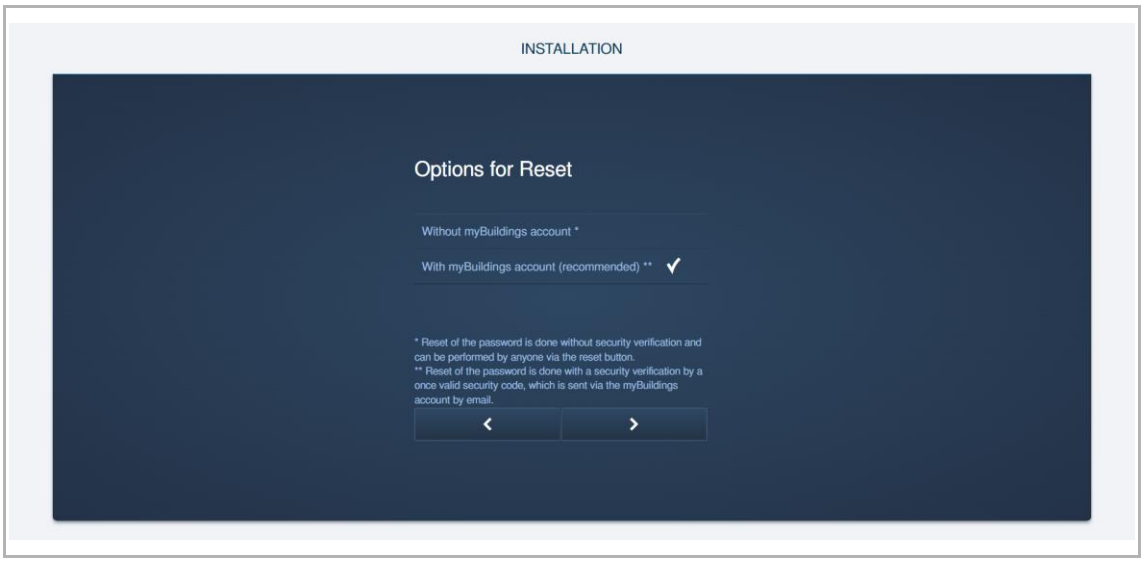
New password: •••

Repeat password:

×At least 10 characters
√Uppercase to lowercase letters
×At least one special character
×At least one number

9. Selecting the reset option

You can select the reset option according to the use scenario.



INSTALLATION

Options for Reset

Without myBuildings account *

With myBuildings account (recommended) ** ✓

* Reset of the password is done without security verification and can be performed by anyone via the reset button.
** Reset of the password is done with a security verification by a once valid security code, which is sent via the myBuildings account by email.

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 SmartAP is installed in a private area and is not physically accessible to unauthorised 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 SmartAP is installed in a public area and is physically accessible to unauthorised users.

Attention!

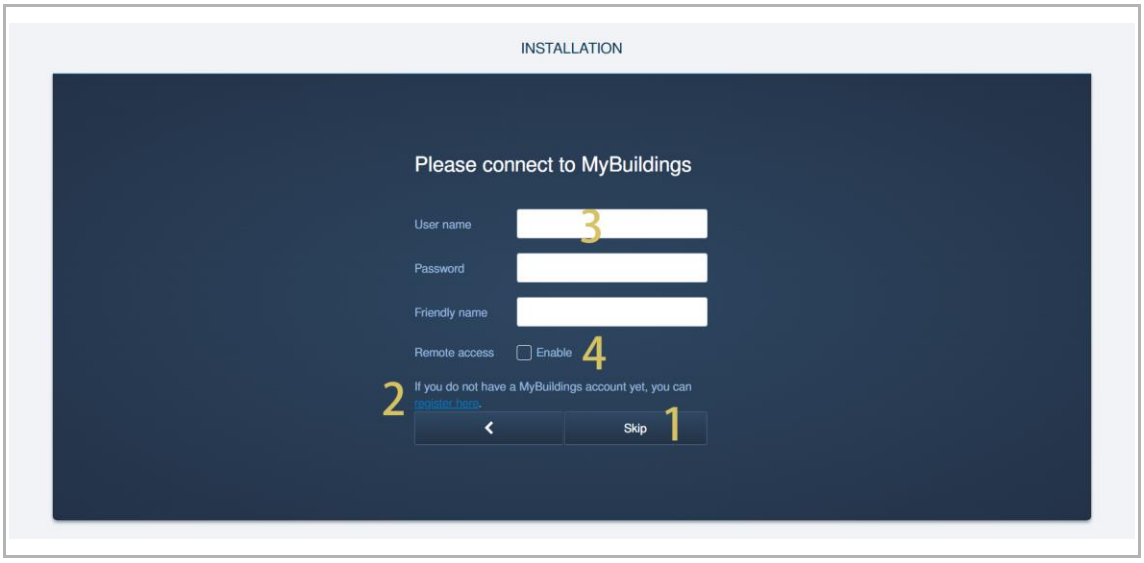
The reset option can only be set in the initial setup and cannot be changed after the initial setup.

The reset option can only be changed when you restore SmartAP to the factory defaults.

10. MyBuildings settings

Reset option = Without MyBuildings account

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


INSTALLATION

Please connect to MyBuildings

User name

Password

Friendly name

Remote access □ Enable

If you do not have a MyBuildings account yet, you can register here.

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

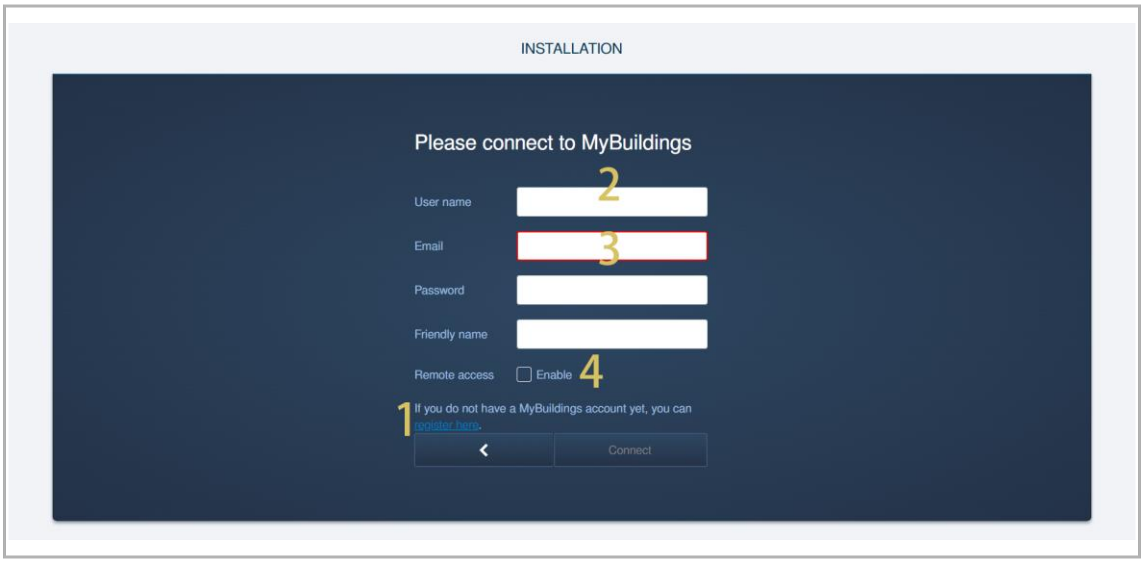
[2] Click "Register here" to access the MyBuildings portal to register an account.

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

[4] If you want to access SmartAP 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.



INSTALLATION

Please connect to MyBuildings

User name

Email

Password

Friendly name

Remote access □ Enable

If you do not have a MyBuildings account yet, you can register here.

[1] Click "Register here" to access the MyBuildings portal to register an account.

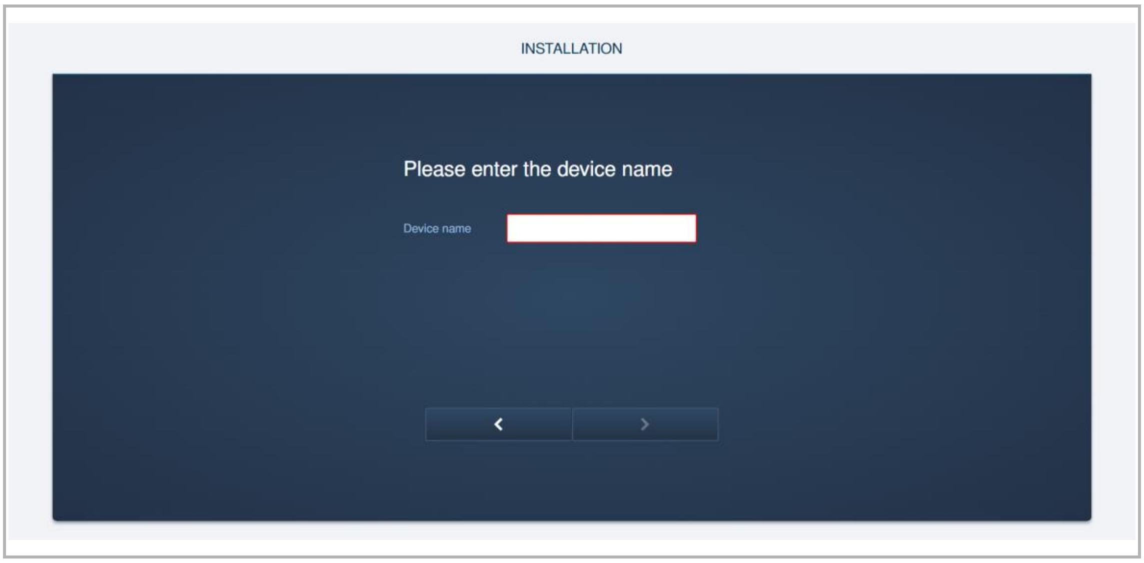
[2] Enter the username, password and friendly name, followed by "Connect" to connect to the MyBuildings portal.

[3] Enter the email address used to activate the MyBuildings account. This email address will receive a security code when you want to reset the first admin user.see chapter 10.6 “Resetting the password for the primary admin“ on page 280.

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

11. Setting the device name

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



INSTALLATION

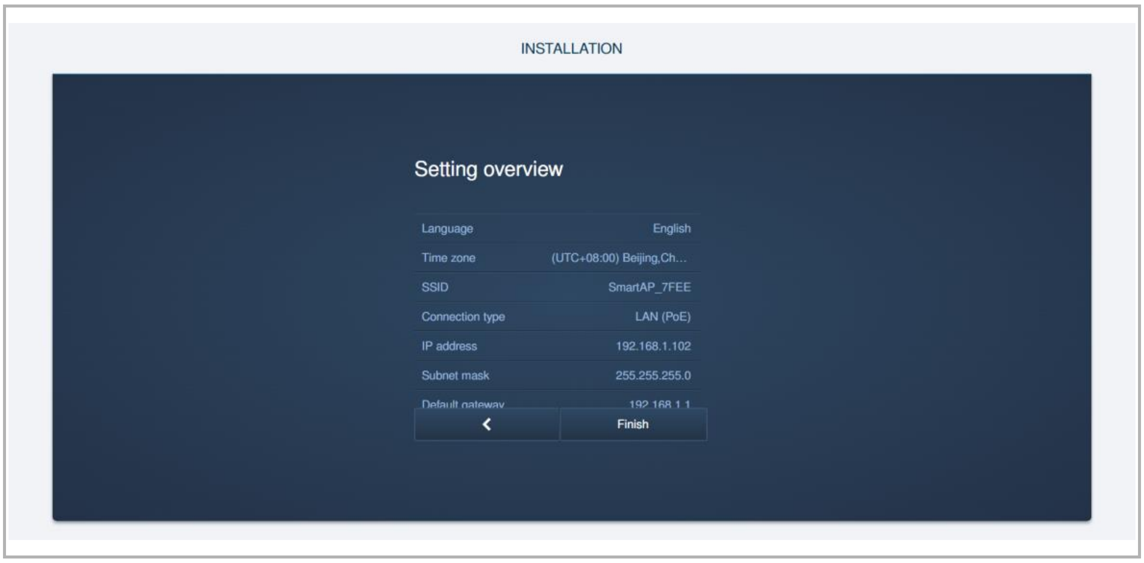
Please enter the device name

Device name

12. Confirming the settings

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

Click "Finish" to complete the initial setup.



INSTALLATION

Setting overview

Language	English
Time zone	(UTC+08:00) Beijing,Ch...
SSID	SmartAP_7FEE
Connection type	LAN (PoE)
IP address	192.168.1.102
Subnet mask	255.255.255.0
Default gateway	192.168.1.1

10.2 Viewing the signature of the device

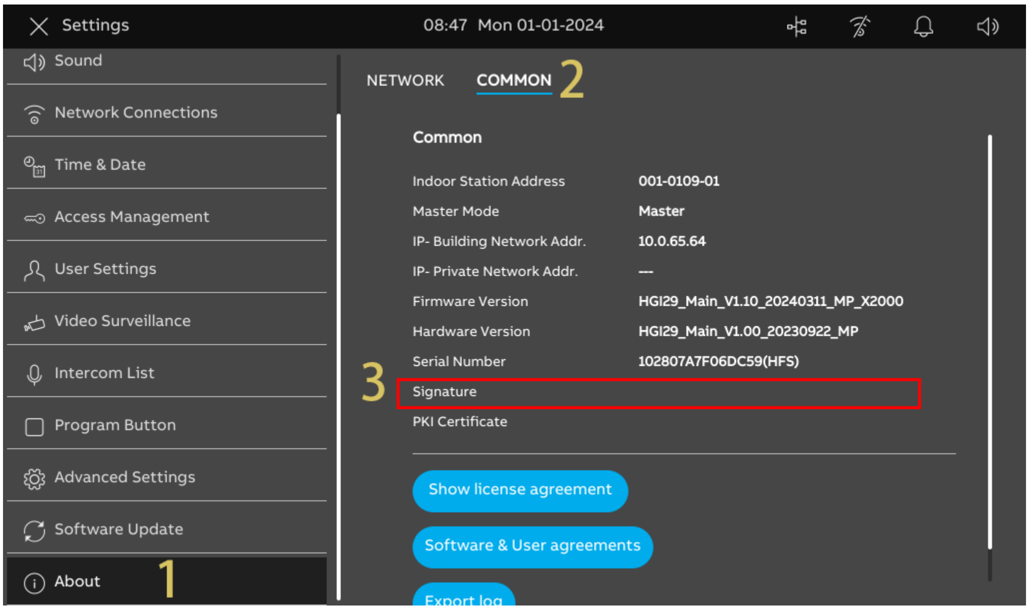
10.2.1 Video IS

Please follow the steps below:

[1] On the "Settings" screen, tap "About".

[2] Tap "Common".

[3] Go to the "Signature" section to check the signature.

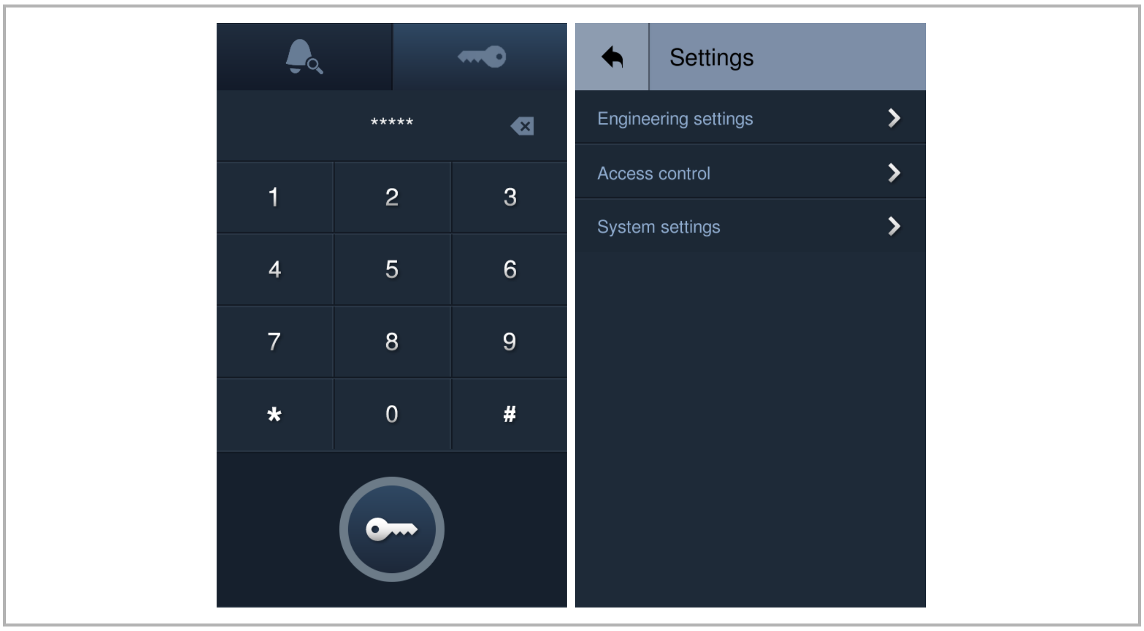


Common

Indoor Station Address	001-0109-01
Master Mode	Master
IP- Building Network Addr.	10.0.65.64
IP- Private Network Addr.	---
Firmware Version	HGI29_Main_V1.10_20240311_MP_X2000
Hardware Version	HGI29_Main_V1.00_20230922_MP
Serial Number	102807A7F06DC59(HFS)
Signature	
PKI Certificate	

10.2.2 IP Touch 5 OS

- On the home screen, tap " 🔑 ", followed by [#] [*] [engineering password] [#] to access the "Settings" screen.
- On the "Settings" screen, tap "Engineering settings", "Help" to view the signature.



10.2.3 IP Pushbutton OS

This device can be configured on Video IS.

IP Pushbutton OS entering engineering mode

Please follow the steps below:

[1] Power on the IP Pushbutton OS, wait until all 3 LED indicators go out.

[2] Press and hold the first pushbutton for 10 seconds until all 3 LED indicators flash.

Video IS accessing the "Outdoor Stations" screen

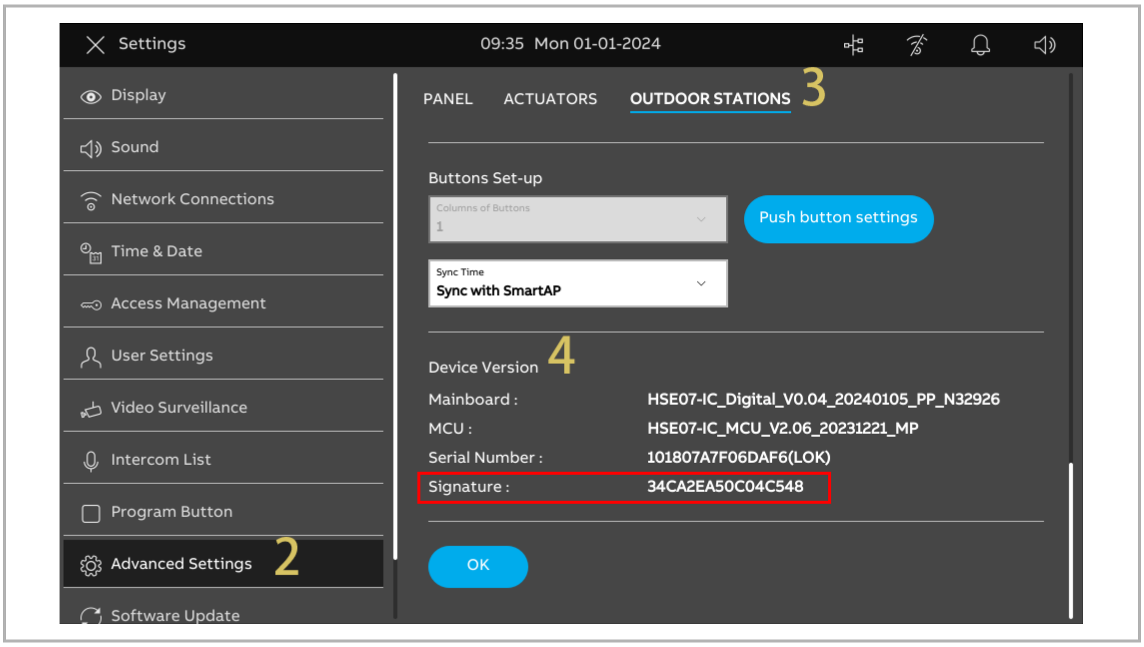
Please follow the steps below:

[1] Ensure that IP Pushbutton OS is in engineering mode.

[2] On the "Settings" screen of the panel, tap "Advanced settings".

[3] Tap "Outdoor Stations" to access the corresponding screen.

[4] On the "Outdoor Stations" screen, go to "Device Version" section to view the signature.



Buttons Set-up

Columns of Buttons: 1

Sync Time: Sync with SmartAP

Device Version

Mainboard : HSE07-IC_Digital_V0.04_20240105_PP_N32926

MCU : HSE07-IC_MCU_V2.06_20231221_MP

Serial Number : 101807A7F06DAF6(LOK)

Signature : 34CA2EA50C04C548

10.2.4 Mini OS

This device could be configured on Video IS.

IP Pushbutton OS entering engineering mode

Please follow the steps below:

[1] Power on the Mini OS, wait until all 3 LED indicators go out.

[2] Press and hold the first pushbutton for 5 seconds until all 3 LED indicators flash.

Video IS accessing the "Outdoor Stations" screen

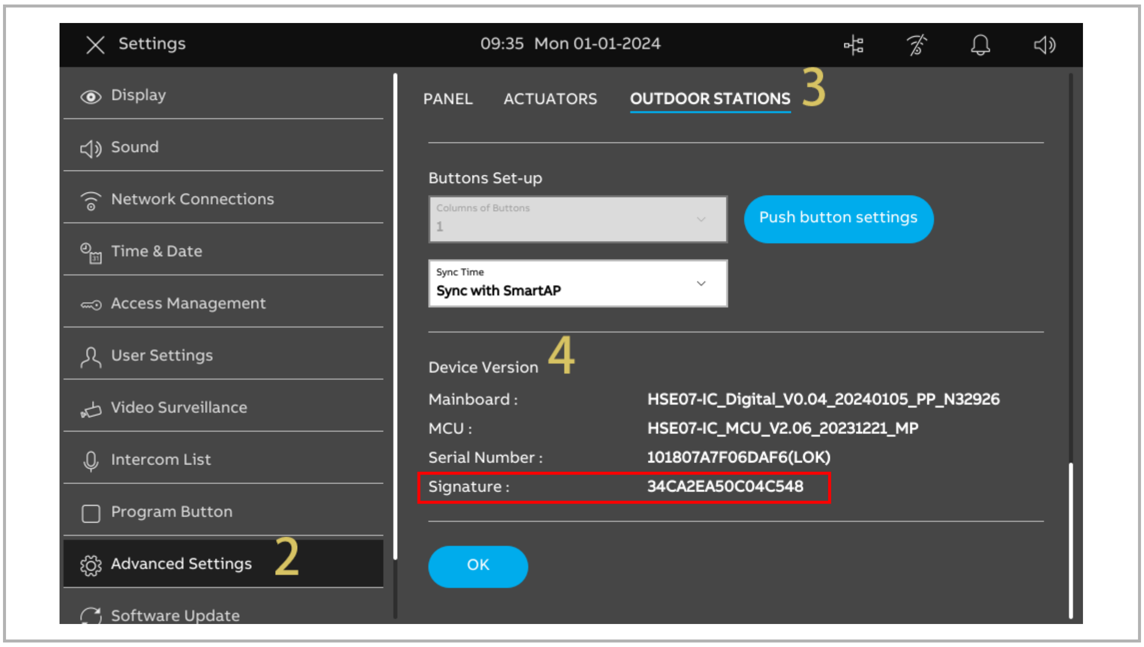
Please follow the steps below:

[1] Ensure that Mini OS is in engineering mode.

[2] On the "Settings" screen of the panel, tap "Advanced settings".

[3] Tap "Outdoor Stations" to access the corresponding screen.

[4] On the "Outdoor Stations" screen, go to "Device Version" section to view the signature.



Buttons Set-up

Columns of Buttons: 1

Sync Time: Sync with SmartAP

Device Version

Mainboard : HSE07-IC_Digital_V0.04_20240105_PP_N32926

MCU : HSE07-IC_MCU_V2.06_20231221_MP

Serial Number : 101807A7F06DAF6(LOK)

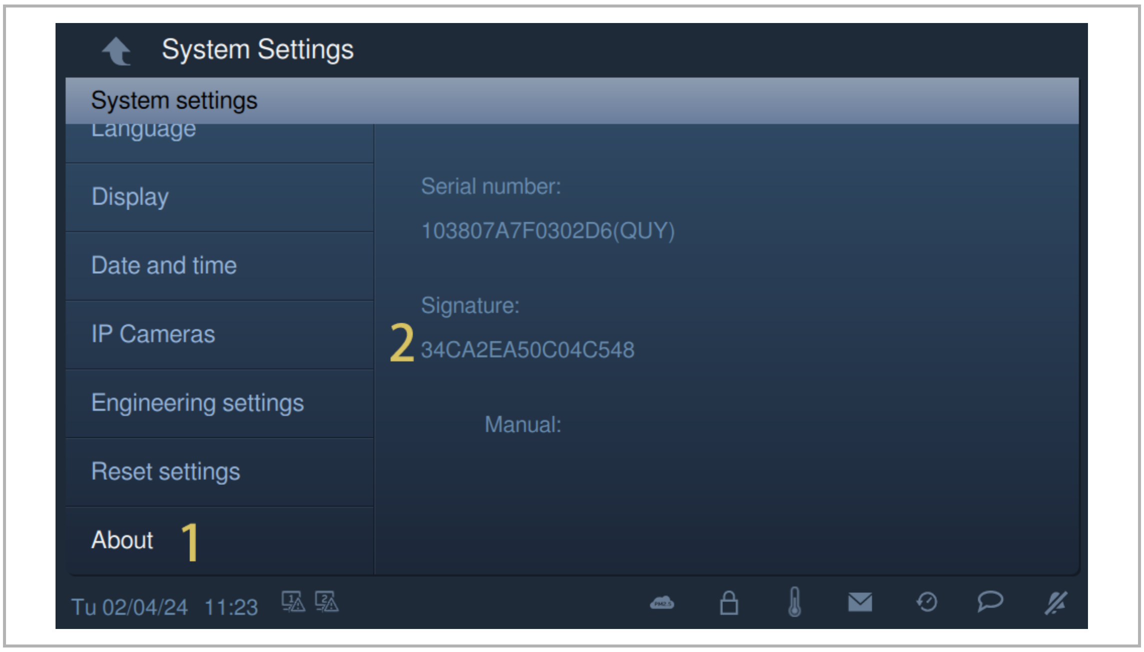
Signature : 34CA2EA50C04C548

10.2.5 Guard Unit

Please follow the steps below:

[1] On the "System Settings" screen, tap "About".

[2] Go to "Signature" section to check the signature.



Serial number:
103807A7F0302D6(QUY)

Signature:
34CA2EA50C04C548

Manual:

10.2.6 IP Actuator

This device could be configured on Video IS.

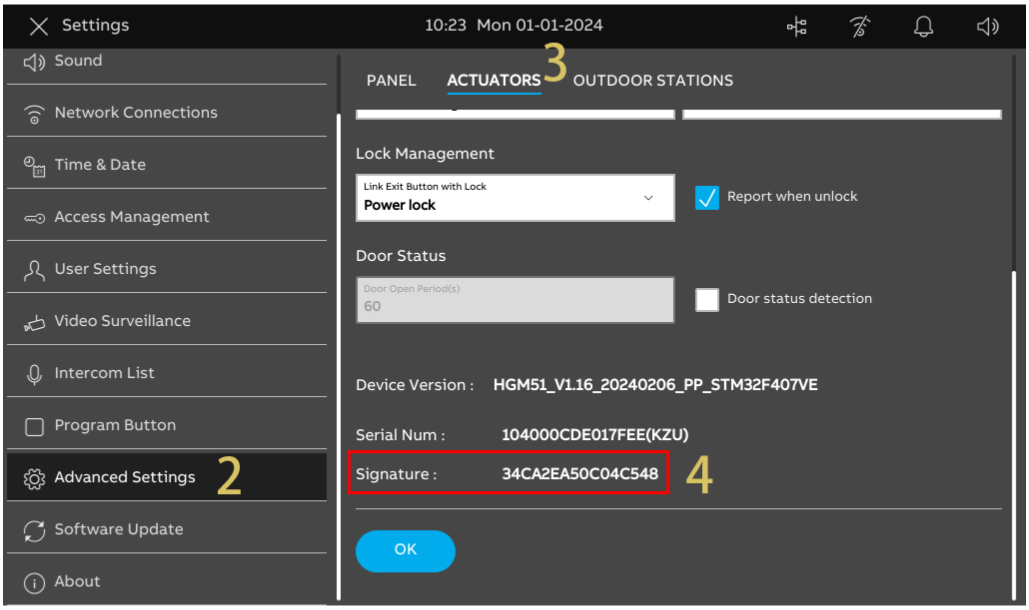
Please follow the steps below:

[1] Press the reset button of the IP Actuator once during normal operation; the LED flashing green means that the IP actuator has entered engineering mode.

[2] On the "Settings" screen of the panel, tap "Advanced settings".

[3] Tap "Actuators" to access the corresponding screen.

[4] On the "Actuators" screen, go to the "Signature" section to view the signature.



Lock Management

Link Exit Button with Lock: Power lock

☑ Report when unlock

Door Status

Door Open Period(s): 60

□ Door status detection

Device Version : HGM51_V1.16_20240206_PP_STM32F407VE

Serial Num : 104000CDE017FEE(KZU)

Signature : 34CA2EA50C04C548

10.3 Clearing the signature of the device

The signature will be empty as one of the following scenarios:

- The device is powered on the first time.
- The device is restored to factory default settings.see chapter 10.5 “Restoring to factory default“ on page 271.
- The device changed its physical address.see chapter 10.4 “Configuring the physical address and IP mode“ on page 259.

10.4 Configuring the physical address and IP mode

10.4.1 Video IS

Please follow the steps below:

[1] On the "Settings" screen, tap "Advanced settings" and enter the advanced password (The system default advanced password is 345678) to access the corresponding screen.

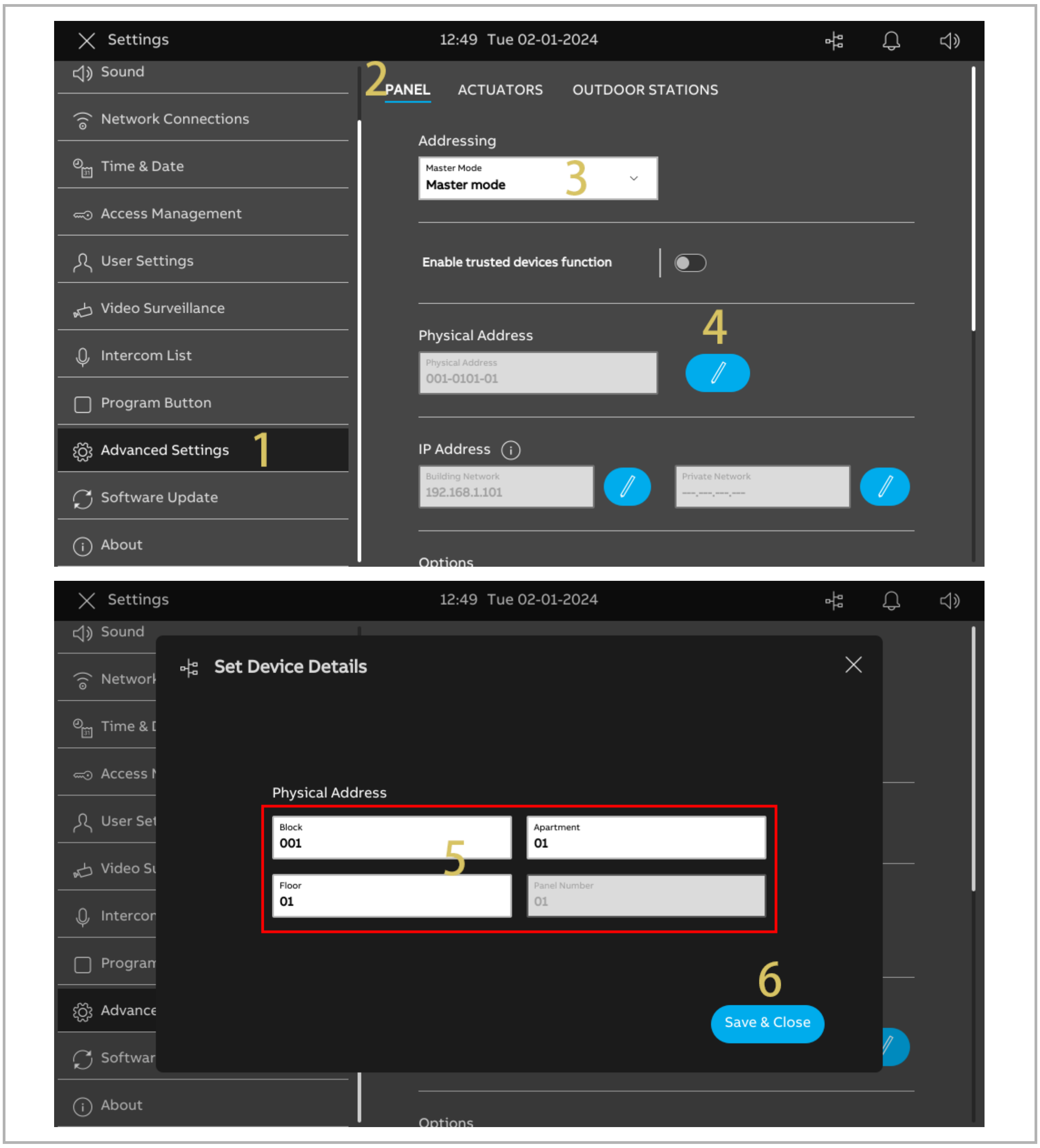
[2] On the "Advanced settings" screen, tap "Panel".

[3] Go to the "Addressing" section, select the device type from the drop-down list.

[4] Go to the "Physical address" section, tap " ✎ ".

[5] Edit the physical address.

[6] Tap "Save & Close".



Settings 12:49 Tue 02-01-2024

Addressing
Master Mode: Master mode

Enable trusted devices function

Physical Address: 001-0101-01

IP Address
Building Network: 192.168.1.101
Private Network: ---.---.---.---

Set Device Details

Physical Address
Block: 001
Apartment: 01
Floor: 01
Panel Number: 01

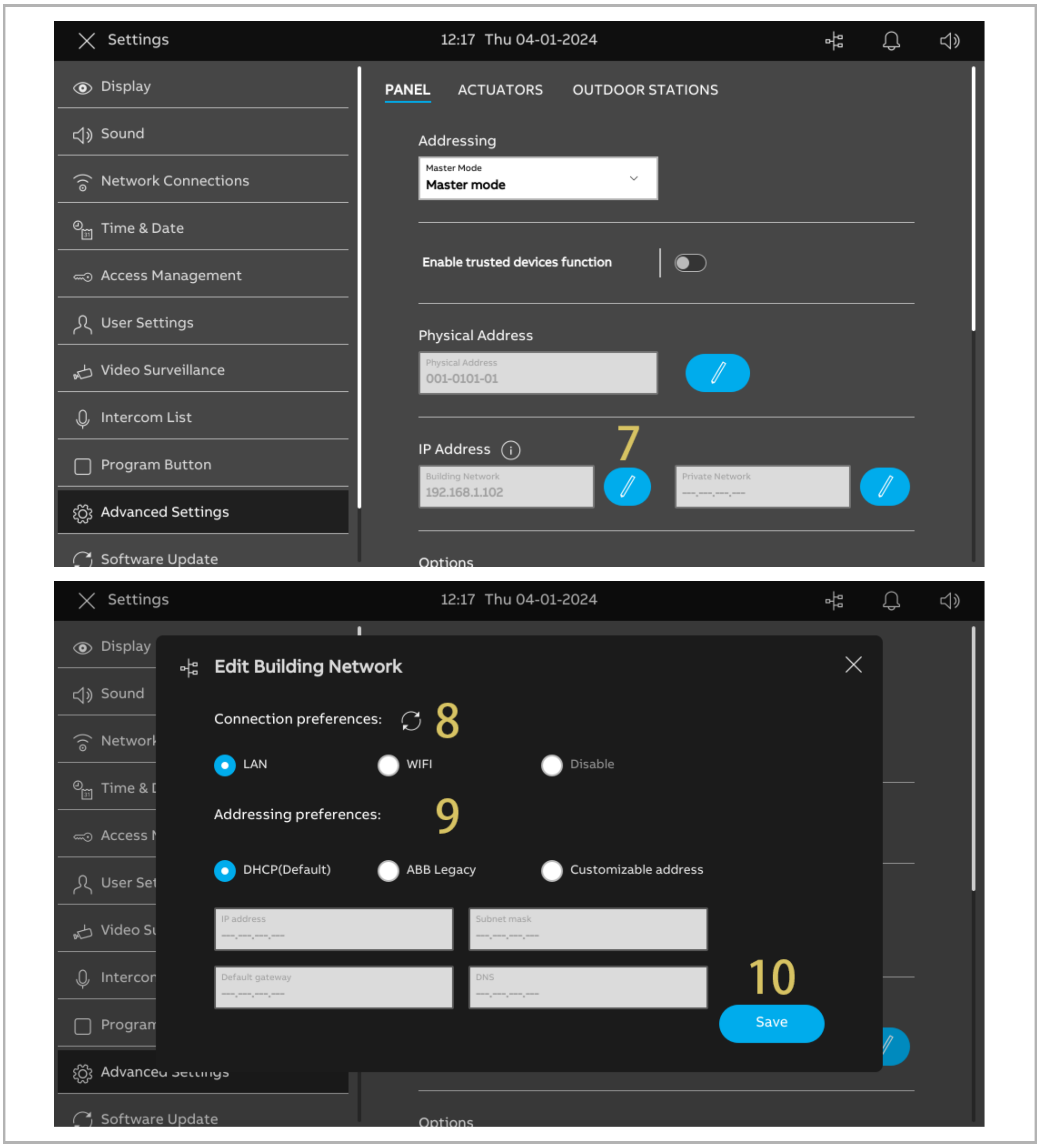
[7] Go to the "IP Address" section, tap " ✎ ".

[8] Select the connection type, it can be set to "LAN" or "WiFi".

[9] Select the network type, it can be set to "DHCP", "Customizable address" or "ABB Legacy".

- If "ABB Legacy" is selected, the IP address will be "10.0.x.x". Its network type should be the same as the SmartAP.
- If the network type of the SmartAP is set to "Legacy IP", you should select "ABB Legacy" to avoid unknown errors.

[10]Tap "Save".



Master Mode: Master mode

Physical Address: 001-0101-01

Building Network: 192.168.1.102

Private Network: ---.---.---.---

Connection preferences:

● LAN ○ WIFI ○ Disable

Addressing preferences:

● DHCP(Default) ○ ABB Legacy ○ Customizable address

IP address: ---.---.---.---

Subnet mask: ---.---.---.---

Default gateway: ---.---.---.---

DNS: ---.---.---.---

10.4.2 Audio IS

This device configures the physical address via SmartAP.

10.4.3 IP Touch 5 OS

Please follow the steps below:

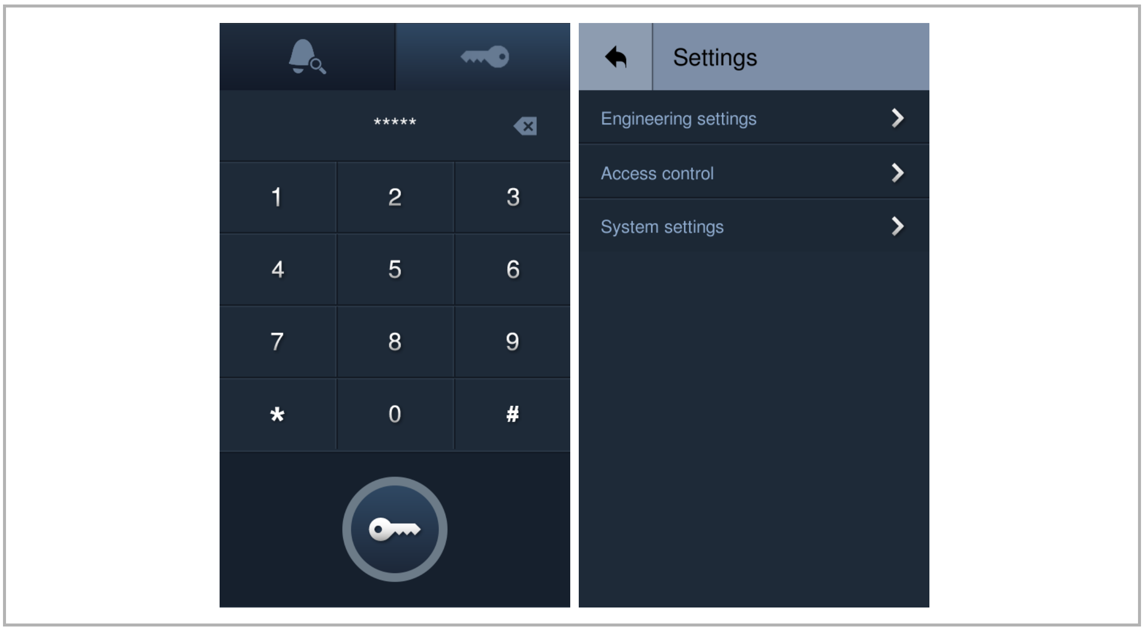
[1] On the home screen, tap " 🔑 ", followed by [#] [*] [engineering password] [#] to access the "Settings" screen.

[2] On the "Settings" screen, tap "Engineering settings".

[3] On the "Engineering settings" screen, tap "Device attribute" to edit the device type & physical address.

[4] On the "Engineering settings" screen, tap "IP address setting" to edit the network type. It can be set to "DHCP", "Customizable address" or "ABB Legacy".

- If "ABB Legacy" is selected, the IP address will be "10.0.x.x". Its network type should be the same as the SmartAP.
- If the address type of the SmartAP is set to "Legacy IP", you should select "Legacy IP" to avoid unknown errors.



10.4.4 IP Pushbutton OS

This device could be configured on Video IS.

IP Pushbutton OS entering engineering mode

Please follow the steps below:

[1] Power on the IP Pushbutton OS, wait until all 3 LED indicators go out.

[2] Press and hold the first pushbutton for 10 seconds until all 3 LED indicators flash.

Video IS accessing the "Outdoor Stations" screen

Please follow the steps below:

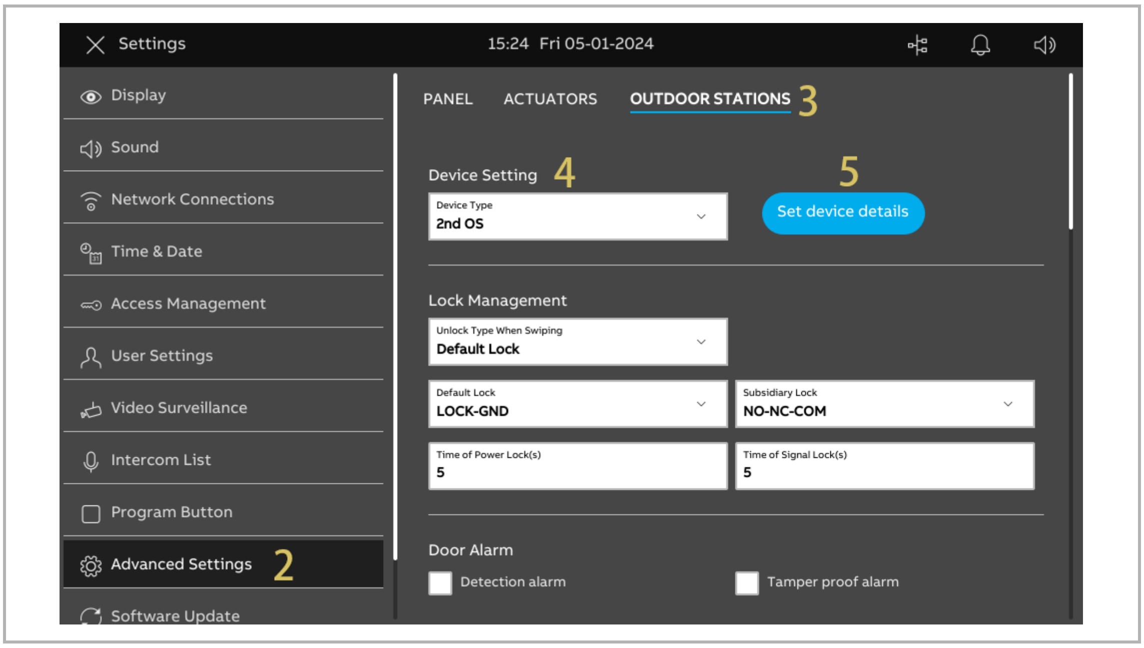
[1] Ensure that IP Pushbutton OS is in engineering mode.

[2] On the "Settings" screen of the panel, tap "Advanced settings".

[3] Tap "Outdoor Stations" to access the corresponding screen.

[4] On the "Outdoor Stations" screen, go to "Device Version" section to select the device type.

[5] Tap "Set device details".



Device Type: 2nd OS

Unlock Type When Swiping: Default Lock

Default Lock: LOCK-GND

Subsidiary Lock: NO-NC-COM

Time of Power Lock(s): 5

Time of Signal Lock(s): 5

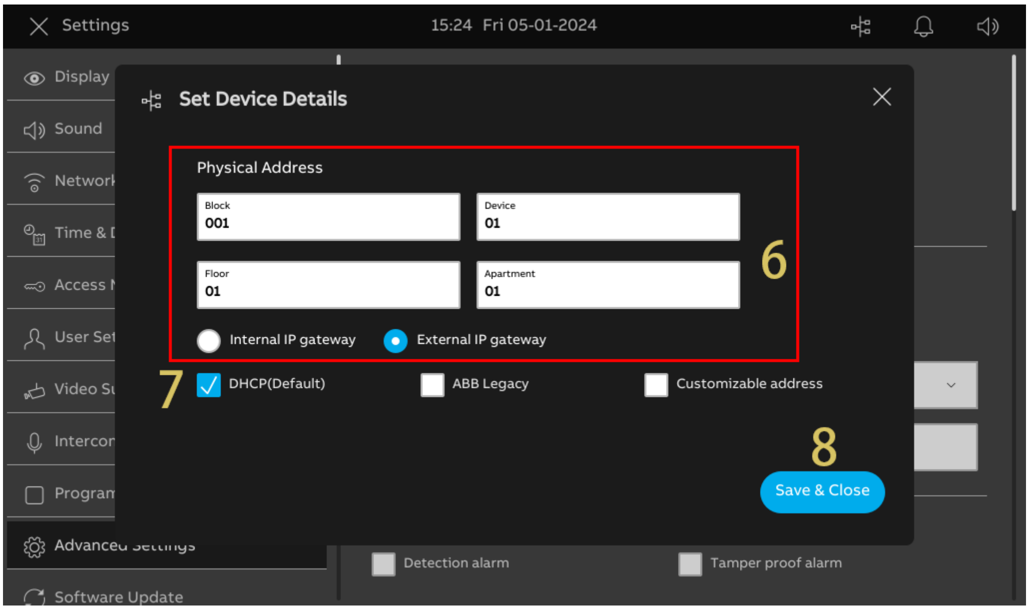
[6] Select the connection type and edit the physical address.

- If IP pushbutton OS is connected to the building network, "External IP gateway" should be selected.
- If IP pushbutton OS is connected to the private network, "Internal IP gateway" should be selected.

[7] Select the network type, it can set to "DHCP", "Customizable address" or "ABB Legacy".

- If "ABB Legacy" is selected, the IP address will be "10.0.x.x". Its network type should be the same as the SmartAP.
- If the address type of the SmartAP is set to "Legacy IP", you should select "ABB Legacy" to avoid unknown errors.

[8] Tap "Save & Close".



Set Device Details

Physical Address

Block: 001

Device: 01

Floor: 01

Apartment: 01

○ Internal IP gateway ● External IP gateway

☑ DHCP(Default) □ ABB Legacy □ Customizable address

10.4.5 Mini OS

This device can be configured on Video IS.

Mini OS entering engineering mode

Please follow the steps below:

[1] Power on the Mini OS, wait until all 3 LED indicators go out.

[2] Press and hold the first pushbutton for 5 seconds until all 3 LED indicators flash.

Video IS accessing the "Outdoor Stations" screen

Please follow the steps below:

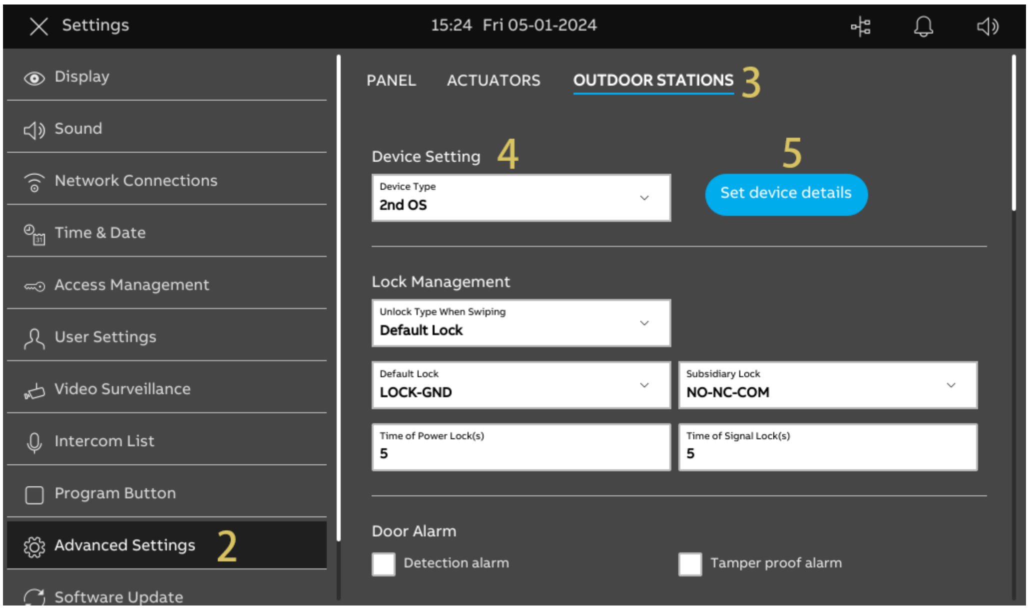
[1] Ensure that Mini OS is in engineering mode.

[2] On the "Settings" screen of the panel, tap "Advanced settings".

[3] Tap "Outdoor Stations" to access the corresponding screen.

[4] On the "Outdoor Stations" screen, go to "Device Version" section to select the device type.

[5] Tap "Set device details".



Device Setting
Device Type: 2nd OS

Unlock Type When Swiping: Default Lock

Default Lock: LOCK-GND

Subsidiary Lock: NO-NC-COM

Time of Power Lock(s): 5

Time of Signal Lock(s): 5

□ Detection alarm
□ Tamper proof alarm

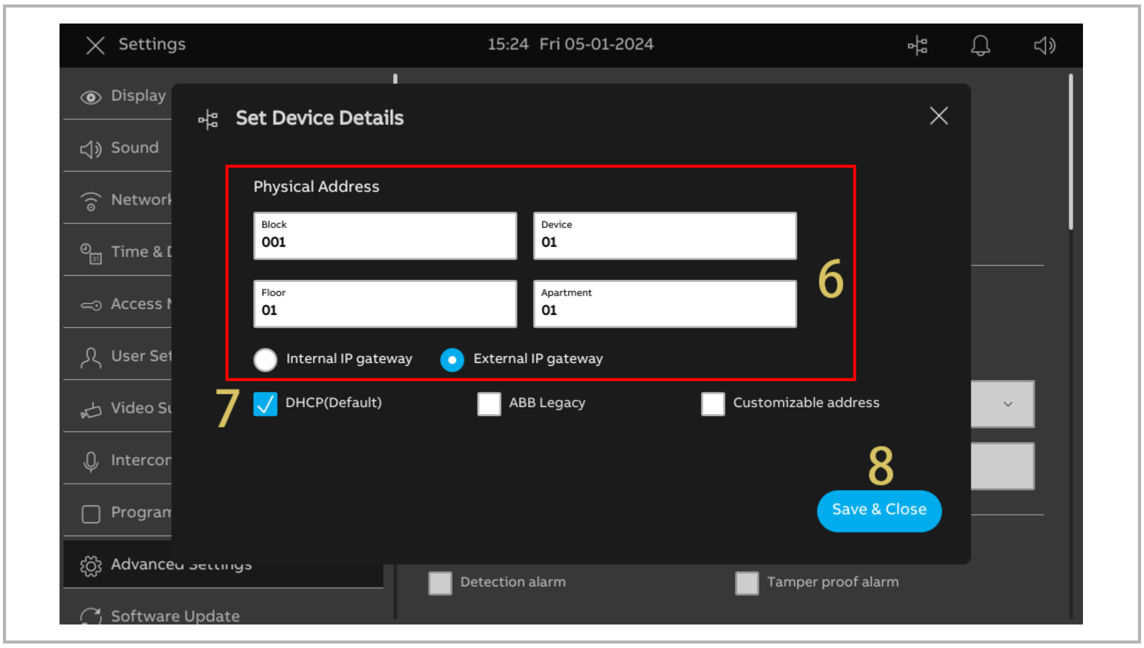
[6] Select the connection type and edit the physical address.

- If IP pushbutton OS is connected to building network, "External IP gateway" should be selected.
- If IP pushbutton OS is connected to private network, "Internal IP gateway" should be selected.

[7] Select the network type, it can set to "DHCP", "Customizable address" or "ABB Legacy".

- If "ABB Legacy" is selected, the IP address will be "10.0.x.x". Its network type should be the same as the SmartAP.
- If the address type of the SmartAP is set to "Legacy IP", you should select "ABB Legacy" to avoid unknown errors.

[8] Tap "Save & Close".



Set Device Details

Physical Address

Block: 001	Device: 01
Floor: 01	Apartment: 01

○ Internal IP gateway ● External IP gateway

☑ DHCP(Default) □ ABB Legacy □ Customizable address

10.4.6 Guard Unit

Please follow the steps below:

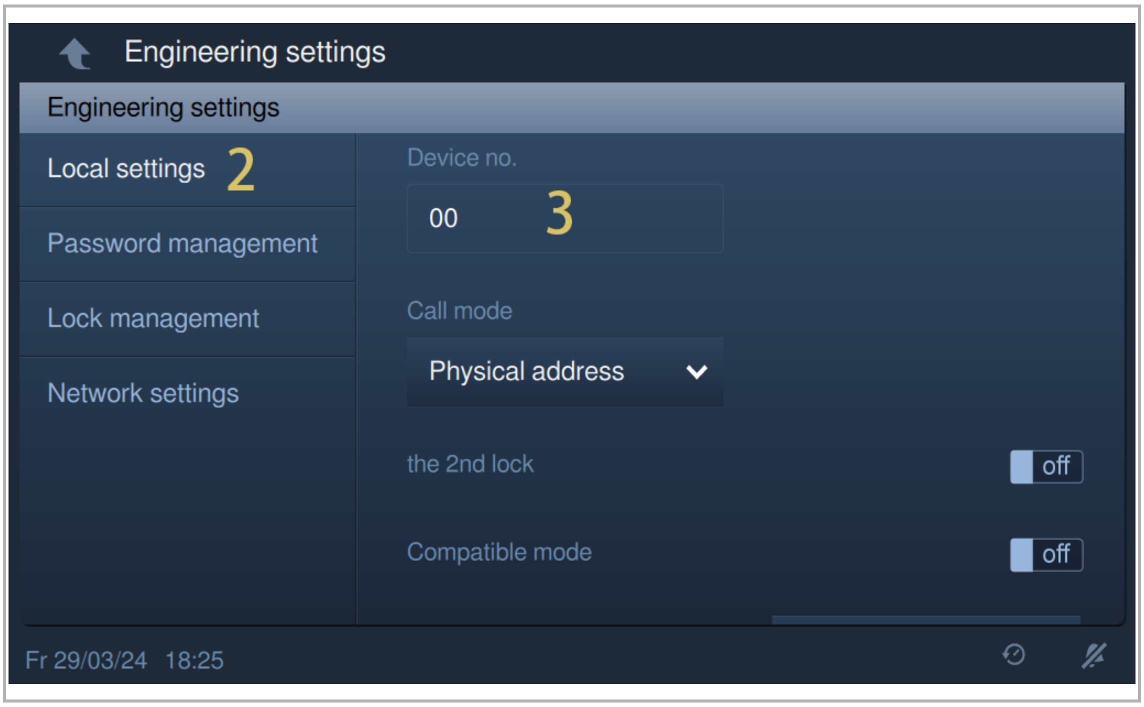
[1] On the "System settings" screen, click "Engineering settings", enter the engineering password to access the settings.

[2] On the "Engineering settings" screen, tap "Local settings".

[3] Go to "Device no." section, edit the physical address.

[4] Tap "Network settings", select the network type, it can set to "DHCP", "Customizable address" or "Legacy IP".

- If "ABB Legacy" is selected, the IP address will be "10.0.x.x". Its network type should be the same as the SmartAP.
- If the network type of the SmartAP is set to "Legacy IP", you should select "Legacy IP" to avoid unknown errors.



Engineering settings

Engineering settings

Local settings 2

Password management

Lock management

Network settings

Device no.

00 3

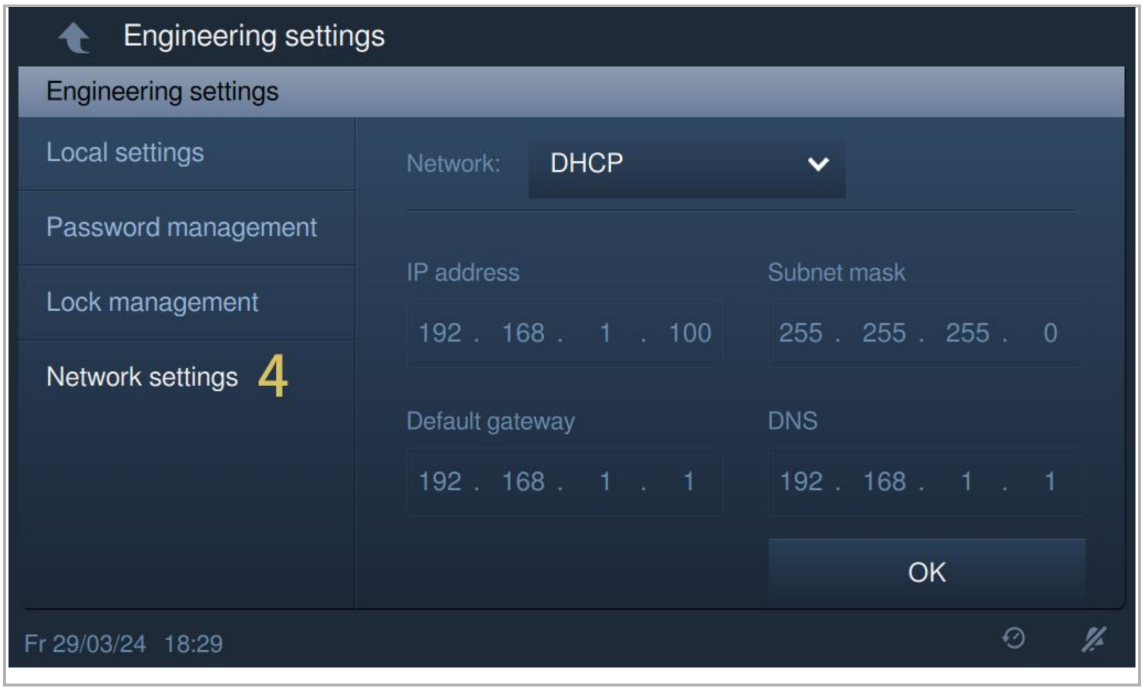
Call mode

Physical address

the 2nd lock off

Compatible mode off

Fr 29/03/24 18:25



Engineering settings

Engineering settings

- Local settings
- Password management
- Lock management
- Network settings 4

Network: DHCP

IP address: 192 . 168 . 1 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

DNS: 192 . 168 . 1 . 1

OK

Fr 29/03/24 18:29

10.4.7 IP Actuator

This device could be configured on Video IS.

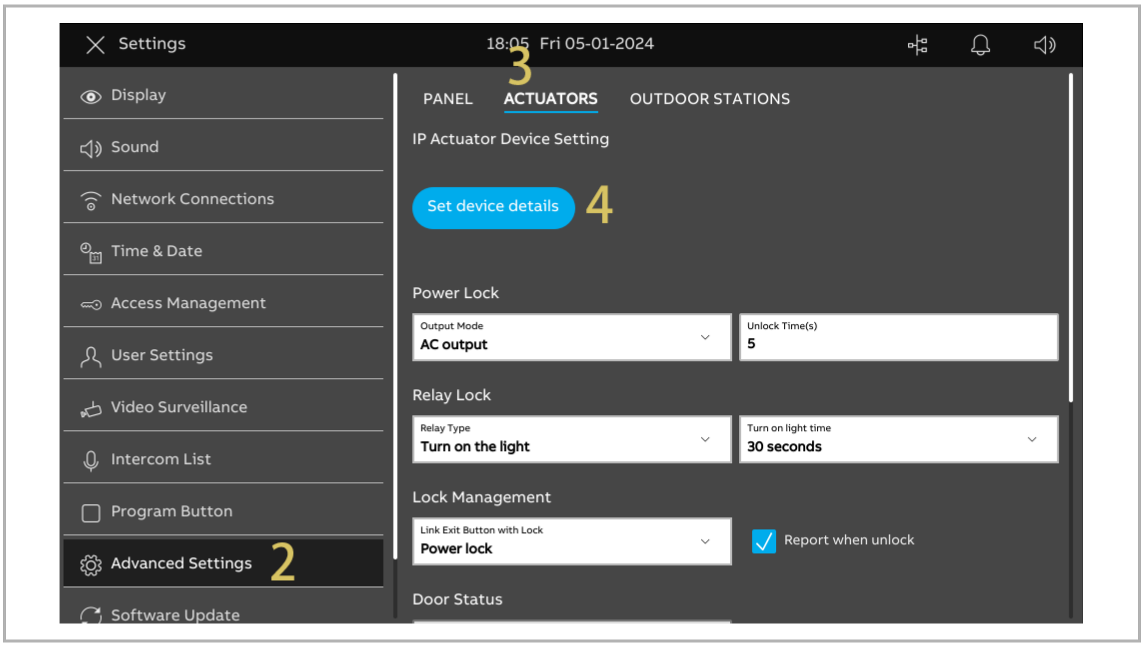
Please follow the steps below:

[1] Press the reset button of the IP Actuator once during normal operation; the LED flashing green means that the IP actuator has entered engineering mode.

[2] On the "Settings" screen of the panel, tap “Advanced settings”.

[3] Tap "Actuators" to access the corresponding screen.

[4] On the "Actuators" screen, go to the "IP Actuator device setting" section, tap "Set device details".



Output Mode: AC output

Unlock Time(s): 5

Relay Type: Turn on the light

Turn on light time: 30 seconds

Link Exit Button with Lock: Power lock

☑ Report when unlock

[5] Select the device type from the drop-down list and enter the device number.

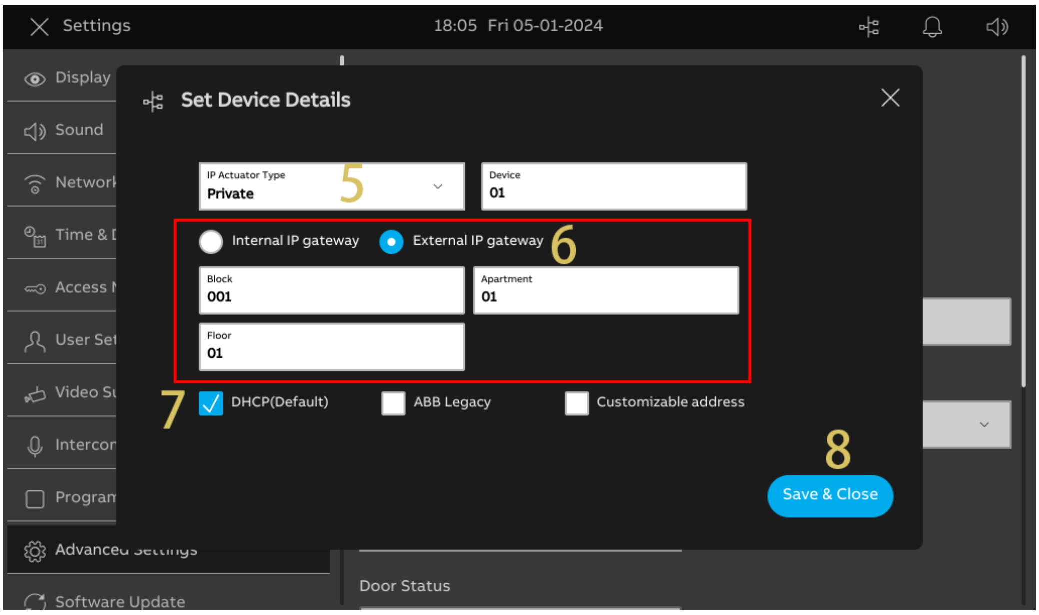
[6] Select the connection type and edit the physical address.

- If IP Actuator is connected to building network, "External IP gateway" should be selected.
- If IP Actuator is connected to private network, "Internal IP gateway" should be selected.

[7] Select the network type, it can set to "DHCP", "Customizable address" or "ABB Legacy".

- If "ABB Legacy" is selected, the IP address will be "10.0.x.x". Its network type should be the same as the SmartAP.
- If the network type of the SmartAP is set to "Legacy IP", you should select "ABB Legacy" to avoid unknown errors.

[8] Tap "Save & Close".



Set Device Details

IP Actuator Type: Private

Device: 01

○ Internal IP gateway ● External IP gateway

Block: 001

Apartment: 01

Floor: 01

☑ DHCP(Default) □ ABB Legacy □ Customizable address

10.5 Restoring to factory default

Note

Building address, signature and all parameters will be restored to the factory default settings after the reset operation.

10.5.1 Video IS

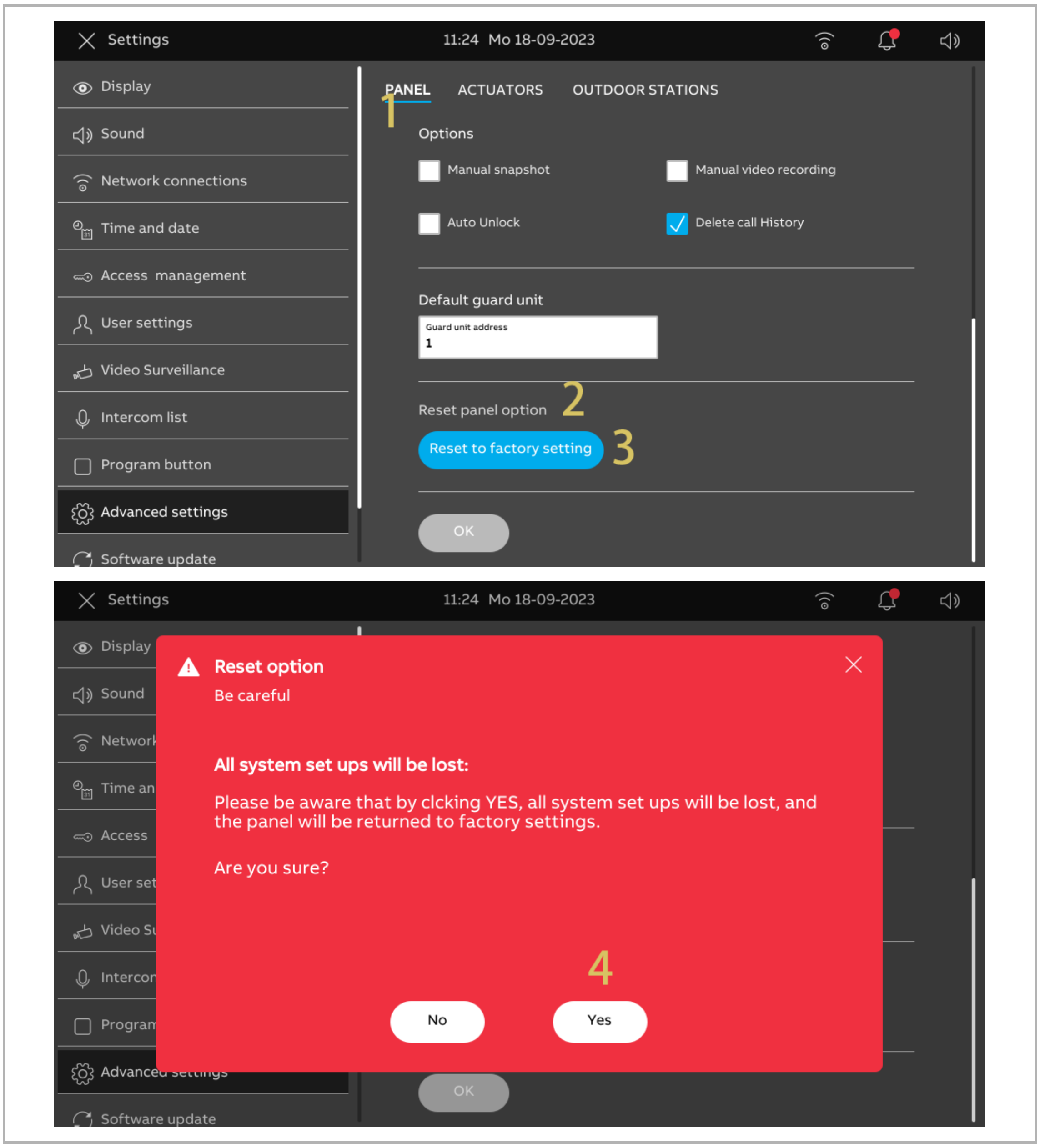
Please follow the steps below:

[1] Within 2 minutes of powering on the IS, on the "Advanced settings" screen, tap "Panel".

[2] Go to the "Reset panel option" section.

[3] Tap "Reset to factory setting".

[4] Tap "Yes".



Options

□ Manual snapshot □ Manual video recording

□ Auto Unlock ☑ Delete call History

Default guard unit

Guard unit address: 1

Reset panel option

Reset option

Be careful

All system set ups will be lost:

Please be aware that by clcking YES, all system set ups will be lost, and the panel will be returned to factory settings.

Are you sure?

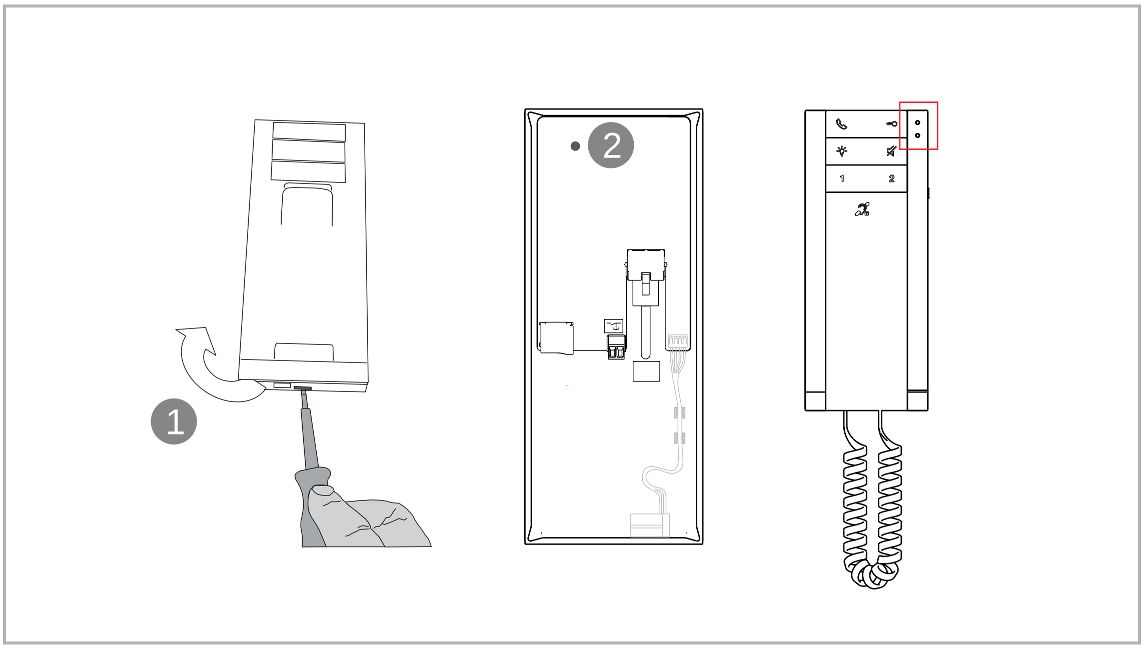
10.5.2 Audio IS

Please follow the steps below:

[1] Disassemble the upper part from the bottom part by using a screwdriver.

[2] Within 2 minutes of powering on the Audio IP, press and hold the reset button (located on the upper part) for 3 seconds until the 2 LED indicators turn on and then off.

[3] After a while, the 2 LED indicators will flash to indicate the initial status.

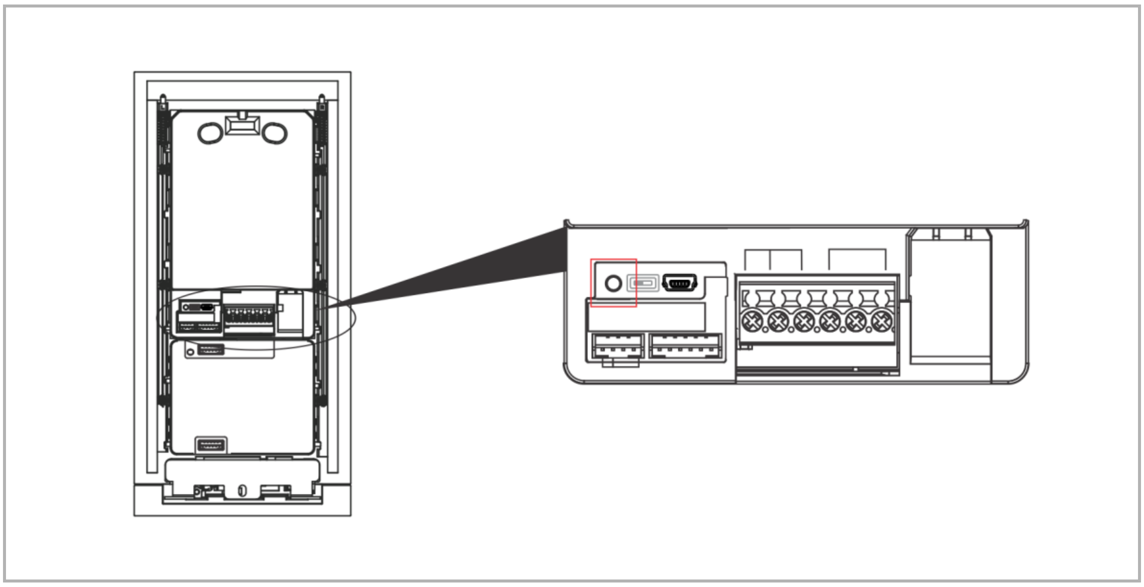


10.5.3 IP Touch 5 OS

Please follow the steps below:

[1] Power on the OS, wait until all 3 LED indicators go out.

[2] Within 2 minutes of powering on the OS, press and hold the reset button for 10 seconds until the 3 LED indicators are lit continuously.

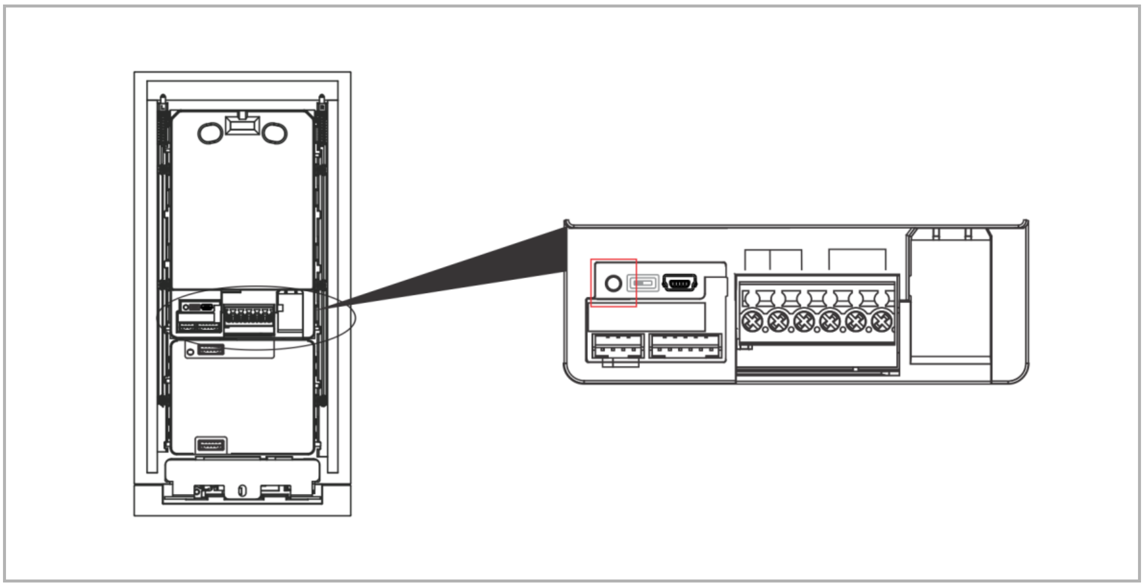


10.5.4 IP Pushbutton OS

Please follow the steps below:

[1] Power on the OS, wait until all 3 LED indicators go out.

[2] Within 2 minutes of powering on the OS, press and hold the reset button for 10 seconds until the 3 LED indicators are lit continuously.



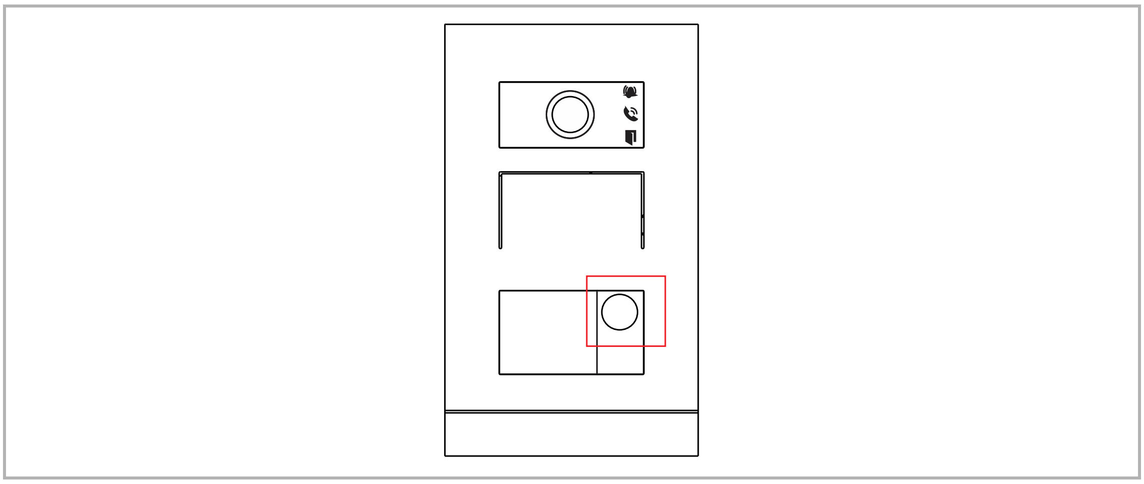
10.5.5 Mini OS

Please follow the steps below:

[1] Power on the mini OS with IC, wait until all 3 LED indicators go out.

[2] Within 2 minutes of powering on the mini OS with IC, press and hold the first pushbutton for 5 seconds until all 3 LED indicators flash.

[3] Press and hold the first pushbutton again for the 10 seconds until the mini OS with IC emits a "di" sound and the 3 LED indicators go out.

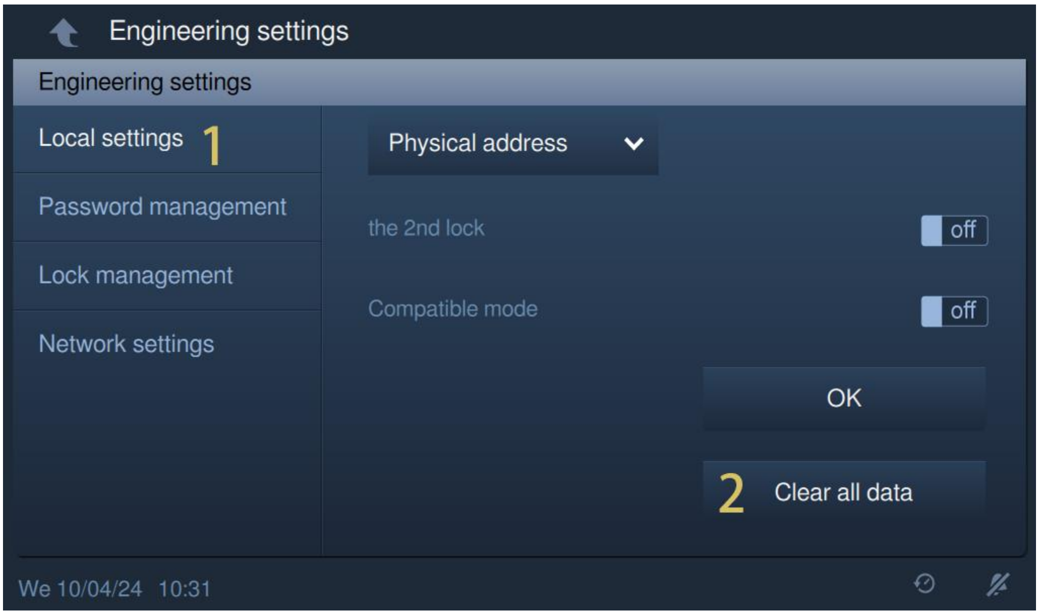


10.5.6 Guard Unit

Please follow the steps below:

[1] Within 2 minutes of powering on the Guard Unit, on the "Engineering settings" screen, tap "Local settings".

[2] Tap "Clear all data".



the 2nd lock off

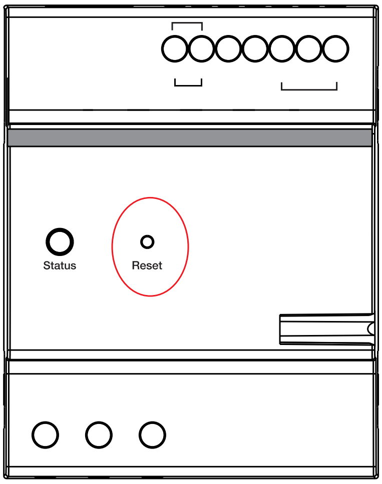
Compatible mode off

10.5.7 IP Actuator

Please follow the steps below:

[1] Within 2 minutes of powering on the IP Actuator, press and hold the reset button for 10 seconds until the indicator goes out.

[2] After a while, the indicator flashes green again.

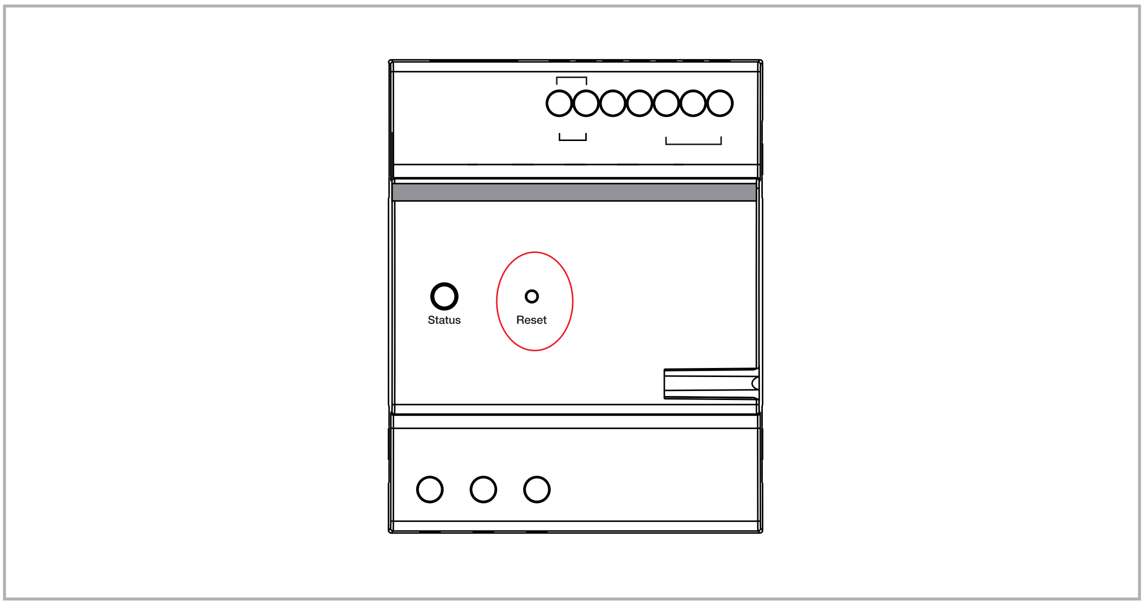


10.5.8 IP Elevator Controller

Please follow the steps below:

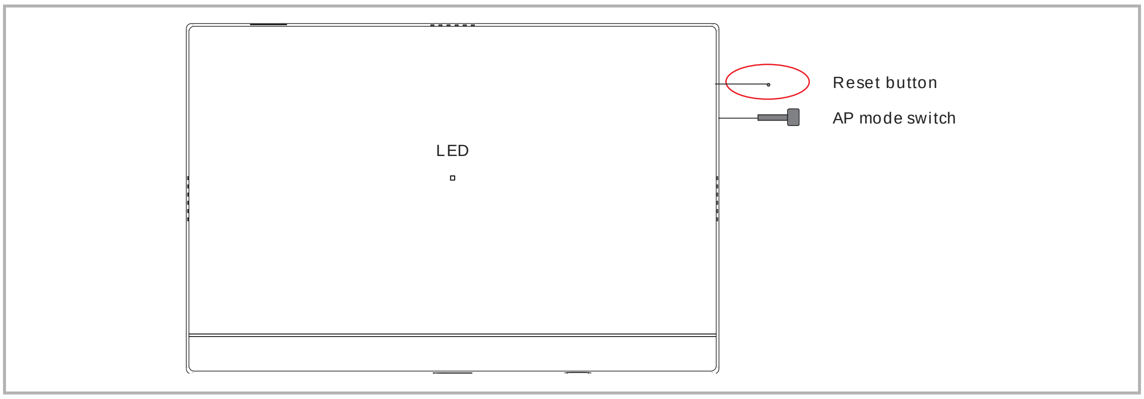
[1] Within 2 minutes of powering on the IP Elevator Controller, press and hold the reset button for 10 seconds until the indicator goes out.

[2] After a while, the indicator flashes green again.



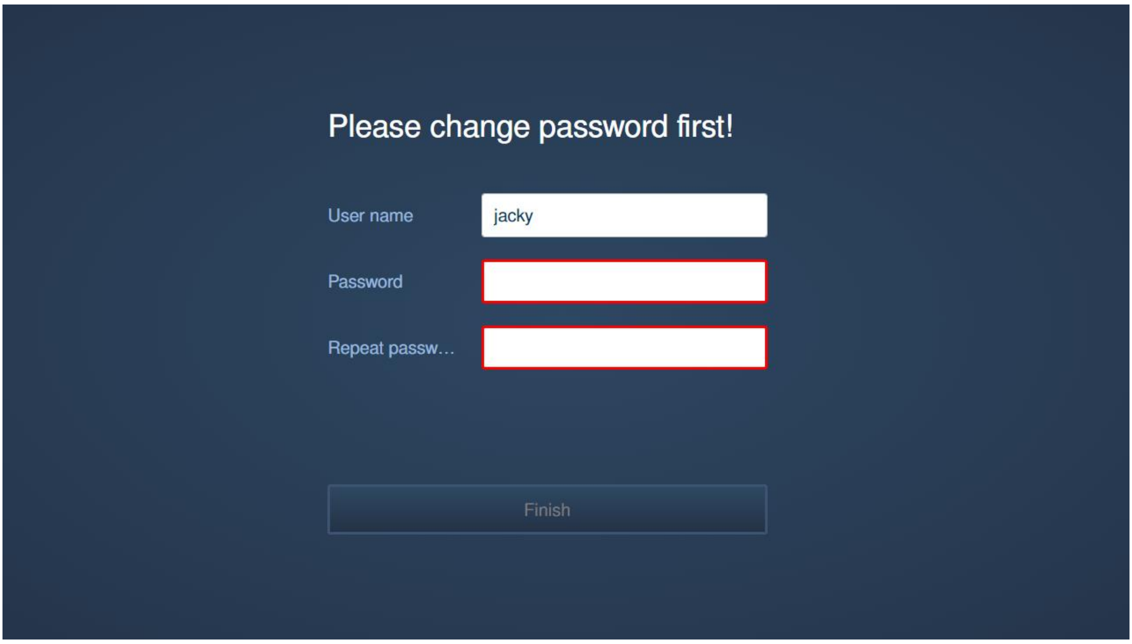
10.6 Resetting the password for the primary admin

Press and hold the reset button for 10 seconds to reset the password for the primary admin and reset AP password in the same time.



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 change password first!

User name: jacky

Password:

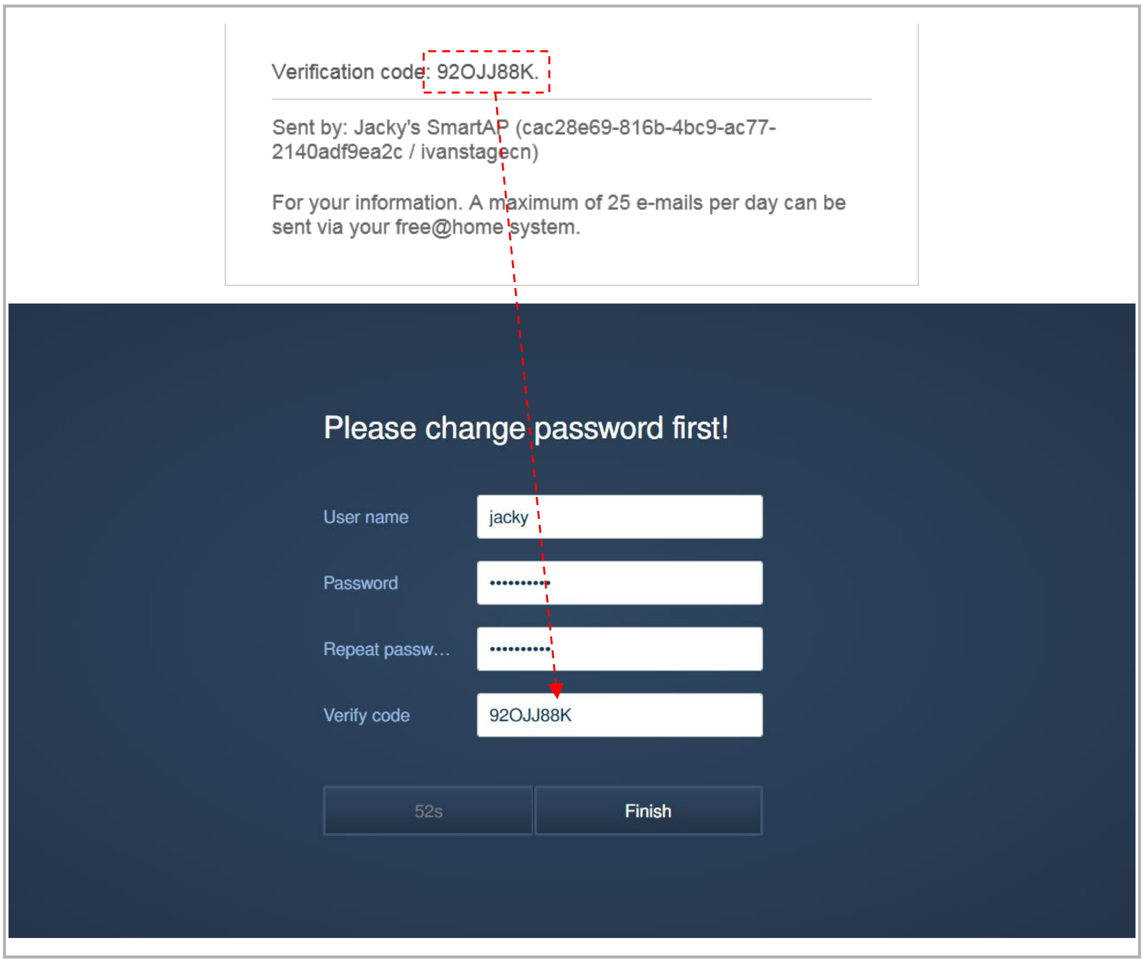
Repeat passw…:

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

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



Verification code: 92OJJ88K.

Sent by: Jacky's SmartAP (cac28e69-816b-4bc9-ac77-2140adf9ea2c / ivanstagecn)

For your information. A maximum of 25 e-mails per day can be sent via your free@home system.

Please change password first!

User name: jacky

Password: ••••••••••

Repeat passw…: ••••••••••

Verify code: 92OJJ88K

10.7 Configuring the IP mode

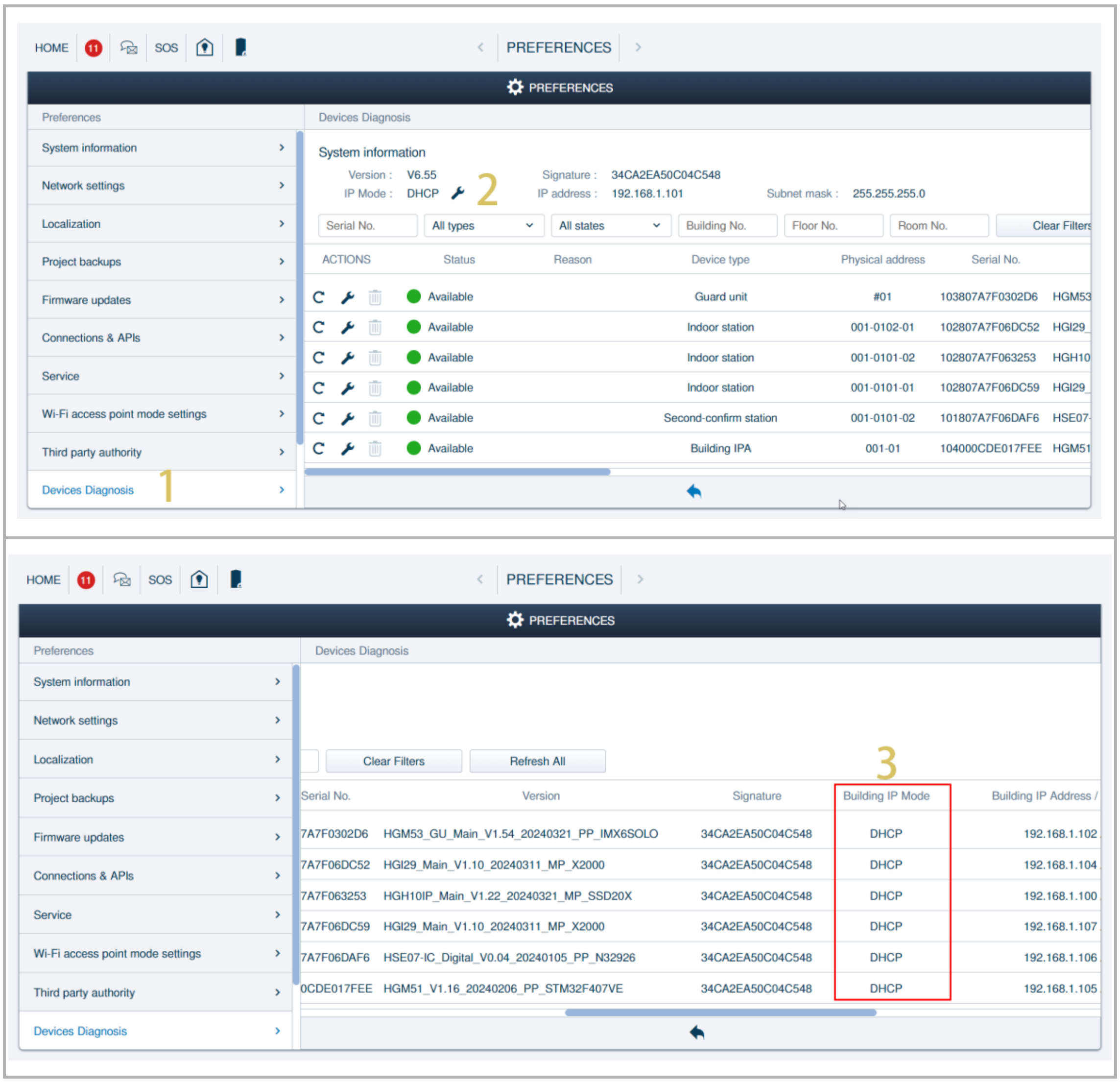
10.7.1 Viewing the IP mode

Please follow the steps below:

[1] On the "Preferences" screen, click "Devices Diagnosis".

[2] Display the IP mode of the SmartAP.

[3] Drag the scroll bar to the right to view the IP mode of the designated device.



System information

Version : V6.55

IP Mode : DHCP

Signature : 34CA2EA50C04C548

IP address : 192.168.1.101

Subnet mask : 255.255.255.0

ACTIONS	Status	Reason	Device type	Physical address	Serial No.	
	Available		Guard unit	#01	103807A7F0302D6	HGM53
	Available		Indoor station	001-0102-01	102807A7F06DC52	HGI29_
	Available		Indoor station	001-0101-02	102807A7F063253	HGH10
	Available		Indoor station	001-0101-01	102807A7F06DC59	HGI29_
	Available		Second-confirm station	001-0101-02	101807A7F06DAF6	HSE07-
	Available		Building IPA	001-01	104000CDE017FEE	HGM51

Serial No.	Version	Signature	Building IP Mode	Building IP Address /
7A7F0302D6	HGM53_GU_Main_V1.54_20240321_PP_IMX6SOLO	34CA2EA50C04C548	DHCP	192.168.1.102
7A7F06DC52	HGI29_Main_V1.10_20240311_MP_X2000	34CA2EA50C04C548	DHCP	192.168.1.104
7A7F063253	HGH10IP_Main_V1.22_20240321_MP_SSD20X	34CA2EA50C04C548	DHCP	192.168.1.100
7A7F06DC59	HGI29_Main_V1.10_20240311_MP_X2000	34CA2EA50C04C548	DHCP	192.168.1.107
7A7F06DAF6	HSE07-IC_Digital_V0.04_20240105_PP_N32926	34CA2EA50C04C548	DHCP	192.168.1.106
0CDE017FEE	HGM51_V1.16_20240206_PP_STM32F407VE	34CA2EA50C04C548	DHCP	192.168.1.105

10.7.2 Changing the IP mode from "DHCP" to "Legacy IP" for all devices

Changing the IP mode of the SmartAP will change the IP mode of all devices in the system.

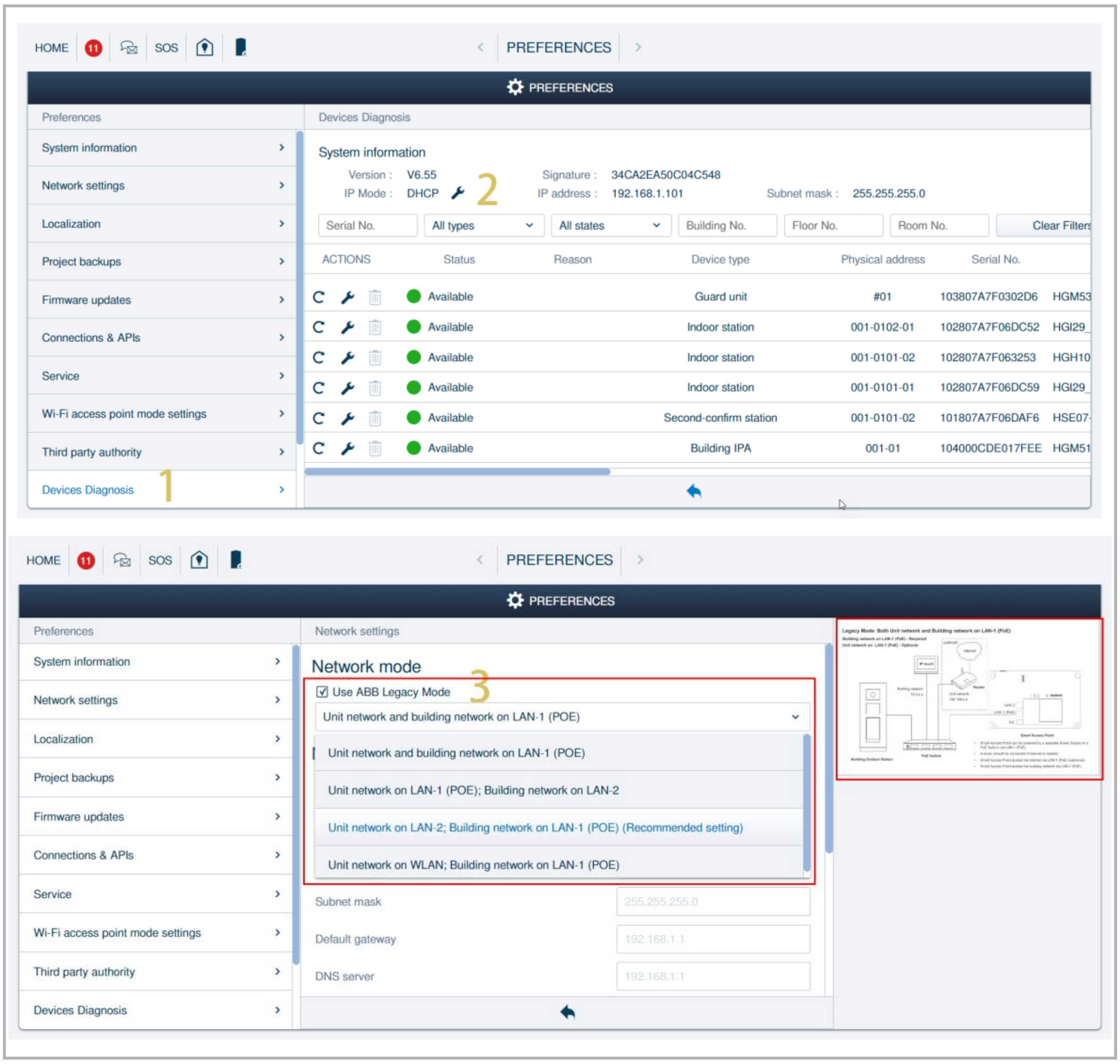
Please follow the steps below:

[1] On the "Preferences" screen, click "Devices Diagnosis".

[2] Click " 🔧 " to go to "Network settings" screen.

[3] On the "Network settings" screen, tick the check box to enable "Legacy IP".

- There are 4 network connections type could be select from the drop-down list. Click the diagram on the right to view the details.



Devices Diagnosis

System information

Version : V6.55
IP Mode : DHCP 🔧
Signature : 34CA2EA50C04C548
IP address : 192.168.1.101
Subnet mask : 255.255.255.0

ACTIONS	Status	Reason	Device type	Physical address	Serial No.	
C 🔧 🗑	● Available		Guard unit	#01	103807A7F0302D6	HGM53
C 🔧 🗑	● Available		Indoor station	001-0102-01	102807A7F06DC52	HGI29_
C 🔧 🗑	● Available		Indoor station	001-0101-02	102807A7F063253	HGH10
C 🔧 🗑	● Available		Indoor station	001-0101-01	102807A7F06DC59	HGI29_
C 🔧 🗑	● Available		Second-confirm station	001-0101-02	101807A7F06DAF6	HSE07-
C 🔧 🗑	● Available		Building IPA	001-01	104000CDE017FEE	HGM51

Network settings

Network mode

☑ Use ABB Legacy Mode

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

- Unit network and building network on LAN-1 (POE)
- Unit network on LAN-1 (POE); Building network on LAN-2
- Unit network on LAN-2; Building network on LAN-1 (POE) (Recommended setting)
- Unit network on WLAN; Building network on LAN-1 (POE)

Subnet mask: 255.255.255.0

Default gateway: 192.168.1.1

DNS server: 192.168.1.1

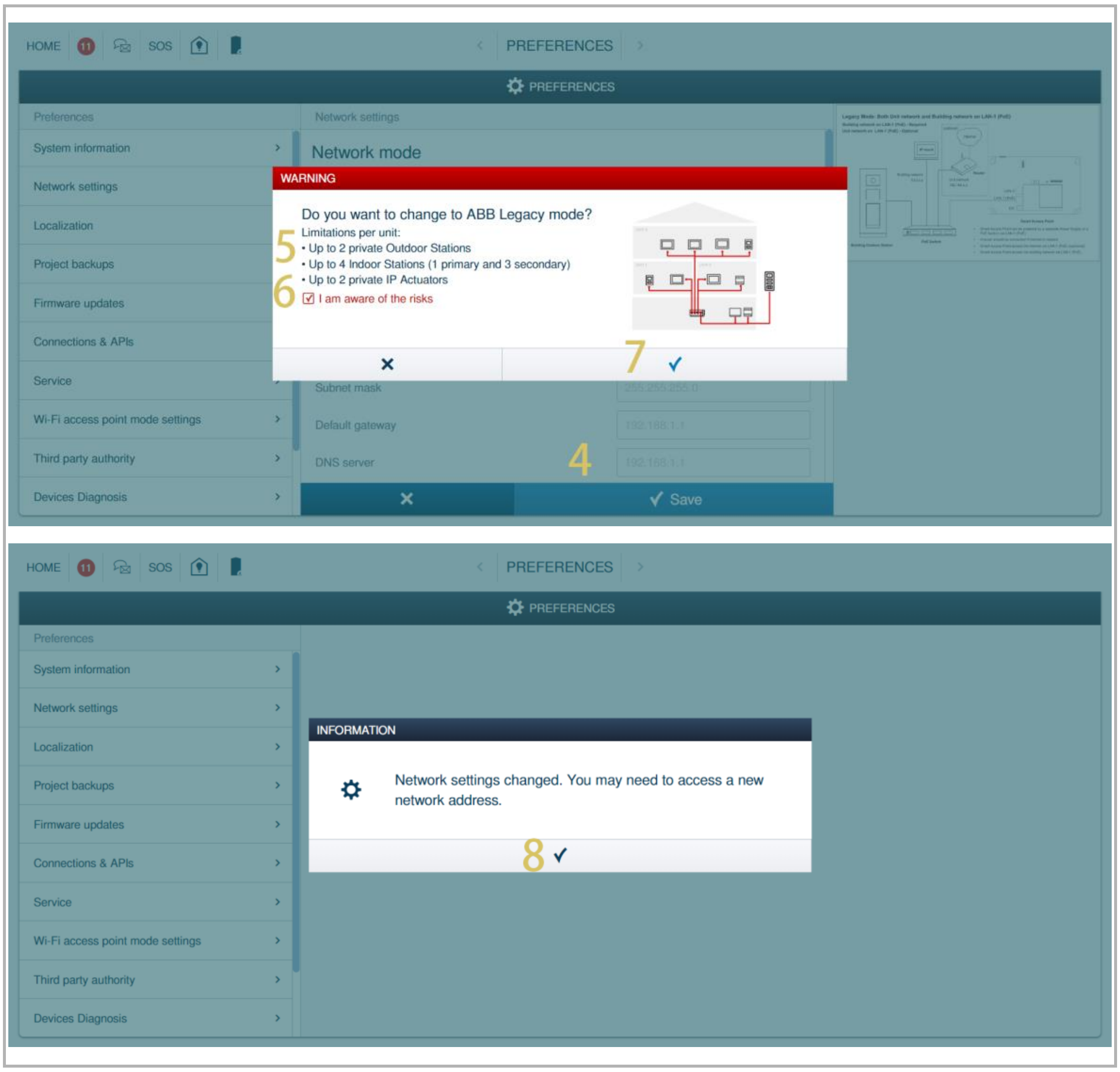
[4] Click "Save" to save the settings.

[5] A warning window will pop up to display the notice.

[6] Tick the check box if you want to continue.

[7] Click " √ " to continue.

[8] Click " √ " to access the SmartAP again.



WARNING

Do you want to change to ABB Legacy mode?

Limitations per unit:

- Up to 2 private Outdoor Stations
- Up to 4 Indoor Stations (1 primary and 3 secondary)
- Up to 2 private IP Actuators

☑ I am aware of the risks

× ✓

INFORMATION

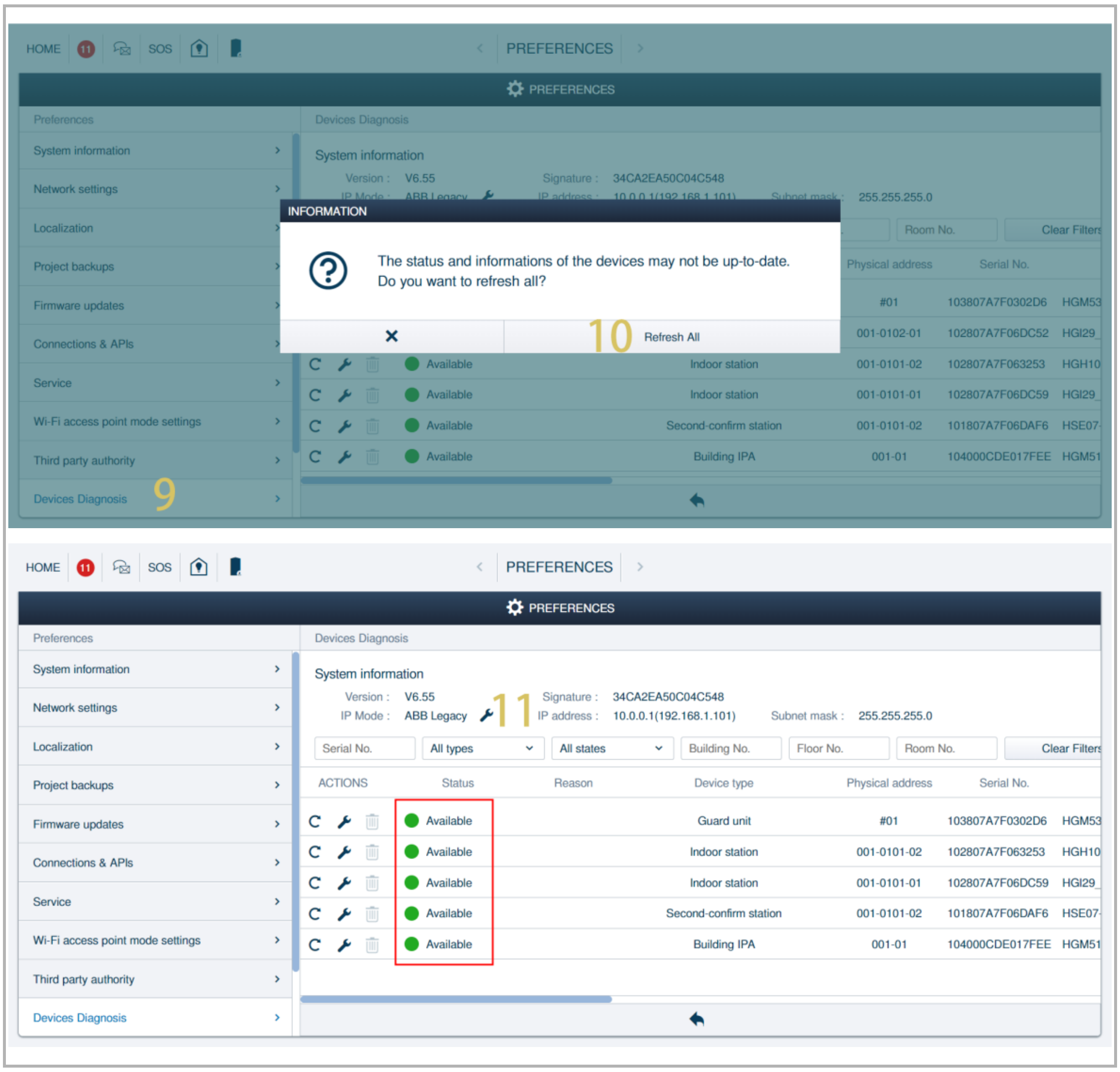
Network settings changed. You may need to access a new network address.

✓

[9] On the "Preferences" screen, click "Devices Diagnosis".

[10]Click "Refresh All".

[11]"ABB Legacy" will be displayed on the screen and all the devices will be available after this change.



System information

Version : V6.55 Signature : 34CA2EA50C04C548

IP Mode : ABB Legacy IP address : 10.0.0.1(192.168.1.101) Subnet mask : 255.255.255.0

INFORMATION

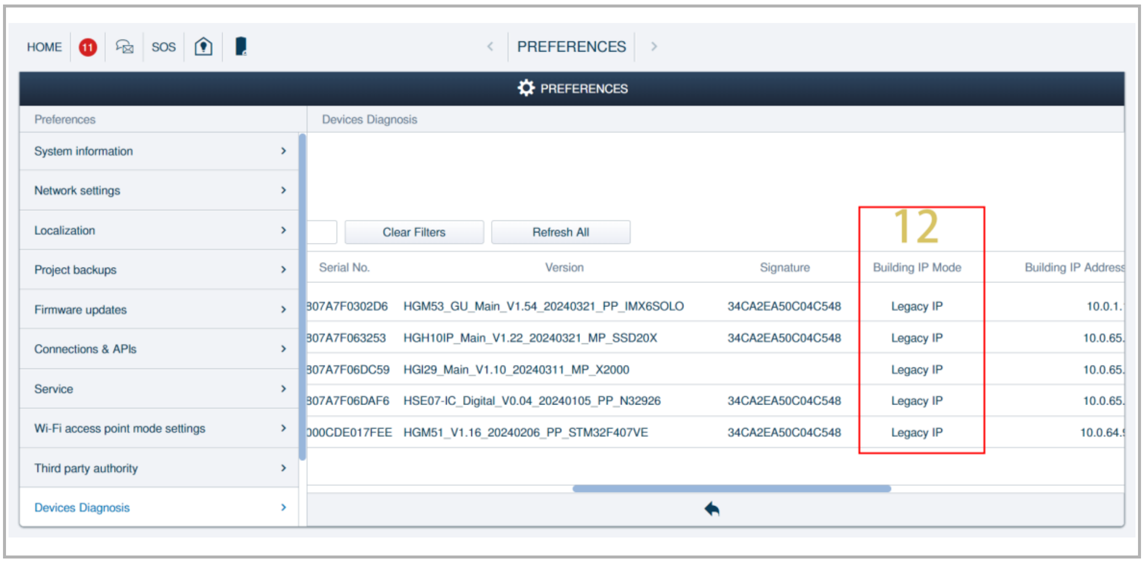
The status and informations of the devices may not be up-to-date.
Do you want to refresh all?

✕ Refresh All

Status	Device type	Physical address	Serial No.	
		#01	103807A7F0302D6	HGM53
		001-0102-01	102807A7F06DC52	HGI29_
● Available	Indoor station	001-0101-02	102807A7F063253	HGH10
● Available	Indoor station	001-0101-01	102807A7F06DC59	HGI29_
● Available	Second-confirm station	001-0101-02	101807A7F06DAF6	HSE07-
● Available	Building IPA	001-01	104000CDE017FEE	HGM51

ACTIONS	Status	Reason	Device type	Physical address	Serial No.	
	● Available		Guard unit	#01	103807A7F0302D6	HGM53
	● Available		Indoor station	001-0101-02	102807A7F063253	HGH10
	● Available		Indoor station	001-0101-01	102807A7F06DC59	HGI29_
	● Available		Second-confirm station	001-0101-02	101807A7F06DAF6	HSE07-
	● Available		Building IPA	001-01	104000CDE017FEE	HGM51

[12]The IP mode of all the devices will be changed to "Legacy IP" at the same time.



Serial No.	Version	Signature	Building IP Mode	Building IP Address
307A7F0302D6	HGM53_GU_Main_V1.54_20240321_PP_IMX6SOLO	34CA2EA50C04C548	Legacy IP	10.0.1.
307A7F063253	HGH10IP_Main_V1.22_20240321_MP_SSD20X	34CA2EA50C04C548	Legacy IP	10.0.65.
307A7F06DC59	HGI29_Main_V1.10_20240311_MP_X2000		Legacy IP	10.0.65.
307A7F06DAF6	HSE07-IC_Digital_V0.04_20240105_PP_N32926	34CA2EA50C04C548	Legacy IP	10.0.65.
000CDE017FEE	HGM51_V1.16_20240206_PP_STM32F407VE	34CA2EA50C04C548	Legacy IP	10.0.64.

10.7.3 Changing the IP mode from "Legacy IP" to "DHCP" for all devices

Changing the IP mode of the SmartAP will change the IP mode of all devices on the system.

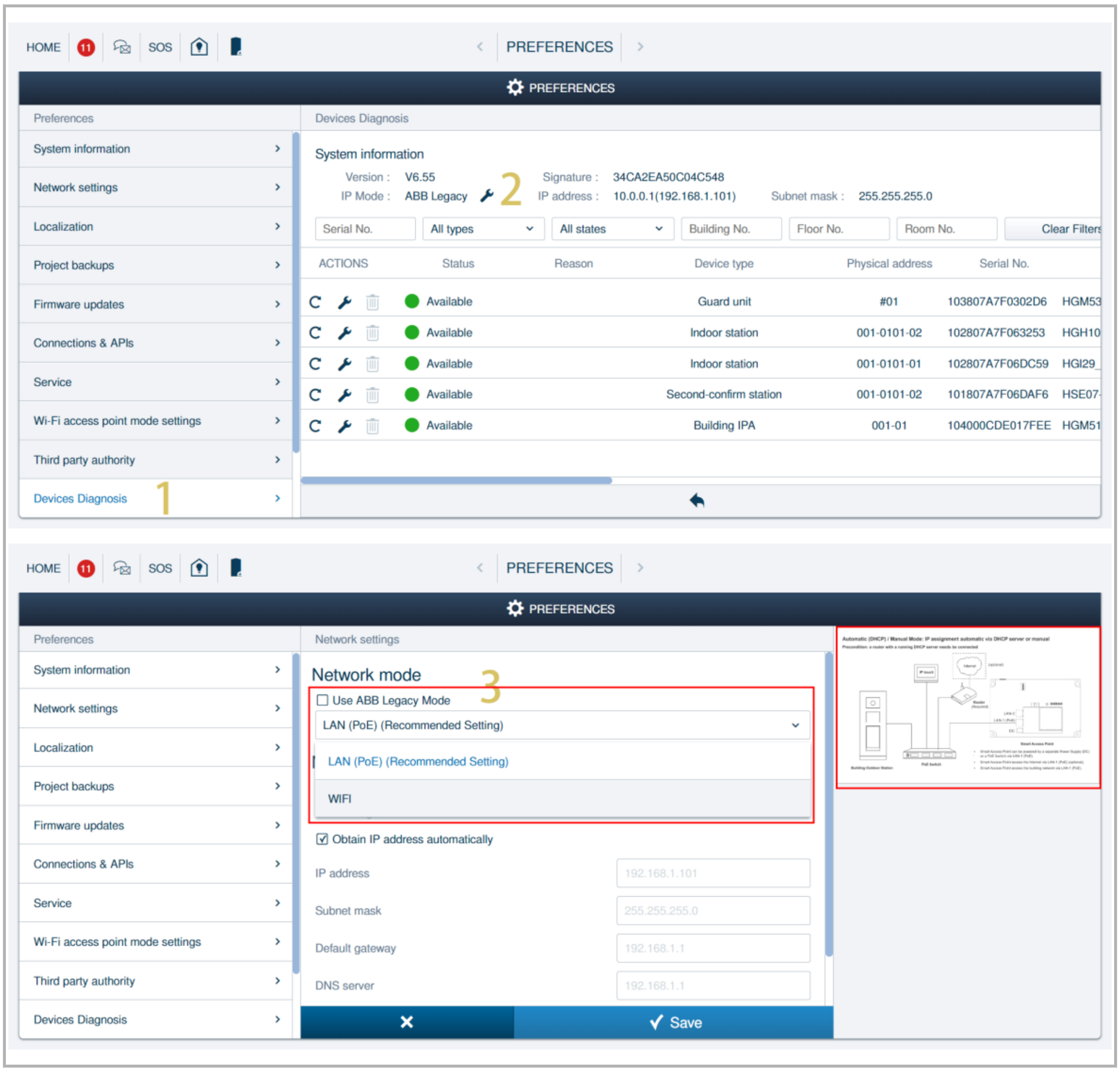
Please follow the steps below:

[1] On the "Preferences" screen, click "Devices Diagnosis".

[2] Click " 🔧 " to go to "Network settings" screen.

[3] On the "Network settings" screen, untick the check box to disable "Legacy IP".

- There are 2 network connections type could be select from the drop-down list. Click the diagram on the right to view the details.



Devices Diagnosis

System information

Version : V6.55
IP Mode : ABB Legacy 🔧
Signature : 34CA2EA50C04C548
IP address : 10.0.0.1(192.168.1.101)
Subnet mask : 255.255.255.0

Serial No. | All types | All states | Building No. | Floor No. | Room No.

ACTIONS	Status	Reason	Device type	Physical address	Serial No.	
	● Available		Guard unit	#01	103807A7F0302D6	HGM53
	● Available		Indoor station	001-0101-02	102807A7F063253	HGH10
	● Available		Indoor station	001-0101-01	102807A7F06DC59	HGI29_
	● Available		Second-confirm station	001-0101-02	101807A7F06DAF6	HSE07-
	● Available		Building IPA	001-01	104000CDE017FEE	HGM51

Network settings

Network mode

□ Use ABB Legacy Mode

LAN (PoE) (Recommended Setting)

LAN (PoE) (Recommended Setting)

WIFI

☑ Obtain IP address automatically

IP address: 192.168.1.101

Subnet mask: 255.255.255.0

Default gateway: 192.168.1.1

DNS server: 192.168.1.1

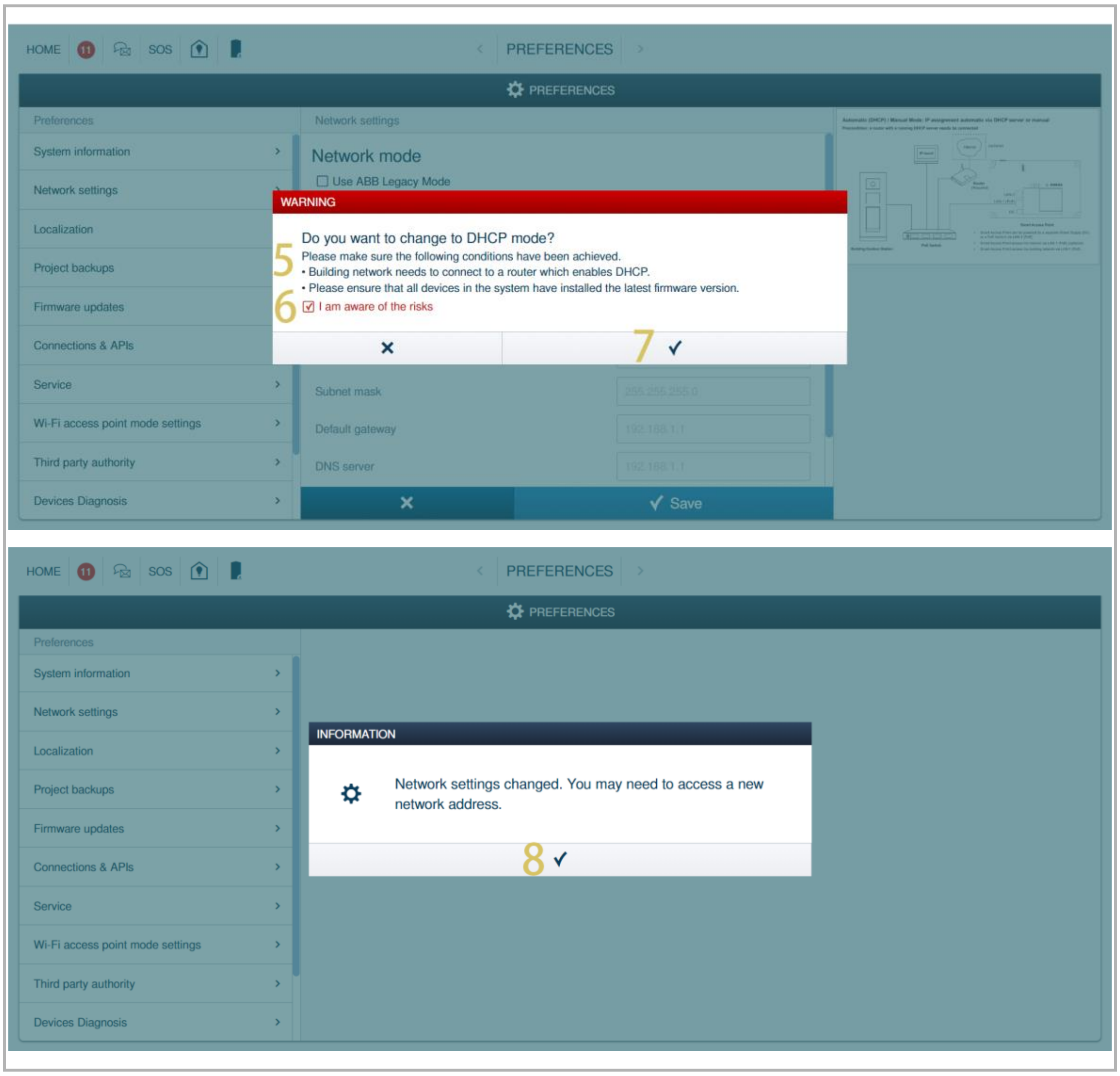
[4] Click "Save" to save the settings.

[5] A warning window will pop up to display the notice.

[6] Tick the check box if you want to continue.

[7] Click " √ " to continue.

[8] Click " √ " to access the SmartAP again.



WARNING

Do you want to change to DHCP mode?
Please make sure the following conditions have been achieved.
• Building network needs to connect to a router which enables DHCP.
• Please ensure that all devices in the system have installed the latest firmware version.
☑ I am aware of the risks

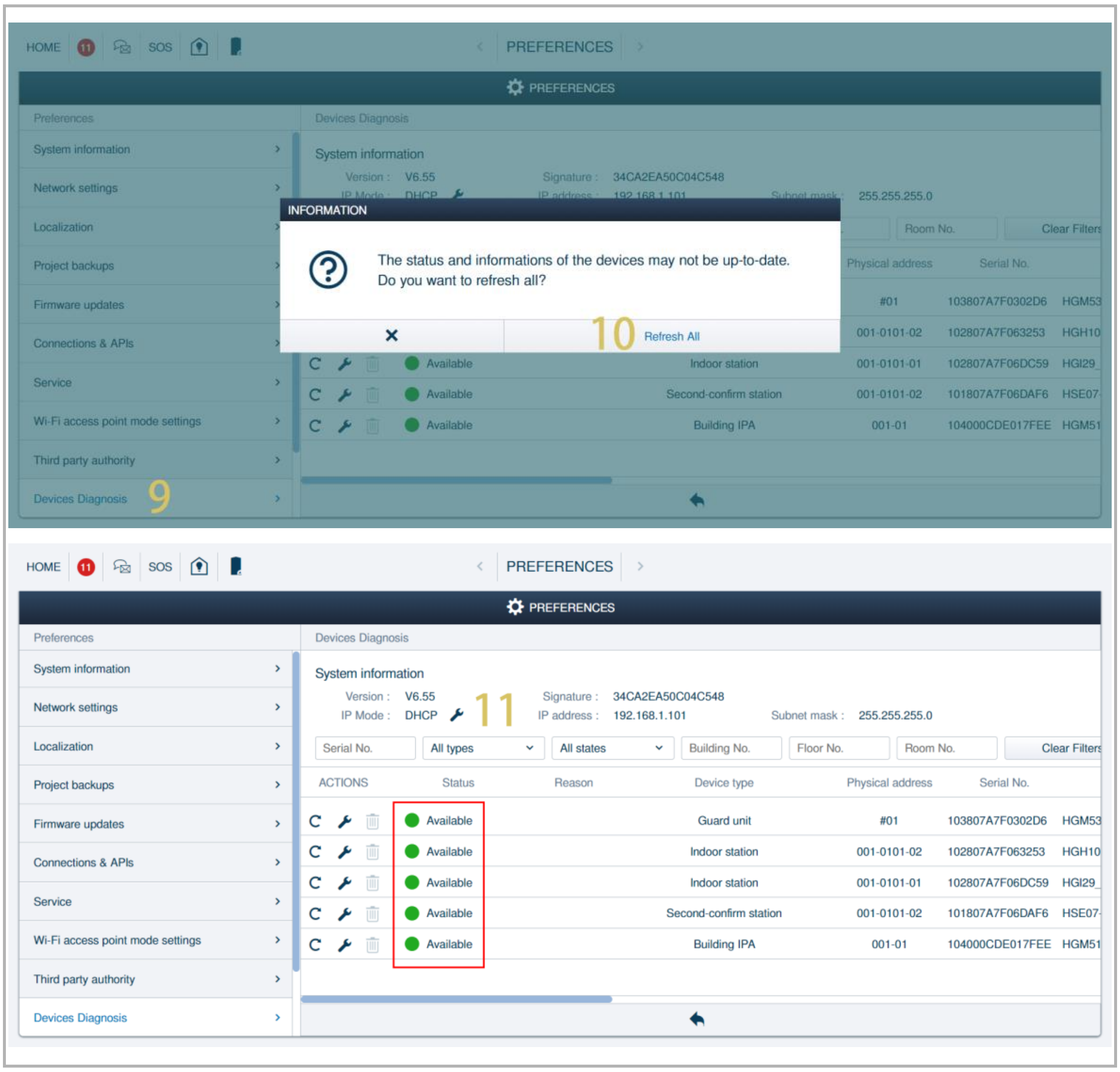
INFORMATION

Network settings changed. You may need to access a new network address.

[9] On the "Preferences" screen, click "Devices Diagnosis".

[10]Click "Refresh All".

[11]"DHCP" will be displayed on the screen and all the devices will be available after this change.



INFORMATION

The status and informations of the devices may not be up-to-date.
Do you want to refresh all?

× | Refresh All

Devices Diagnosis

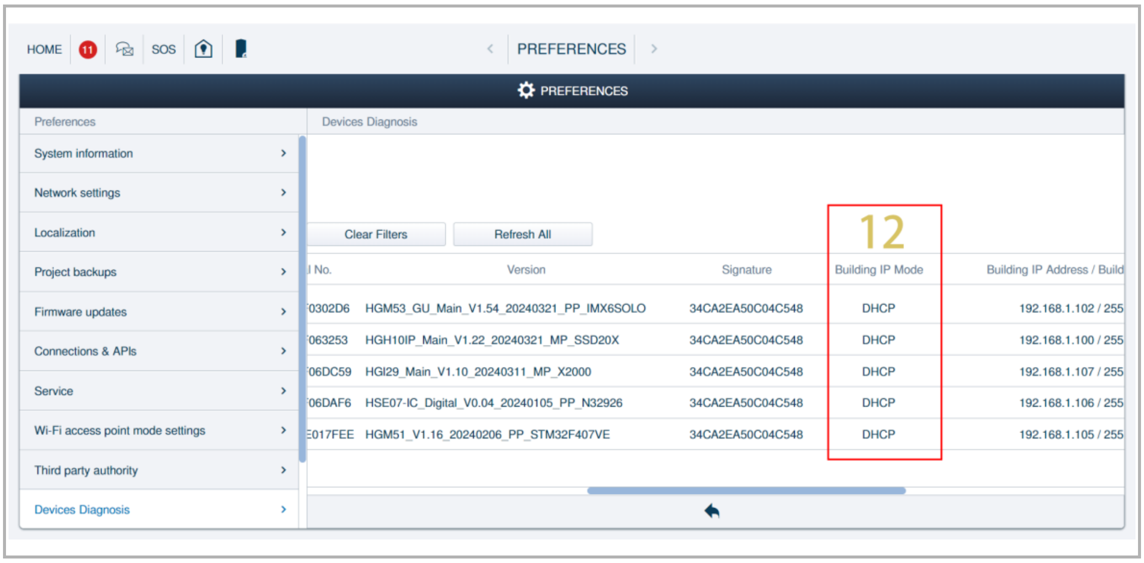
System information

Version : V6.55
IP Mode : DHCP
Signature : 34CA2EA50C04C548
IP address : 192.168.1.101
Subnet mask : 255.255.255.0

Serial No. | All types | All states | Building No. | Floor No. | Room No. | Clear Filters

ACTIONS	Status	Reason	Device type	Physical address	Serial No.	
	● Available		Guard unit	#01	103807A7F0302D6	HGM53
	● Available		Indoor station	001-0101-02	102807A7F063253	HGH10
	● Available		Indoor station	001-0101-01	102807A7F06DC59	HGI29_
	● Available		Second-confirm station	001-0101-02	101807A7F06DAF6	HSE07-
	● Available		Building IPA	001-01	104000CDE017FEE	HGM51

[12]The IP mode of all the devices will be changed to "DHCP" at the same time.



l No.	Version	Signature	Building IP Mode	Building IP Address / Build
0302D6	HGM53_GU_Main_V1.54_20240321_PP_IMX6SOLO	34CA2EA50C04C548	DHCP	192.168.1.102 / 255
063253	HGH10IP_Main_V1.22_20240321_MP_SSD20X	34CA2EA50C04C548	DHCP	192.168.1.100 / 255
06DC59	HGI29_Main_V1.10_20240311_MP_X2000	34CA2EA50C04C548	DHCP	192.168.1.107 / 255
06DAF6	HSE07-IC_Digital_V0.04_20240105_PP_N32926	34CA2EA50C04C548	DHCP	192.168.1.106 / 255
E017FEE	HGM51_V1.16_20240206_PP_STM32F407VE	34CA2EA50C04C548	DHCP	192.168.1.105 / 255

10.7.4 Changing IP mode for the designated device

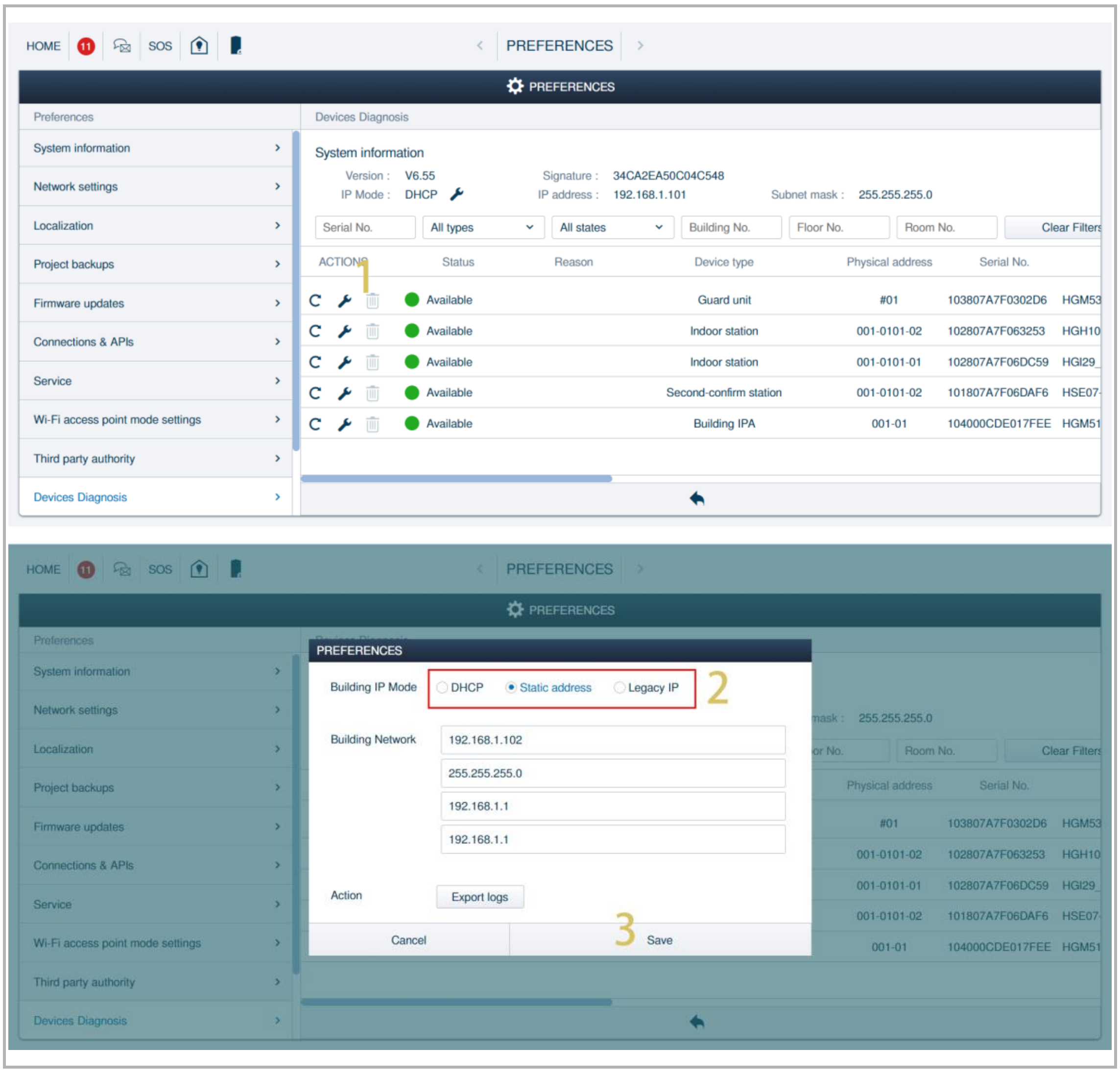
Please follow the steps below:

[1] On the "Device Diagnosis" screen, click " 🔧 ".

[2] Changing the IP mode.

- If "Static address" is selected, you need to enter the IP address manually or accept the default value.

[3] Click "Save".



Devices Diagnosis

System information

Version : V6.55 Signature : 34CA2EA50C04C548

IP Mode : DHCP 🔧 IP address : 192.168.1.101 Subnet mask : 255.255.255.0

Serial No. | All types | All states | Building No. | Floor No. | Room No. | Clear Filters

ACTIONS	Status	Reason	Device type	Physical address	Serial No.	
C 🔧 🗑	● Available		Guard unit	#01	103807A7F0302D6	HGM53
C 🔧 🗑	● Available		Indoor station	001-0101-02	102807A7F063253	HGH10
C 🔧 🗑	● Available		Indoor station	001-0101-01	102807A7F06DC59	HGI29_
C 🔧 🗑	● Available		Second-confirm station	001-0101-02	101807A7F06DAF6	HSE07-
C 🔧 🗑	● Available		Building IPA	001-01	104000CDE017FEE	HGM51

PREFERENCES

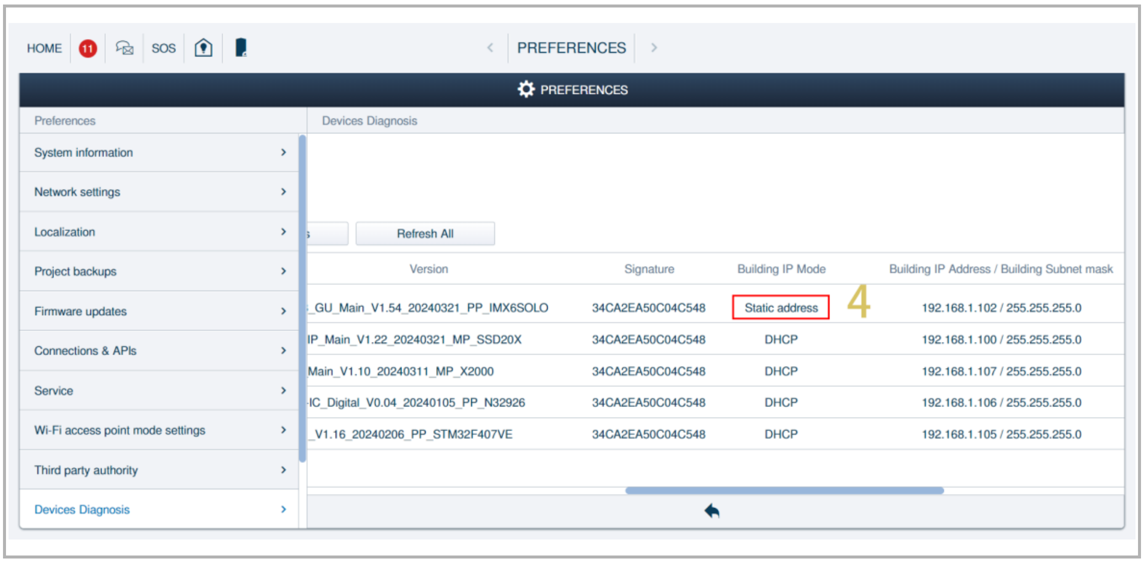
Building IP Mode: ○ DHCP ● Static address ○ Legacy IP

Building Network: 192.168.1.102
255.255.255.0
192.168.1.1
192.168.1.1

Action: Export logs

Cancel Save

[4] New IP mode of the designated device will be displayed on the screen.



Version	Signature	Building IP Mode	Building IP Address / Building Subnet mask
_GU_Main_V1.54_20240321_PP_IMX6SOLO	34CA2EA50C04C548	Static address	192.168.1.102 / 255.255.255.0
IP_Main_V1.22_20240321_MP_SSD20X	34CA2EA50C04C548	DHCP	192.168.1.100 / 255.255.255.0
Main_V1.10_20240311_MP_X2000	34CA2EA50C04C548	DHCP	192.168.1.107 / 255.255.255.0
IC_Digital_V0.04_20240105_PP_N32926	34CA2EA50C04C548	DHCP	192.168.1.106 / 255.255.255.0
_V1.16_20240206_PP_STM32F407VE	34CA2EA50C04C548	DHCP	192.168.1.105 / 255.255.255.0

IP mode matching

- If the IP mode of the SmartAP is set to "DHCP", the IP mode the designated device could be "DHCP" or "Static address".
- If the IP mode of the SmartAP is set to "Legacy IP", the IP mode the designated device must be "Legacy IP" as well.
- If the IP mode is not matched between the designated device and the SmartAP, "Error" will be displayed on the screen.

10.8 Managing the trusted devices

10.8.1 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 have been signed on the SmartAP.
- If the Indoor Station has been added on the trusted list of the Outdoor Station.

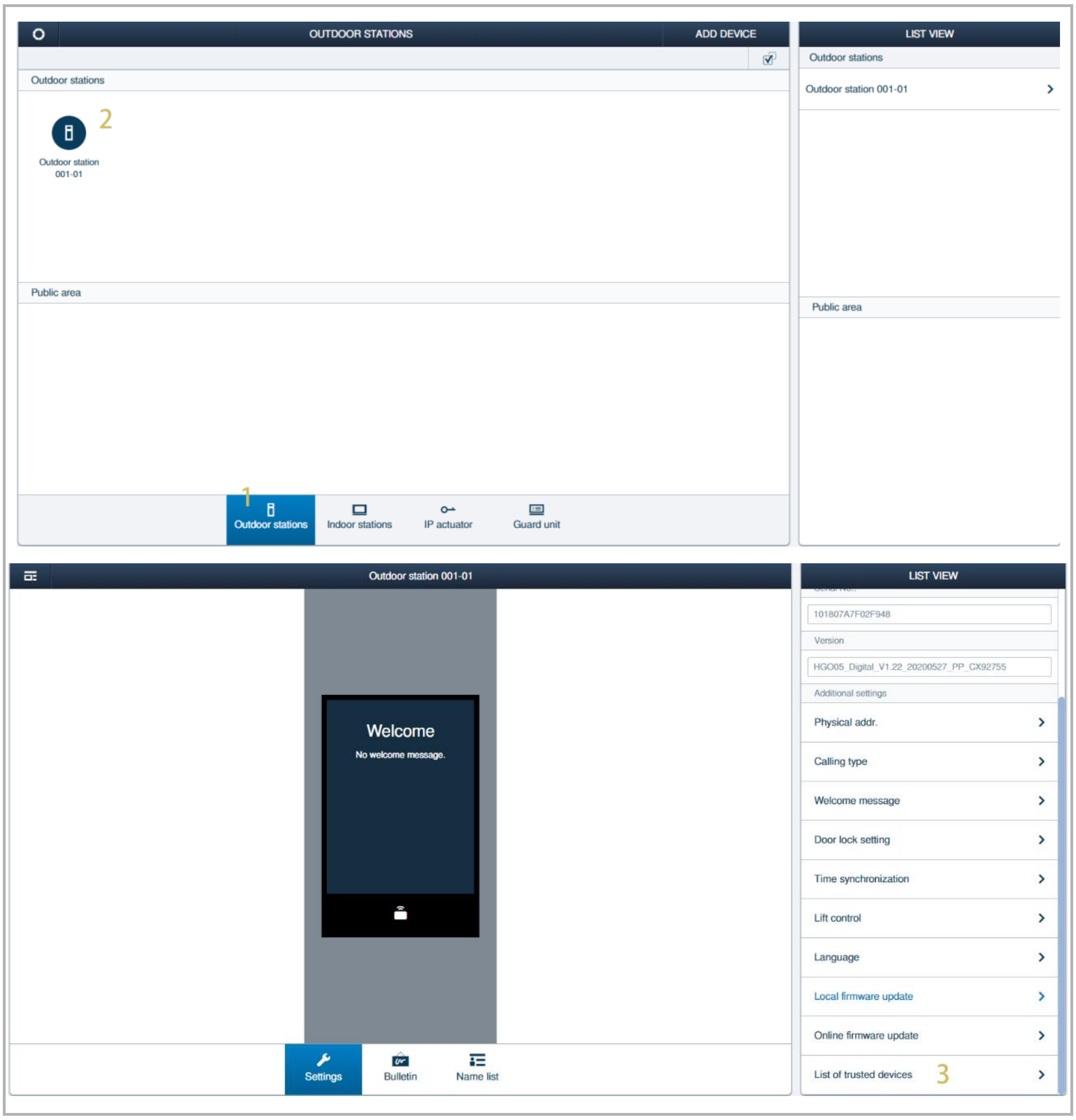
1. Adding the trusted devices

Please follow the steps below:

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

[2] Click the designated Outdoor Station.

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



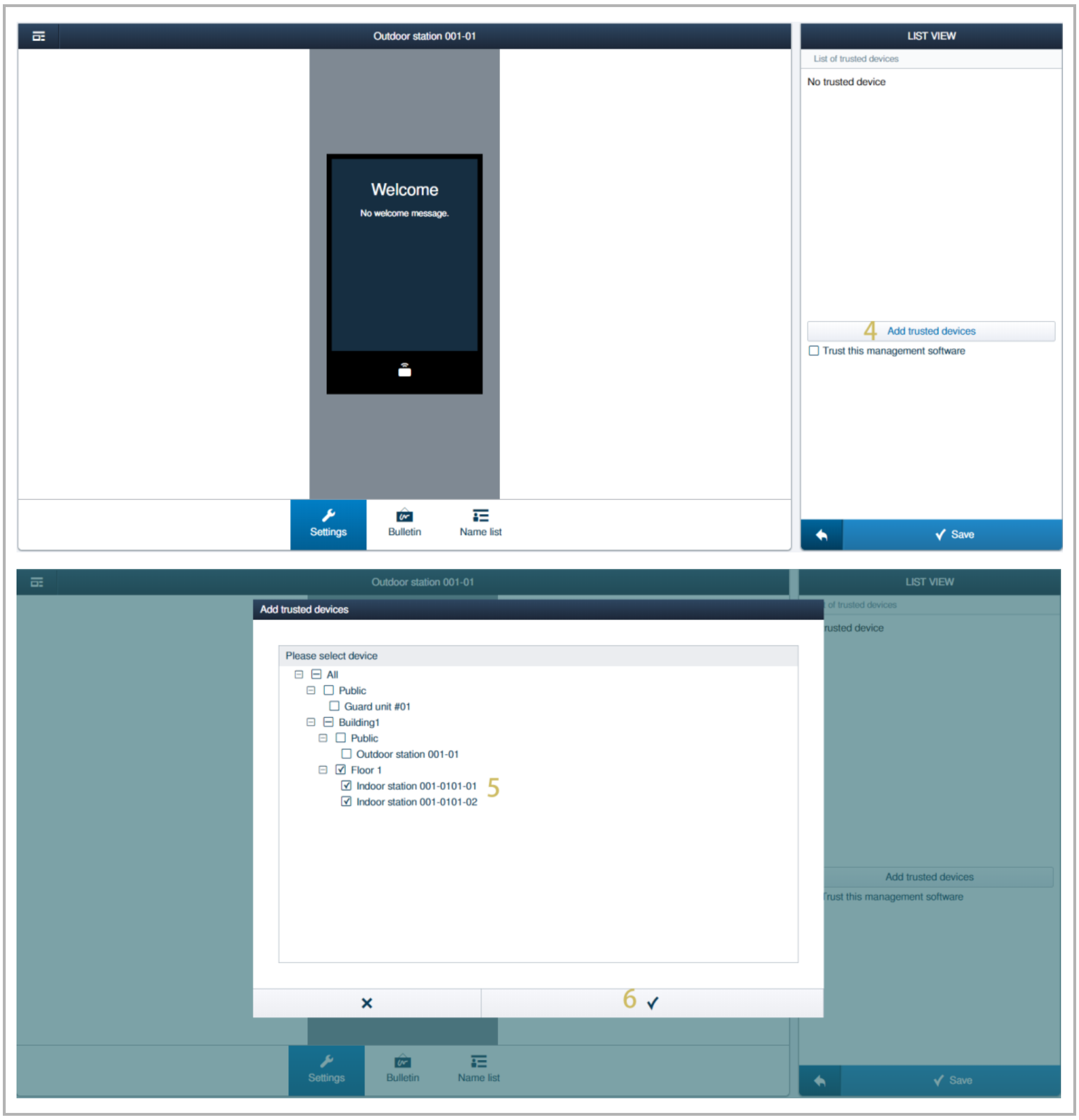
Serial No.: 101807A7F02F948

Version: HGO05_Digital_V1.22_20200527_PP_CX92755

[4] Click "Add trusted devices".

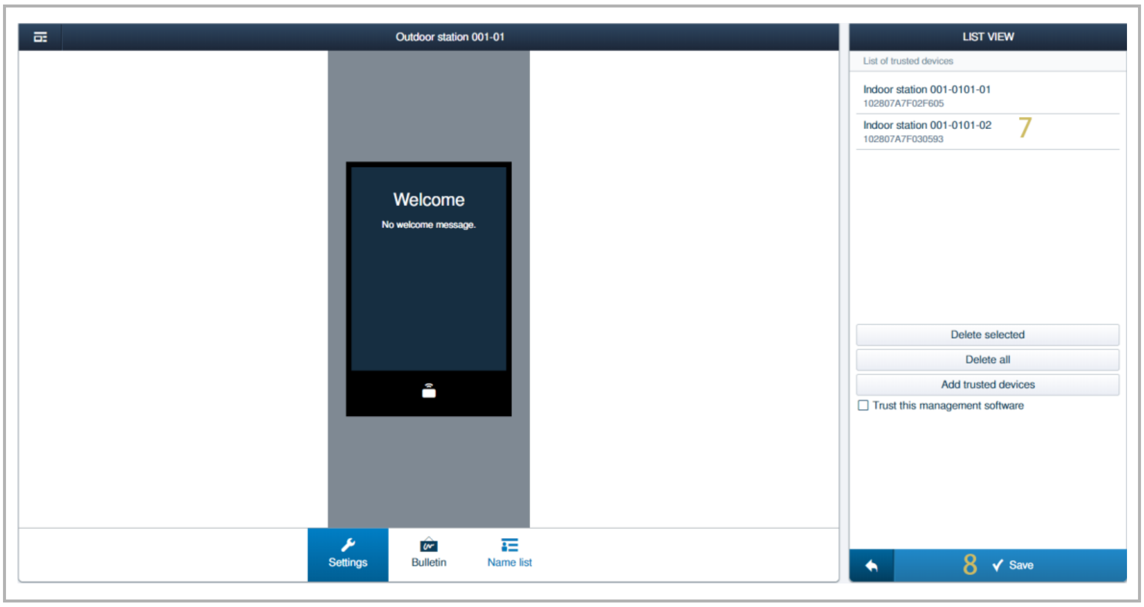
[5] Tick the check boxes to select the devices to be trusted.

[6] Click " √ " to confirm.



[7] The result is displayed on the screen.

[8] Click "Save" to save.



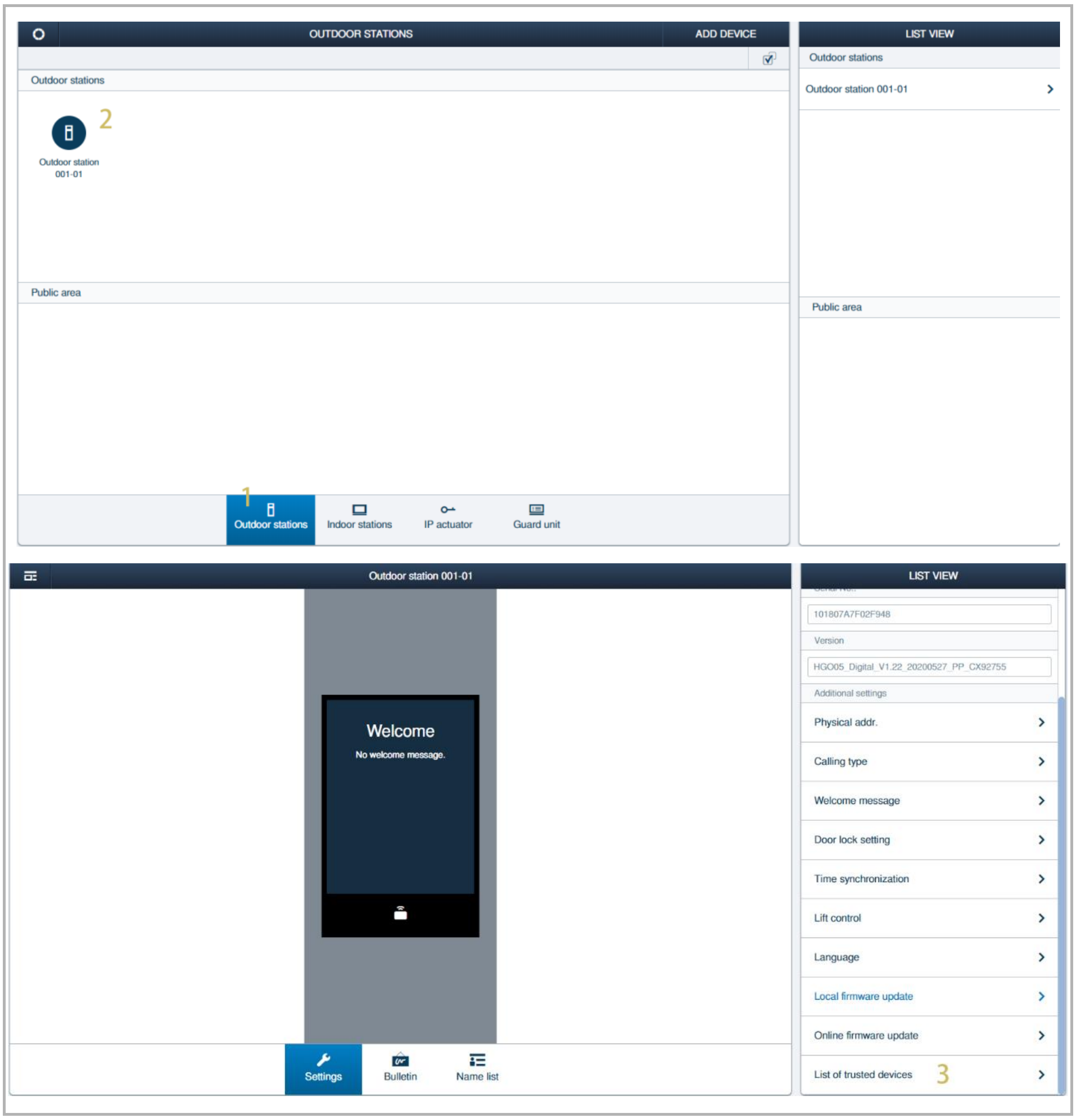
2. Removing the trusted devices

Please follow the steps below:

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

[2] Click the designated outdoor station.

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

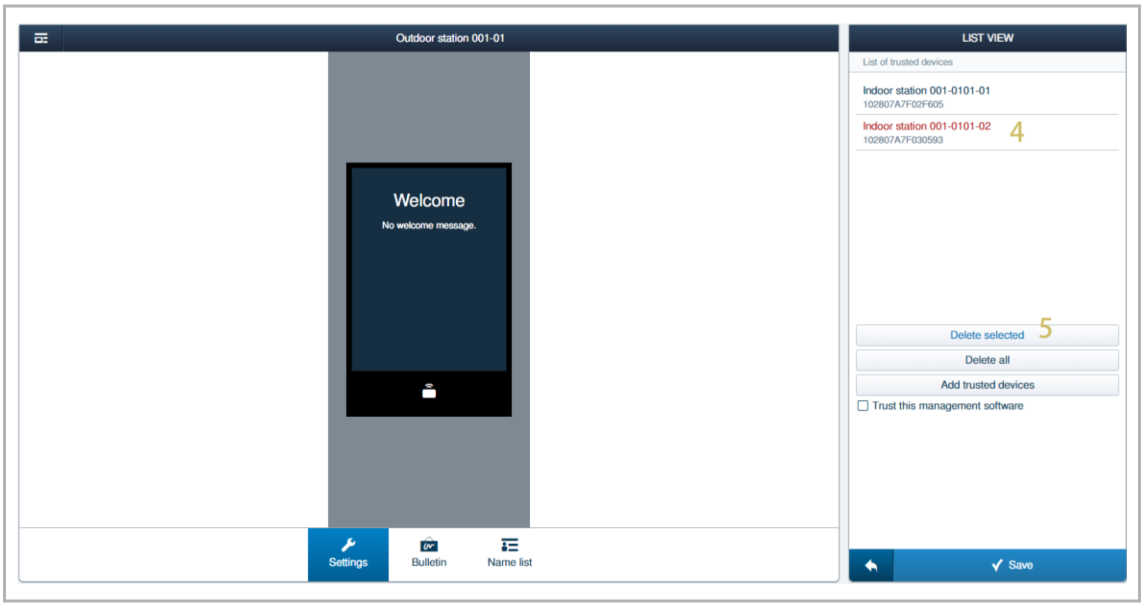


Serial No.: 101807A7F02F948

Version: HGO05_Digital_V1.22_20200527_PP_CX92755

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

[5] Click "Delete selected".



10.8.2 Managing the trusted devices for IP actuator

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

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

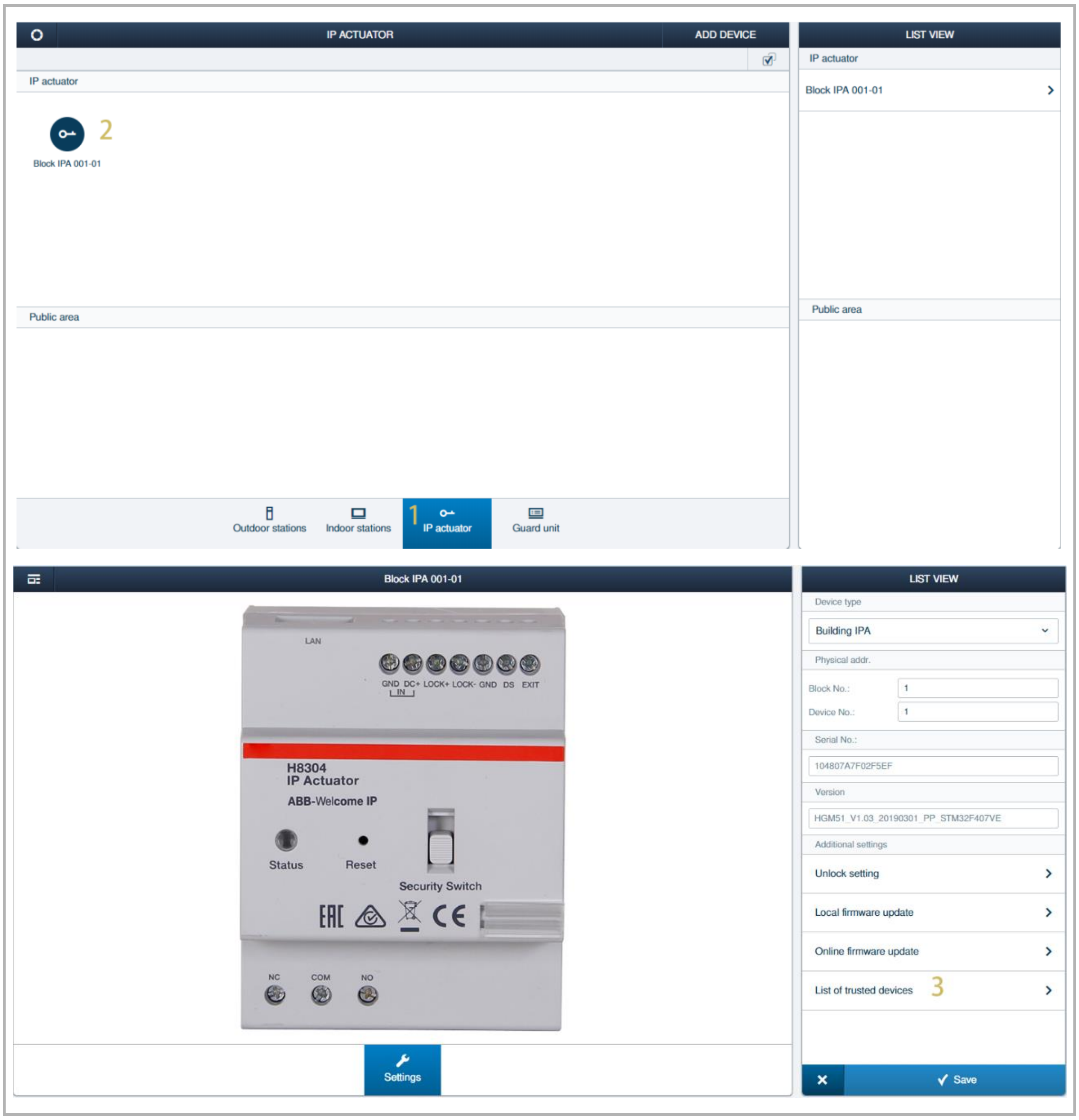
1. Adding the trusted devices

Please follow the steps below:

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

[2] Click the designated IP actuator.

[3] Click "List of trusted devices".



Device type: Building IPA

Physical addr.

Block No.: 1

Device No.: 1

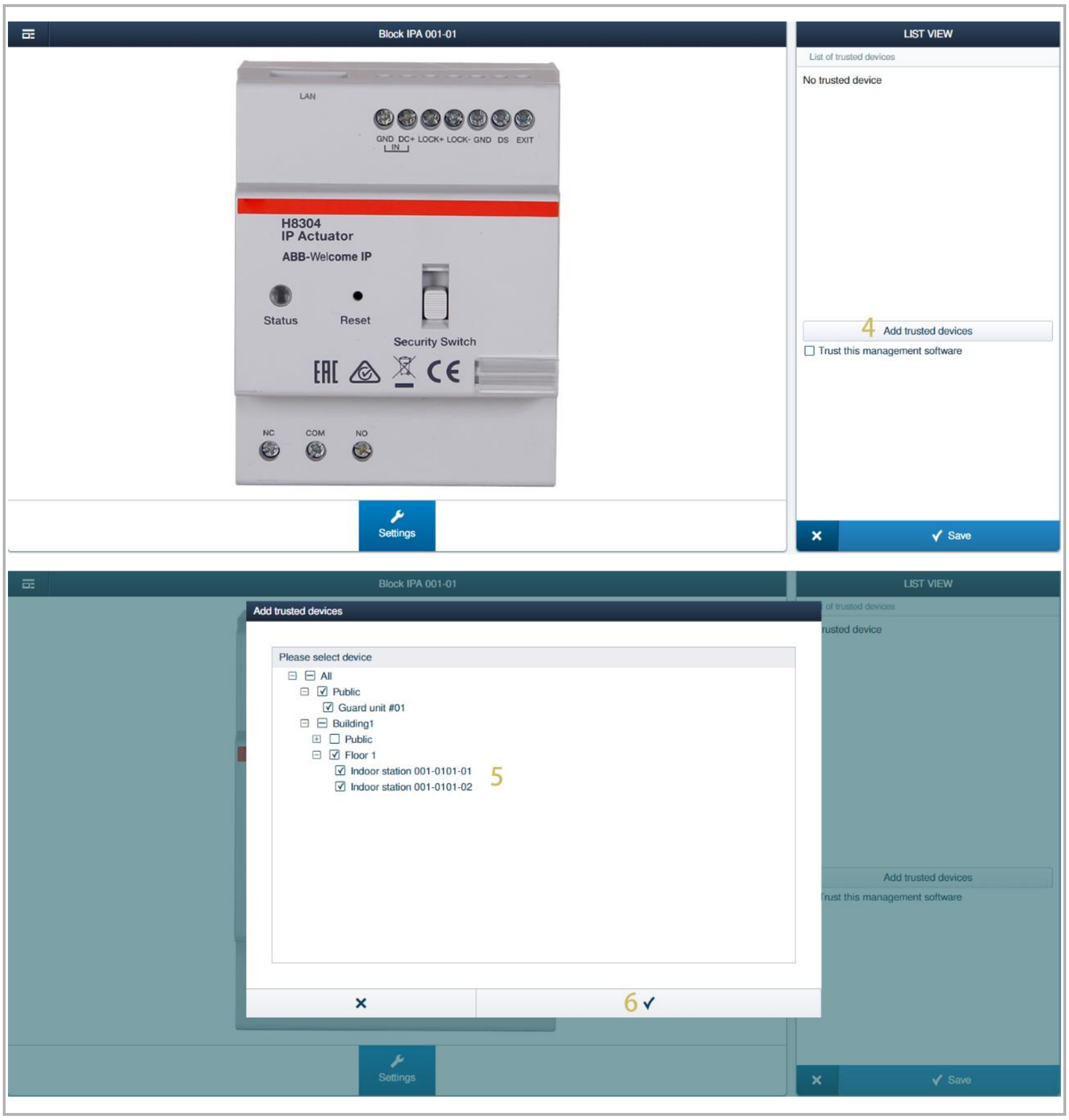
Serial No.: 104807A7F02F5EF

Version: HGM51_V1.03_20190301_PP_STM32F407VE

[4] Click "Add trusted devices".

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

[6] Click " √ " to confirm.



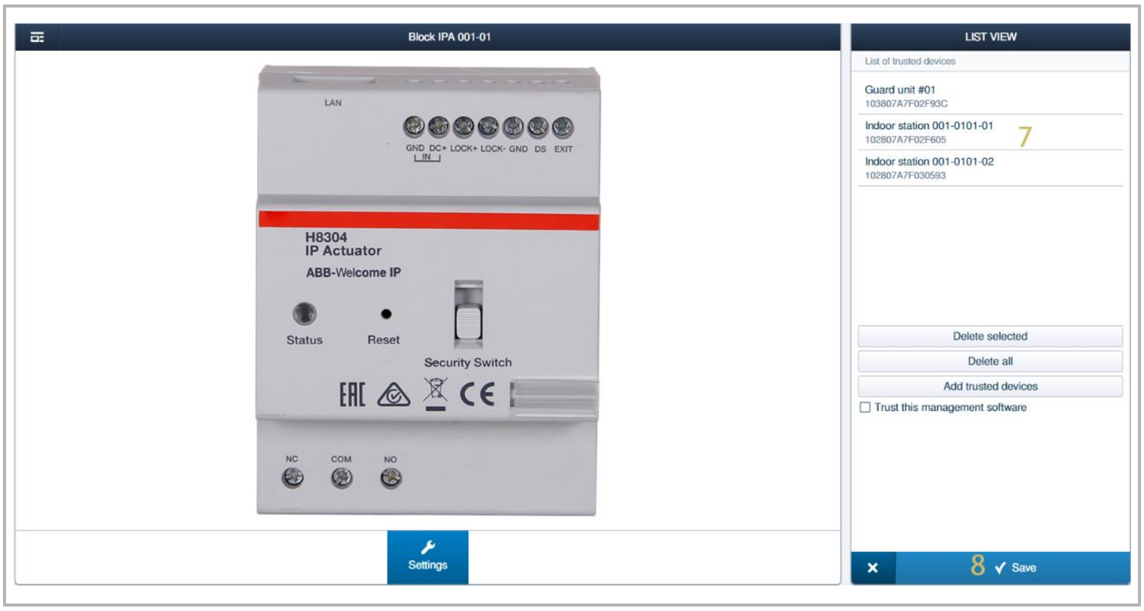
No trusted device

□ Trust this management software

⊟ ⊟ All
⊟ ☑ Public
☑ Guard unit #01
⊟ ⊟ Building1
⊞ □ Public
⊟ ☑ Floor 1
☑ Indoor station 001-0101-01
☑ Indoor station 001-0101-02

[7] The result is displayed on the screen.

[8] Click "Save" to save.



List of trusted devices

Guard unit #01
103807A7F02F93C

Indoor station 001-0101-01
102807A7F02F605

Indoor station 001-0101-02
102807A7F030593

☐ Trust this management software

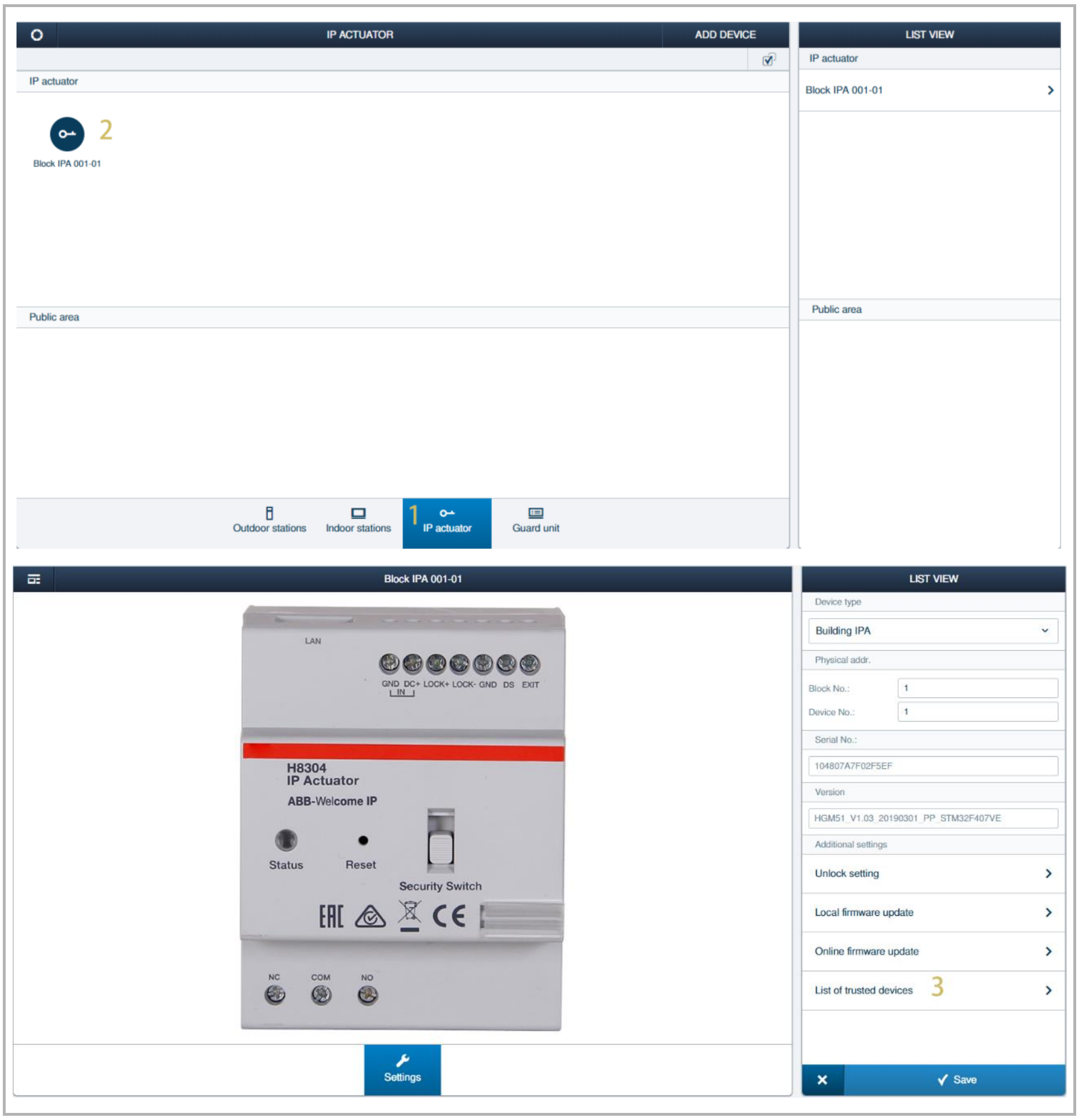
2. Removing the trusted devices

Please follow the steps below:

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

[2] Click the designated IP actuator.

[3] Click "List of trusted devices".



Device type: Building IPA

Physical addr.

Block No.: 1

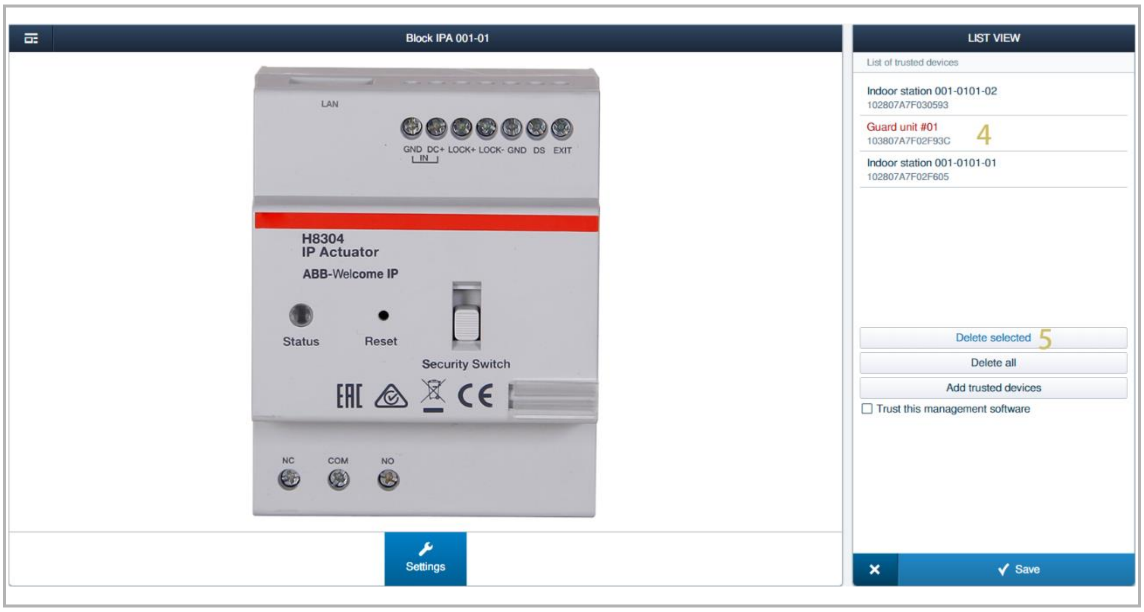
Device No.: 1

Serial No.: 104807A7F02F5EF

Version: HGM51_V1.03_20190301_PP_STM32F407VE

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

[5] Click "Delete selected".



10.8.3 Managing the trusted devices for the SmartAP

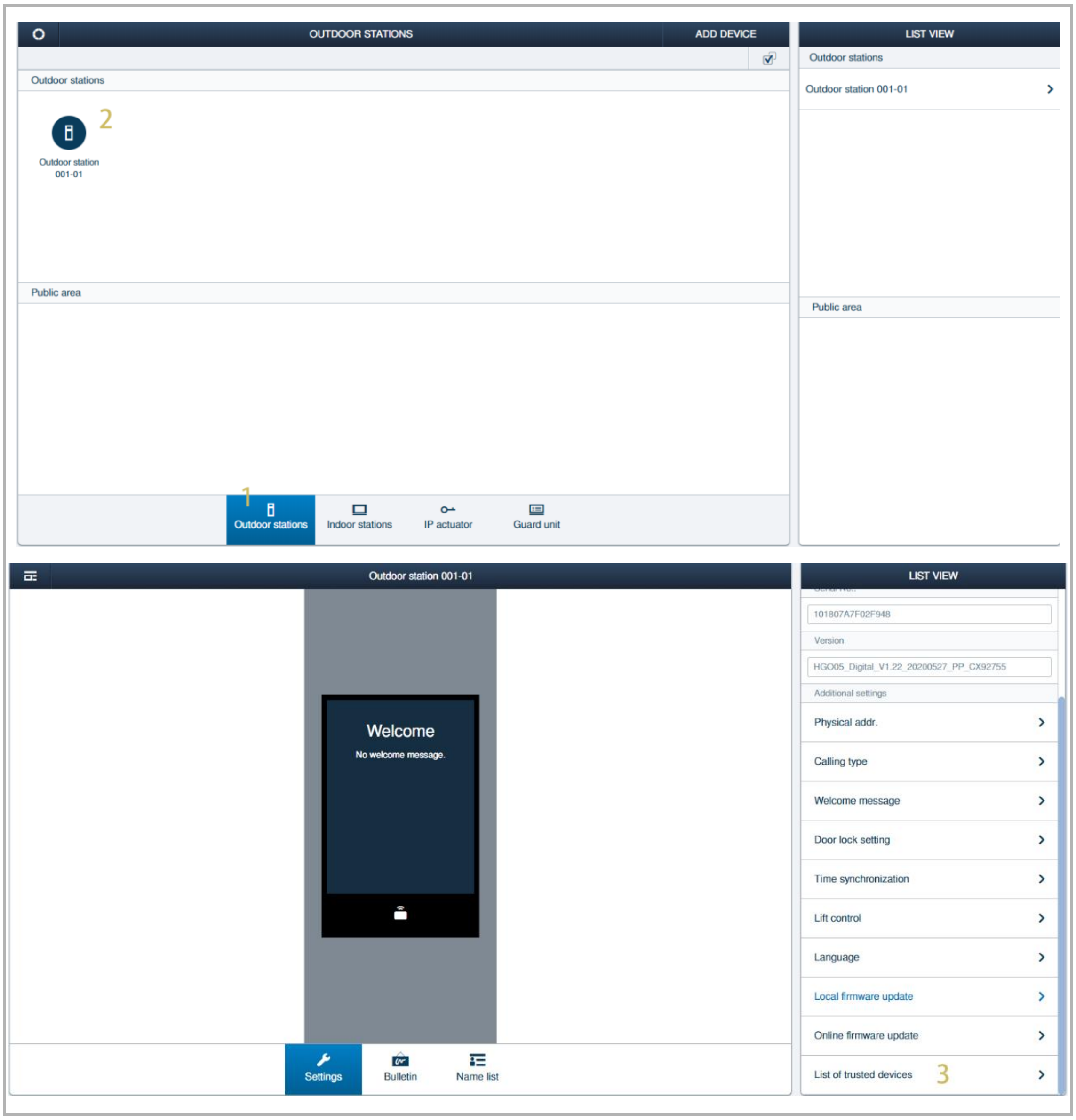
1. Trusting the designated outdoor stations

Please follow the steps below:

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

[2] Click the designated outdoor station.

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



101807A7F02F948

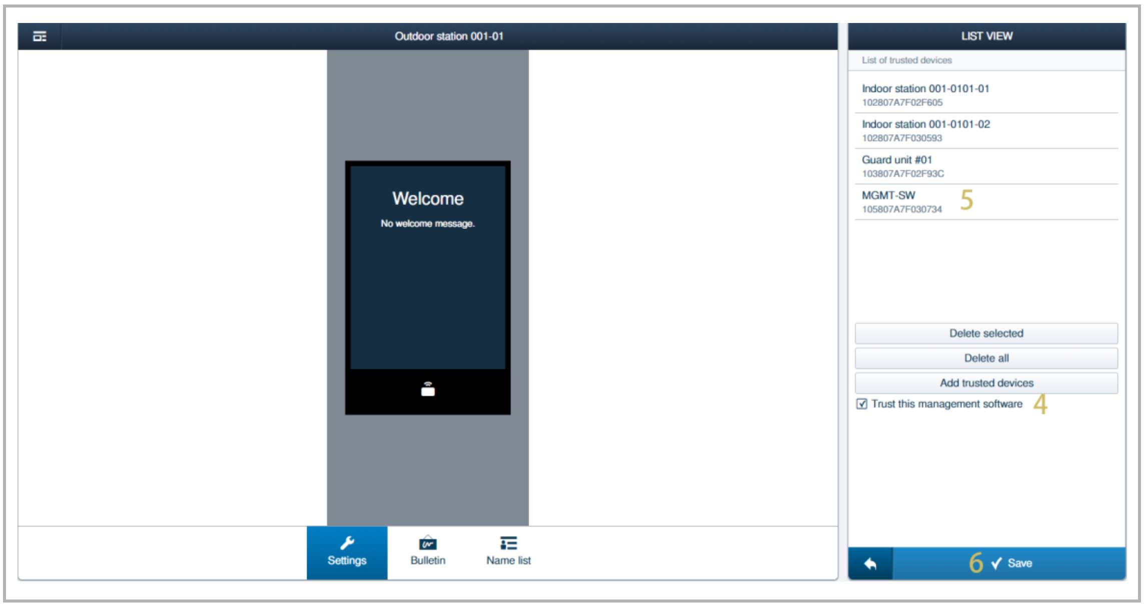
Version

HGO05_Digital_V1.22_20200527_PP_CX92755

[4] Click "Trust this management software".

[5] The result is displayed on the list.

[6] Click " √ " to save.



Indoor station 001-0101-01 102807A7F02F605
Indoor station 001-0101-02 102807A7F030593
Guard unit #01 103807A7F02F93C
MGMT-SW 105807A7F030734

☑ Trust this management software

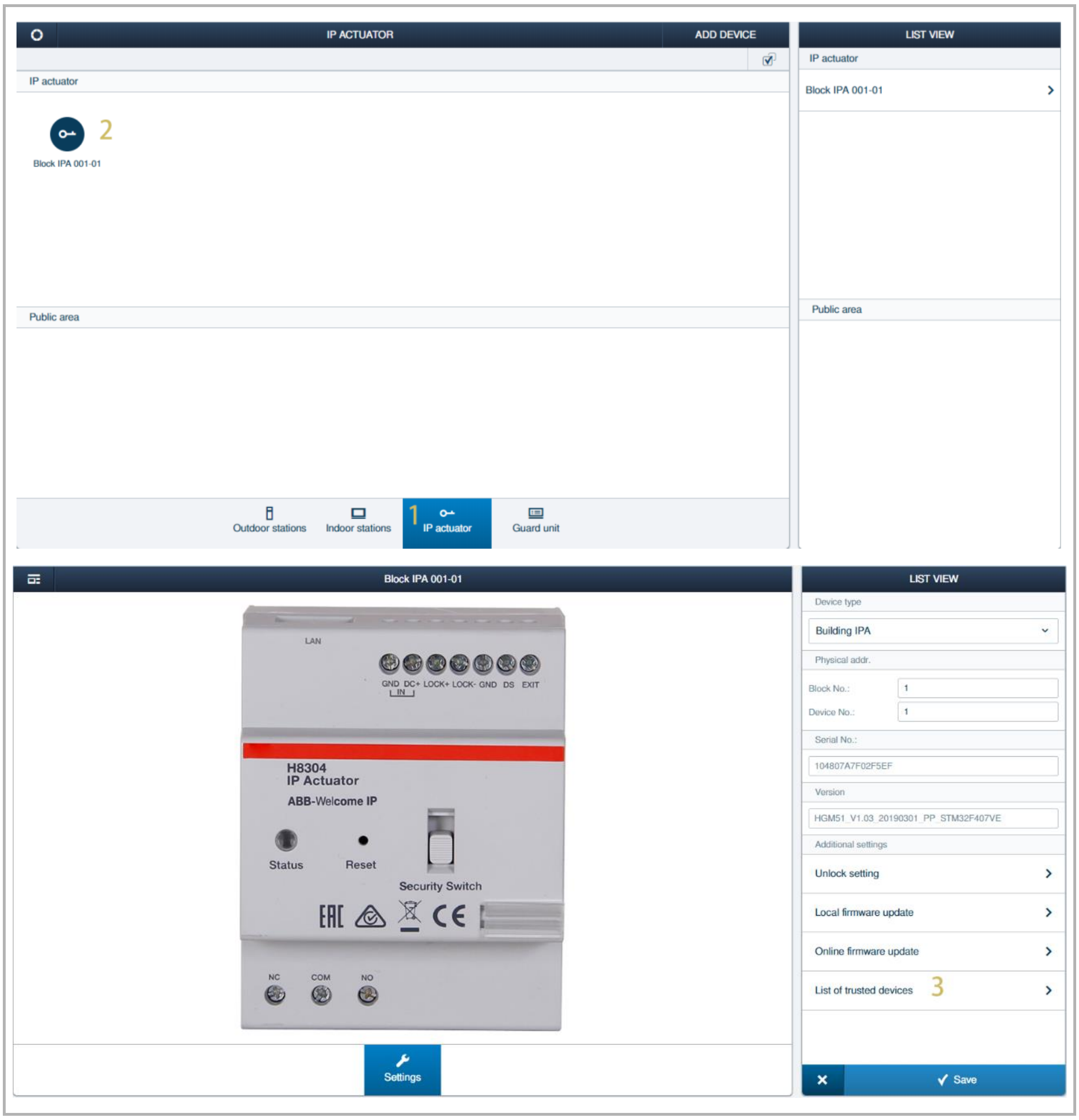
2. Trusting the designated IP Actuators

Please follow the steps below:

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

[2] Click the designated IP actuator.

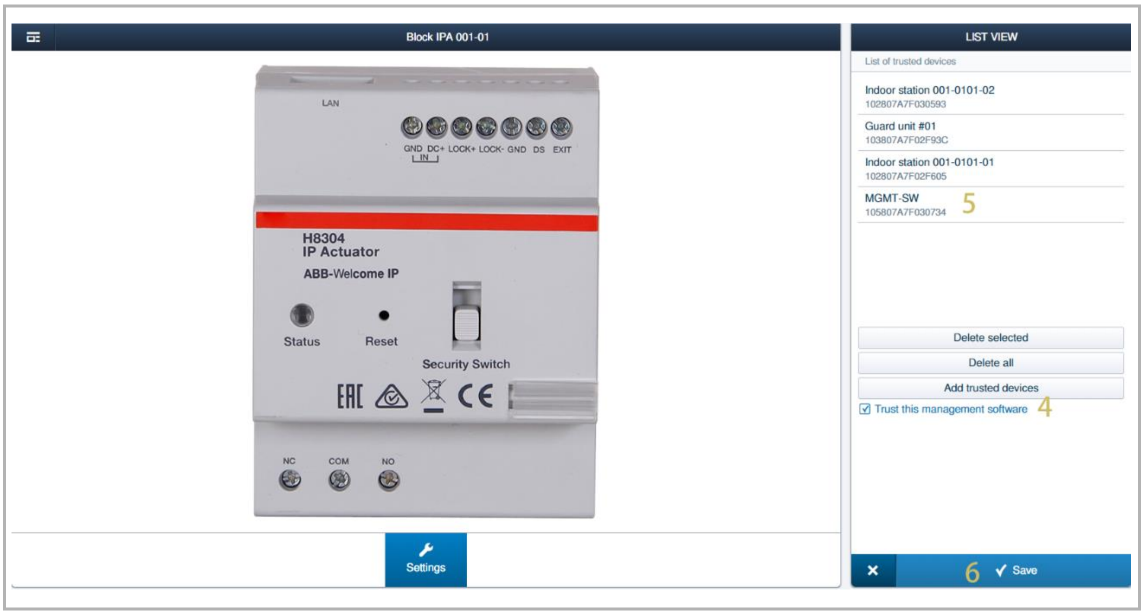
[3] Click "List of trusted devices".



[4] Click "Trust this management software".

[5] The result is displayed on the list.

[6] Click " √ " to save.



Block IPA 001-01

LIST VIEW

List of trusted devices

Indoor station 001-0101-02
102807A7F030593

Guard unit #01
103807A7F02F93C

Indoor station 001-0101-01
102807A7F02F605

MGMT-SW
105807A7F030734

☑ Trust this management software

10.8.4 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 all public IP actuators to "Smart Access Point".

Release all public doors

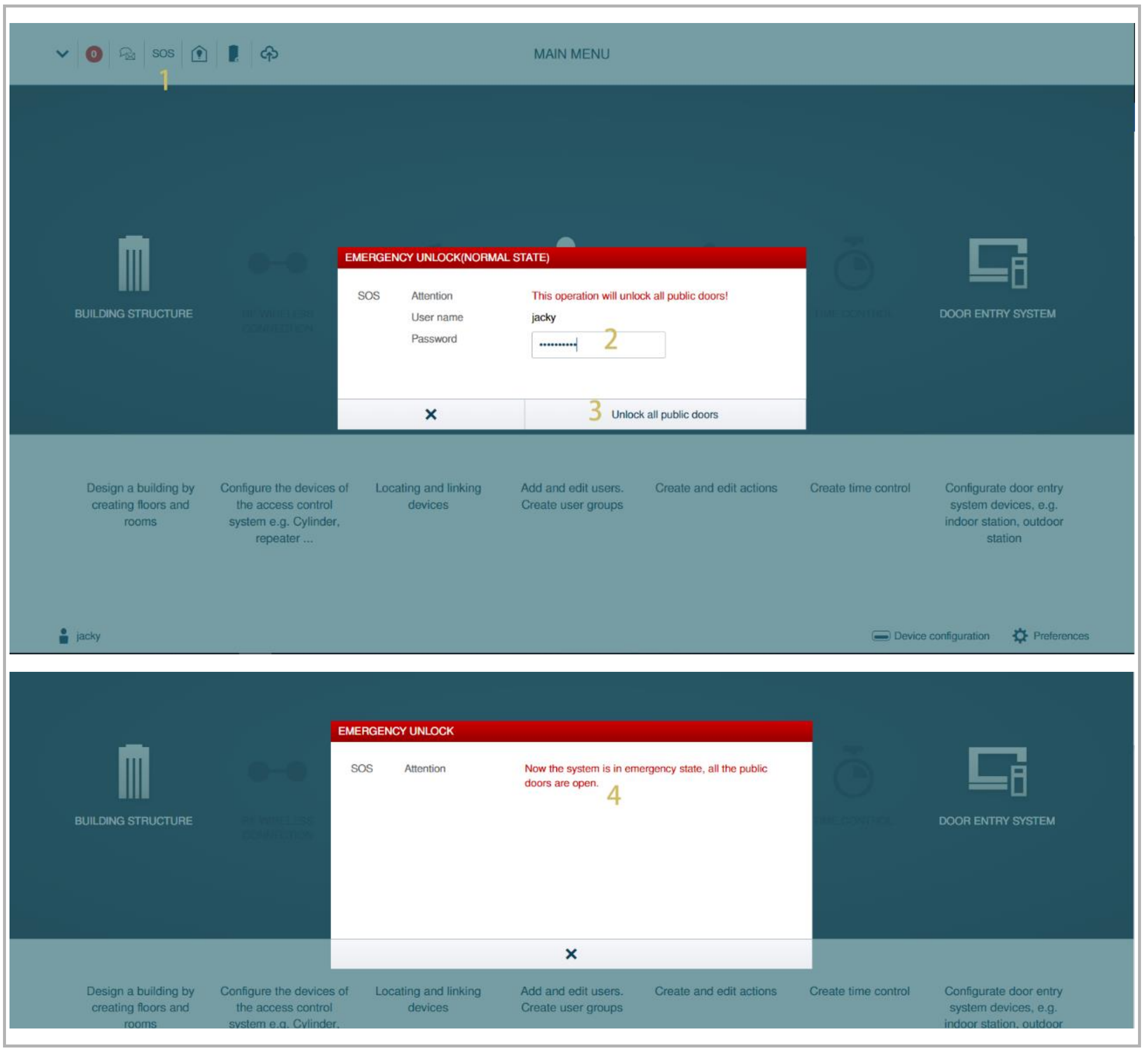
Please follow the steps below:

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

[2] Enter the password for current admin user.

[3] Click "Unlock all public doors".

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



EMERGENCY UNLOCK(NORMAL STATE)

SOS

Attention: This operation will unlock all public doors!

User name: jacky

Password: ••••••••••

× | Unlock all public doors

EMERGENCY UNLOCK

SOS

Attention: Now the system is in emergency state, all the public doors are open.

×

SOS
1
MAIN MENU
2
3
4
BUILDING STRUCTURE
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
Configure door entry system devices, e.g. indoor station, outdoor station
jacky
Device configuration
Preferences

Close all public doors

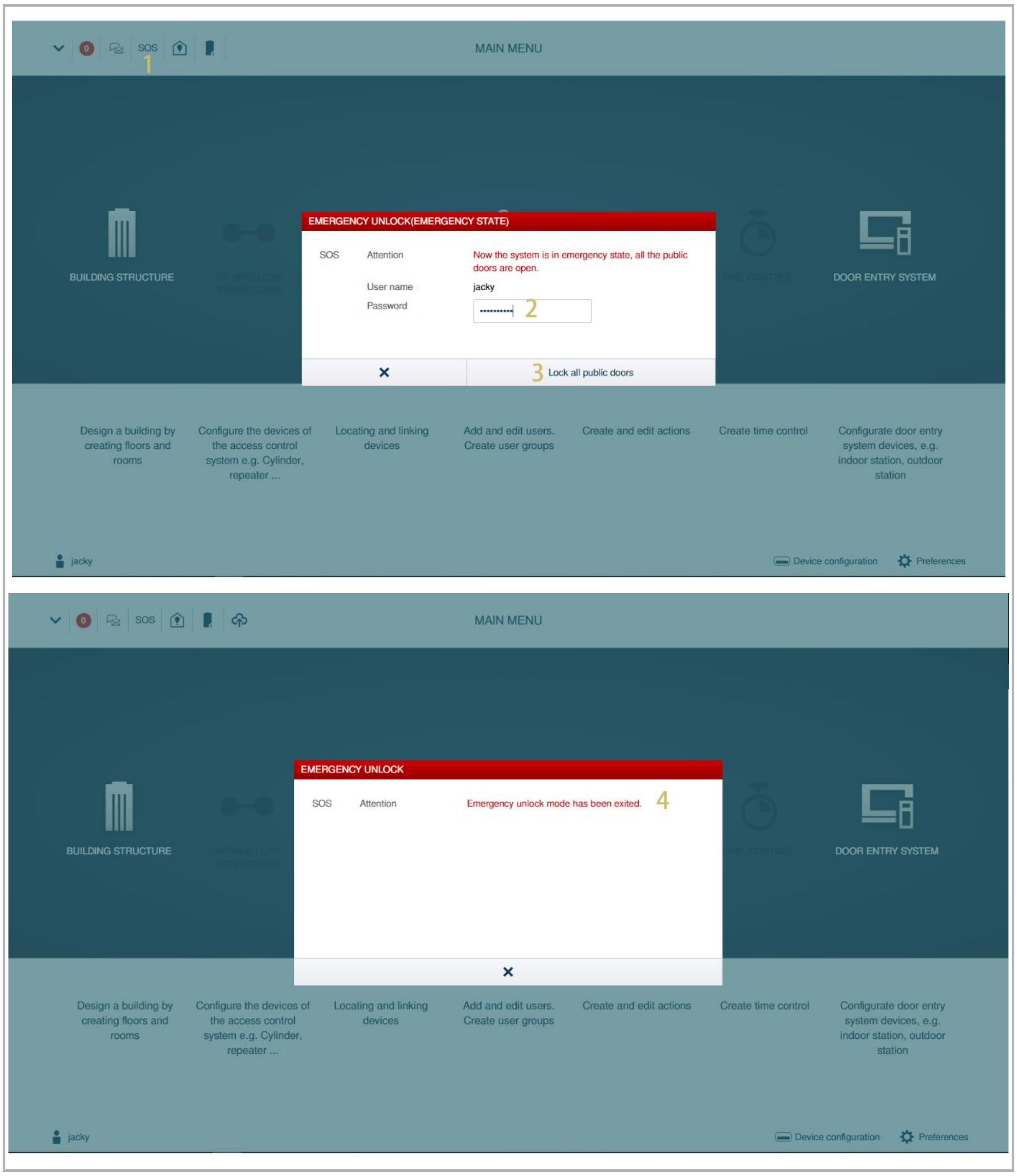
Please follow the steps below:

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

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

[3] Click "Lock all public doors".

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



EMERGENCY UNLOCK(EMERGENCY STATE)

SOS Attention Now the system is in emergency state, all the public doors are open.

User name jacky

Password ••••••••••

✕ Lock all public doors

EMERGENCY UNLOCK

SOS Attention Emergency unlock mode has been exited.

✕

SOS
1
2
3
4
MAIN MENU
BUILDING STRUCTURE
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

10.8.5 Trusting all devices

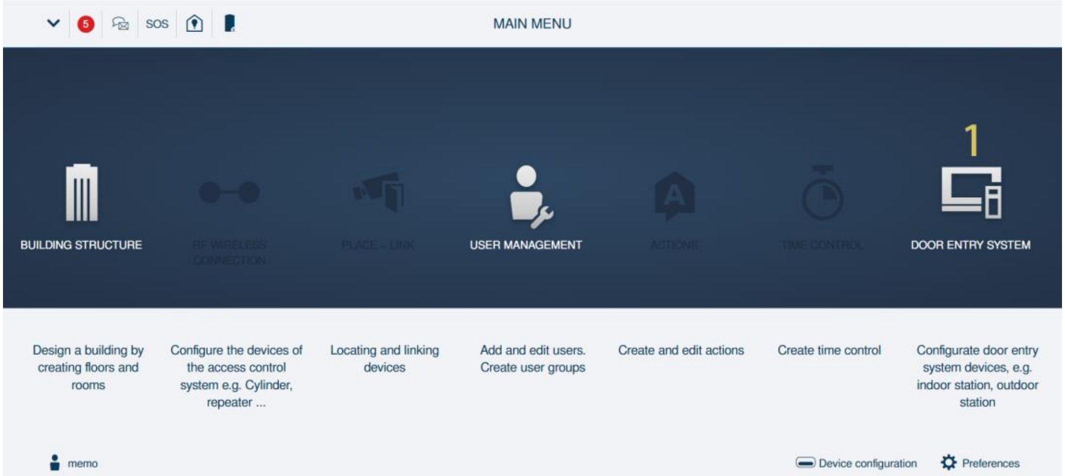
There is a simple way to create a trusting list.

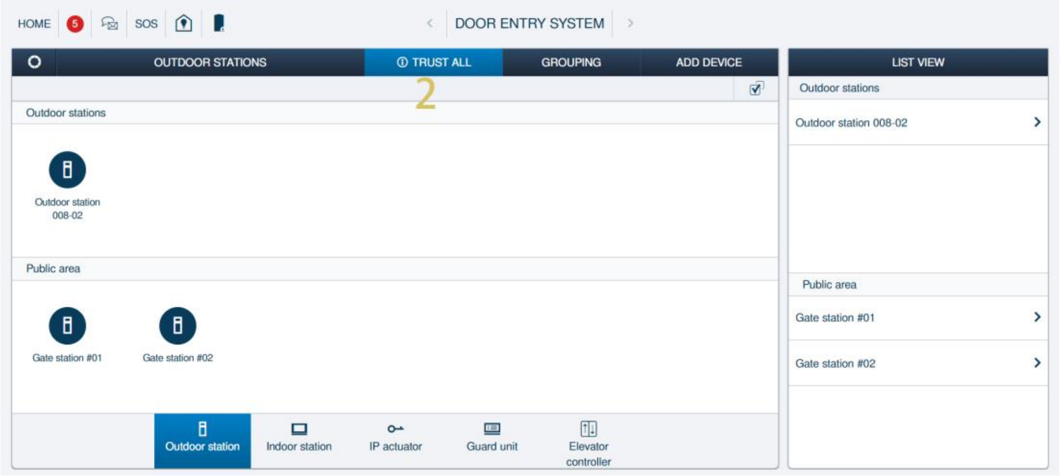
Please follow the steps below:

[1] On the "Main Menu" screen of SmartAP, click "Door Entry System".

[2] Click "Trust All".

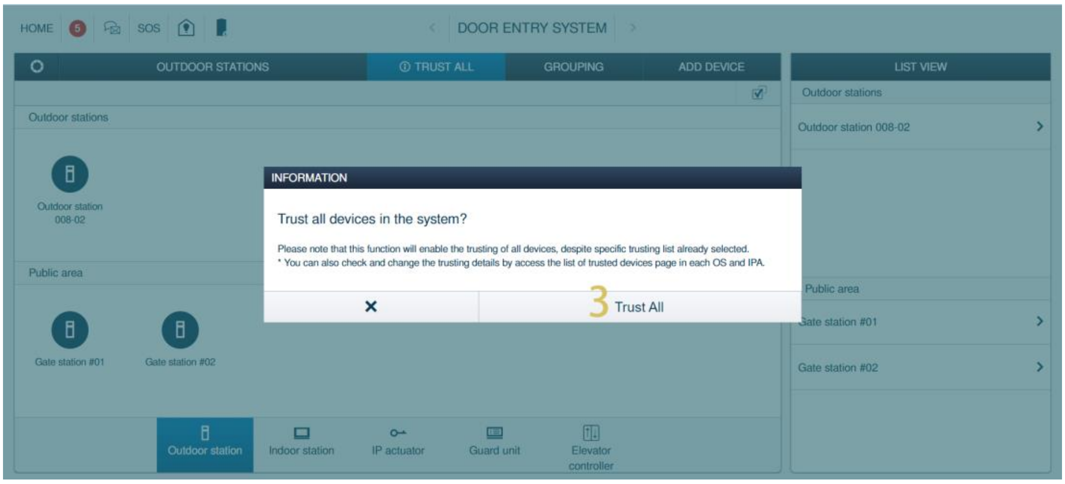
- When new devices are added to the system and the physical address of the device is changed, " ⓘ " will be display to indicate the update.


5
SOS
MAIN MENU
1
BUILDING STRUCTURE
RF WIRELESS CONNECTION
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
memo
Device configuration
Preferences



[3] Click "Trust All".

[4] Click " √ ".

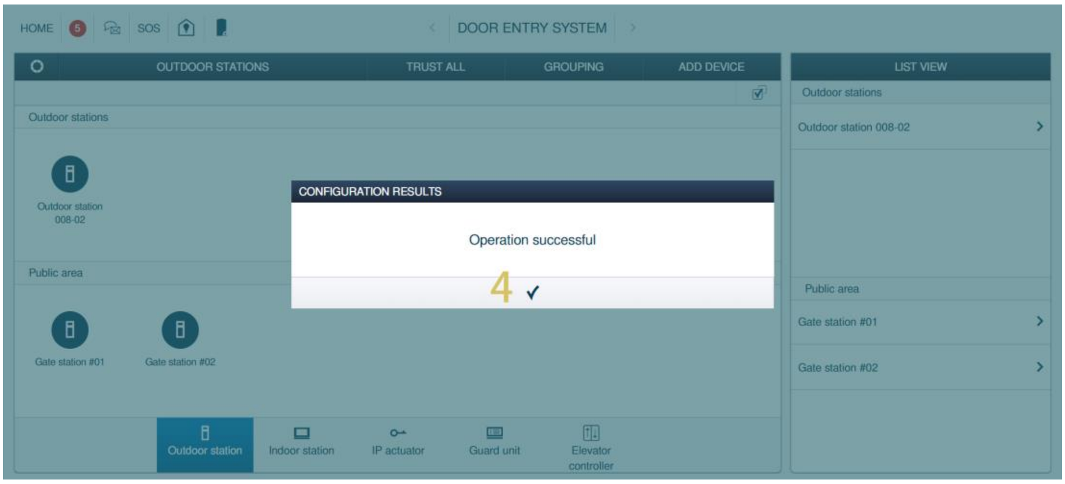


INFORMATION

Trust all devices in the system?

Please note that this function will enable the trusting of all devices, despite specific trusting list already selected.
* You can also check and change the trusting details by access the list of trusted devices page in each OS and IPA.

✕ Trust All



CONFIGURATION RESULTS

Operation successful

✓

The following operations will be carried out by using the "Trusting All" function.

Device name	Operation
Gate Station	Trust all Indoor Stations and all IP Actuators.
Building Outdoor Station	Trust all Indoor Stations, Building IP Actuators and Private IP Actuators within this building.
2nd confirmed Outdoor Station	Trust all Indoor Stations and Private IP Actuators within this apartment.
Network IP Actuator	Trust all Indoor Stations and all Outdoor Stations.
Building IP Actuator	Trust all Indoor Stations and Building Outdoor Stations within this building.
Private IP Actuator	Trust all Indoor Stations and 2nd confirmed Outdoor Stations within this apartment.
Management software	All Outdoor Stations and IP Actuators trust the management software by default.

Busch-Jaeger Elektro GmbH

58513 Lüdenscheid
Freisenbergstraße 2

busch-jaeger.de
info.bje@de.abb.com

Kundenservice:
Tel.: +49 2351 956-1600
Fax: +49 2351 956-1700

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 upon apply for orders. Busch-Jaeger accepts no responsibility for possible errors or incompleteness in this document.

BUSCH-JAEGER