

Product manual

Busch-Welcome® IP

H8304-03 IP Actuator



1	Notes on the instruction manual	4
2	Safety	4
3	Intended use.....	4
4	Environment	5
4.1	Busch-Jaeger devices.....	5
5	Product description.....	6
5.1	Device type	6
5.2	Terminal description.....	7
5.3	Lock type and connection	8
6	Technical data.....	9
7	Mounting/Installation	10
7.1	Requirement for the electrician	10
7.2	Mounting	11
8	Commissioning.....	12
8.1	Configuring the settings on the Indoor Station	12
8.1.1	Accessing the "Actuators" screen.....	12
8.1.2	Configuring the device type	13
8.1.3	Configuring the lock.....	19
8.1.4	Configuring the "Report when unlock" function	21
8.1.5	Linking the exit button with the lock.....	22
8.1.6	Configuring the "Door status detection" function	23
8.1.7	Viewing the information	24
8.1.8	Updating the firmware	25
8.2	Configuring the settings on the SmartAP	27
8.2.1	Adding an IP Actuator	27
8.2.2	Accessing the designated IP Actuator screen	29
8.2.3	Viewing the serial number.....	30
8.2.4	Viewing the version	31
8.2.5	Configuring the physical address	32
8.2.6	Configuring the IP address	34
8.2.7	Configuring the lock.....	35
8.2.8	Configuring the trusted devices	36
8.2.9	Updating the firmware	38
8.3	Restoring to factory default	41
9	Cyber security	42
9.1	Disclaimer	42
9.2	Performance and service	42
9.3	Deployment guideline.....	43
9.4	Upgrading	43
9.5	Backup/restore	43
9.6	Malware prevention solution	43

9.7	Password rule	43
10	Notice	44

1 Notes on the instruction manual

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

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

2 Safety



Warning

Electric voltage!

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

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

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

3 Intended use

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

4 Environment



Consider the protection of the environment!

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

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

4.1 Busch-Jaeger devices

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

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

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

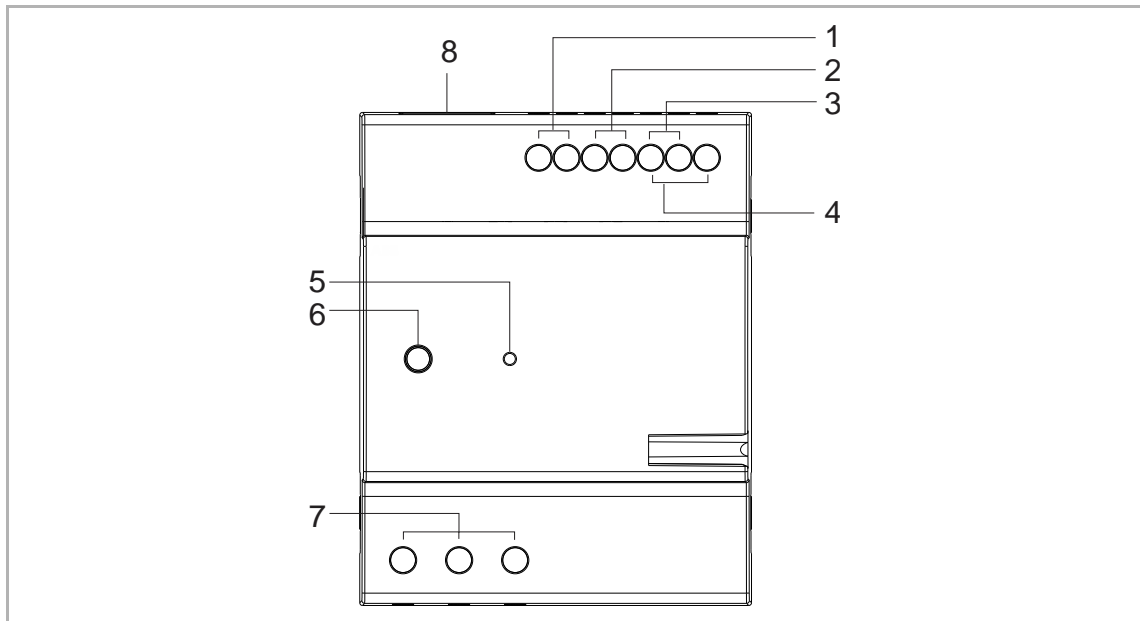
(EU-REACH ordinance and law for the implementation of the ordinance (EG) No.1907/2006)

5 Product description

5.1 Device type





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

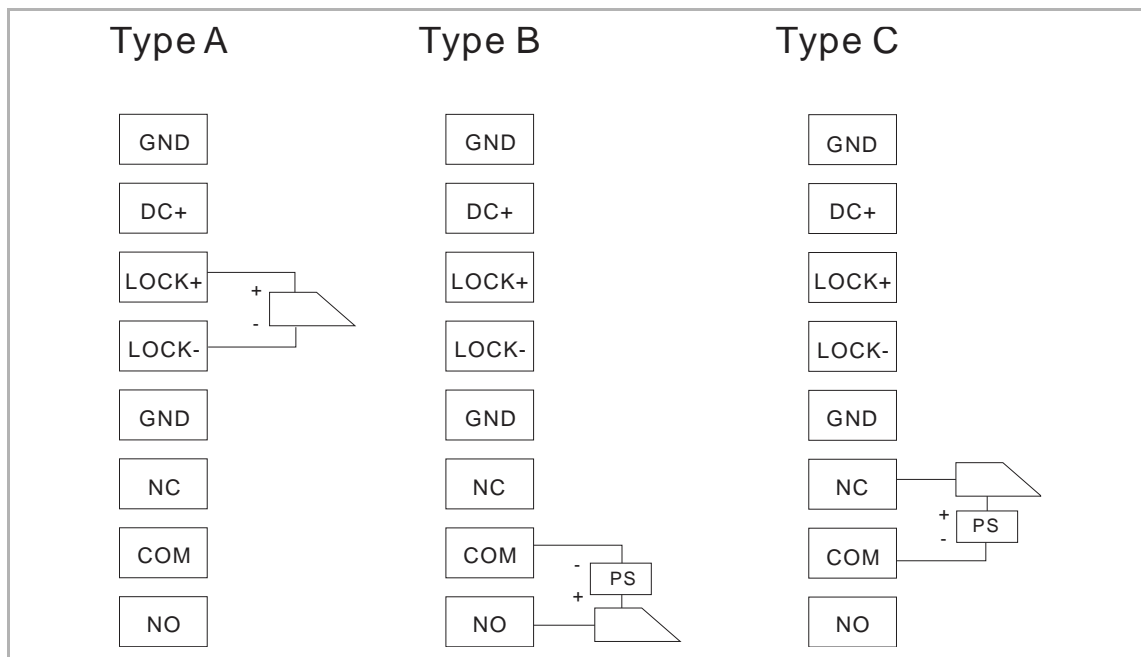
5.2 Terminal description



No.	Function
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)

5.3 Lock type and connection

Lock type	Pic	Operation type	Voltage	Wiring type
Electrical strike lock, 12V		Power on to open	12 V \equiv /~	Type A/B
Electrical strike lock, 24V		Power on to open	24 V \equiv /~	Type B
Electrical rim lock, 12 V		Power on to open	12 V \equiv	Type A/B
Electrical mortise lock		Power off to open	12 V \equiv	Type C
Magnetic lock		Power off to open	12/24 V \equiv	Type C



6 Technical data

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

7 Mounting/Installation

**Warning**

Electric voltage!

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

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

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

7.1 Requirement for the electrician

**Warning**

Electric voltage!

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

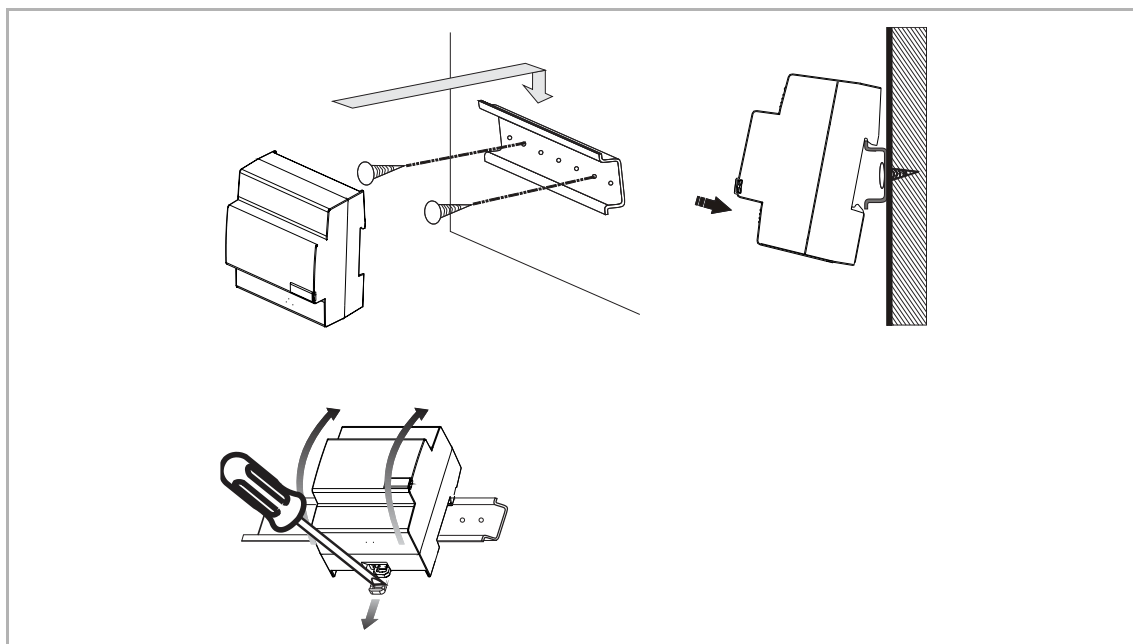
- Incorrect installation endangers your life and that of the user of the electrical system.

- Incorrect installation can cause serious damage to property, e.g. due to fire.

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

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

7.2 Mounting



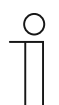
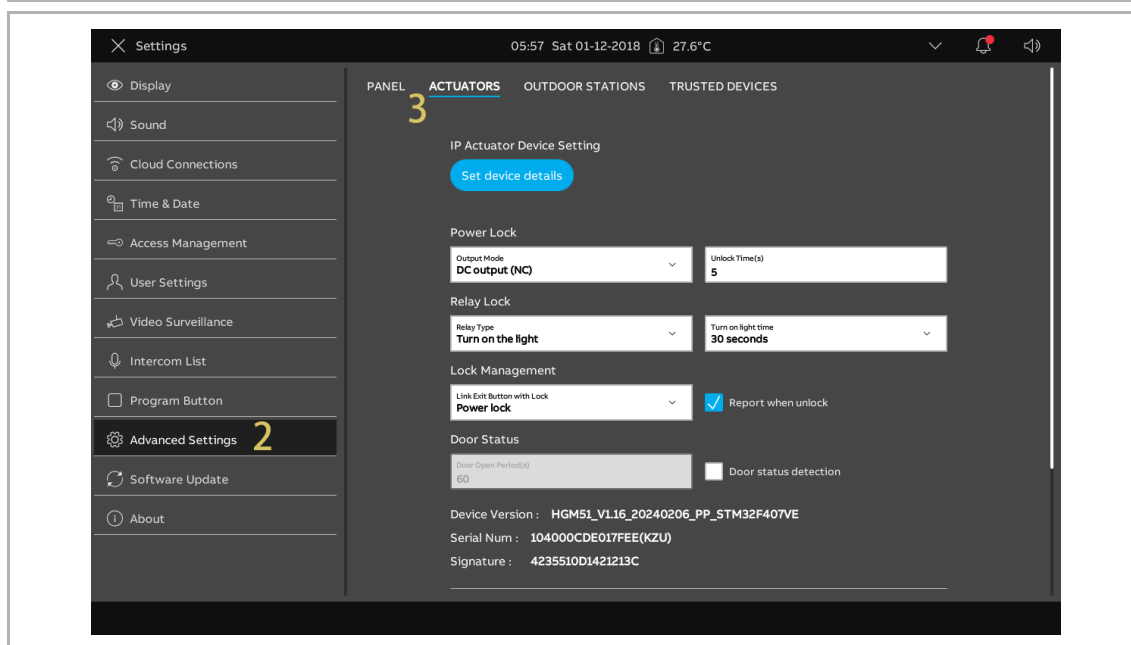
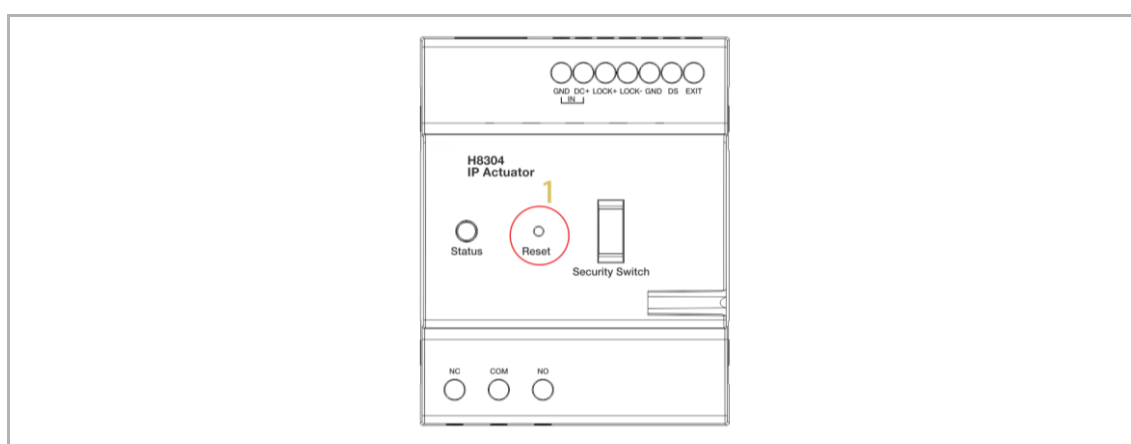
8 Commissioning

8.1 Configuring the settings on the Indoor Station

8.1.1 Accessing the "Actuators" screen

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.



Note

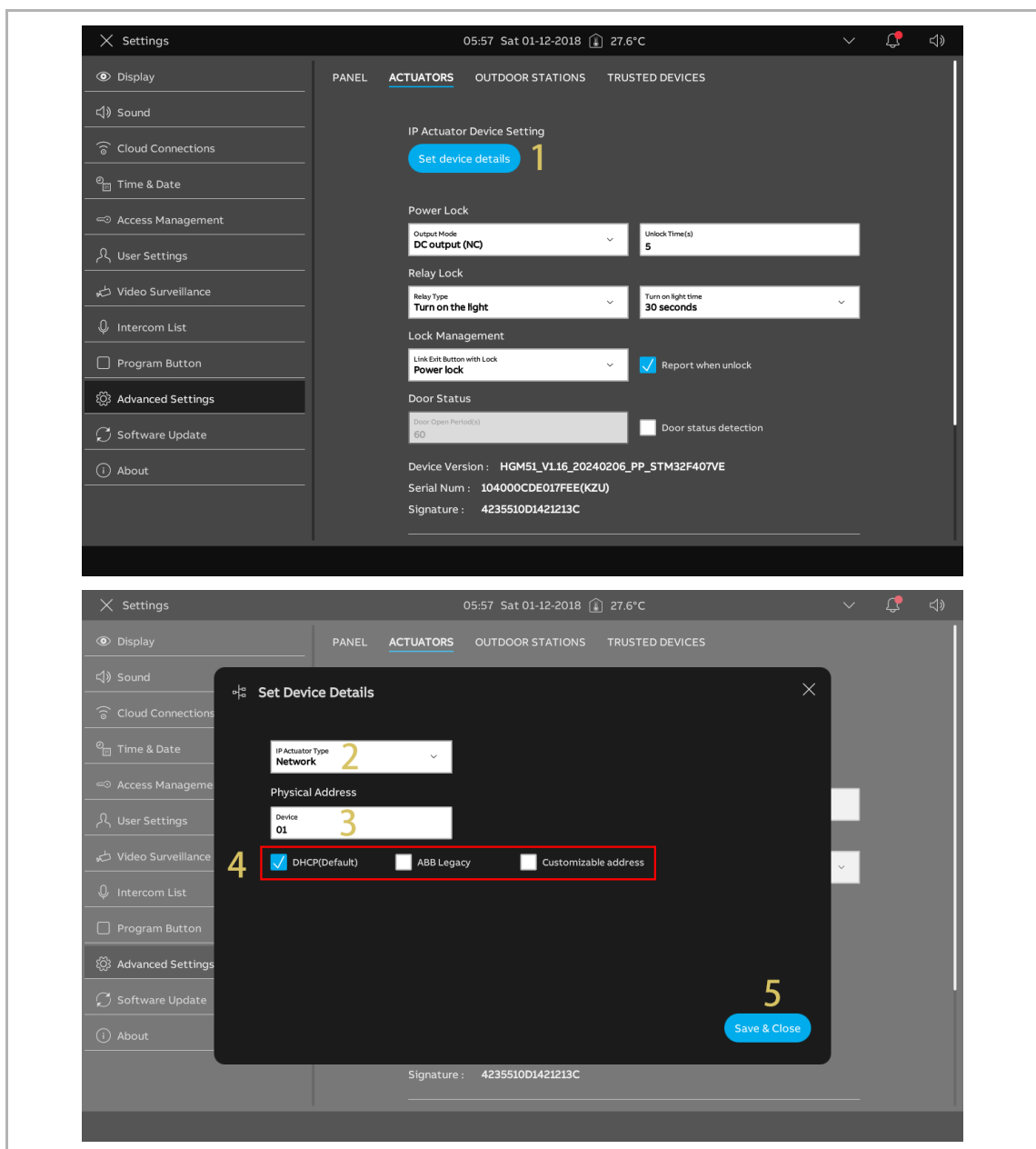
The IP Actuator will exit engineering mode if no operation is carried out for 5 minutes.

8.1.2 Configuring the device type

1. Configuring the network IP Actuator

Please follow the steps below:

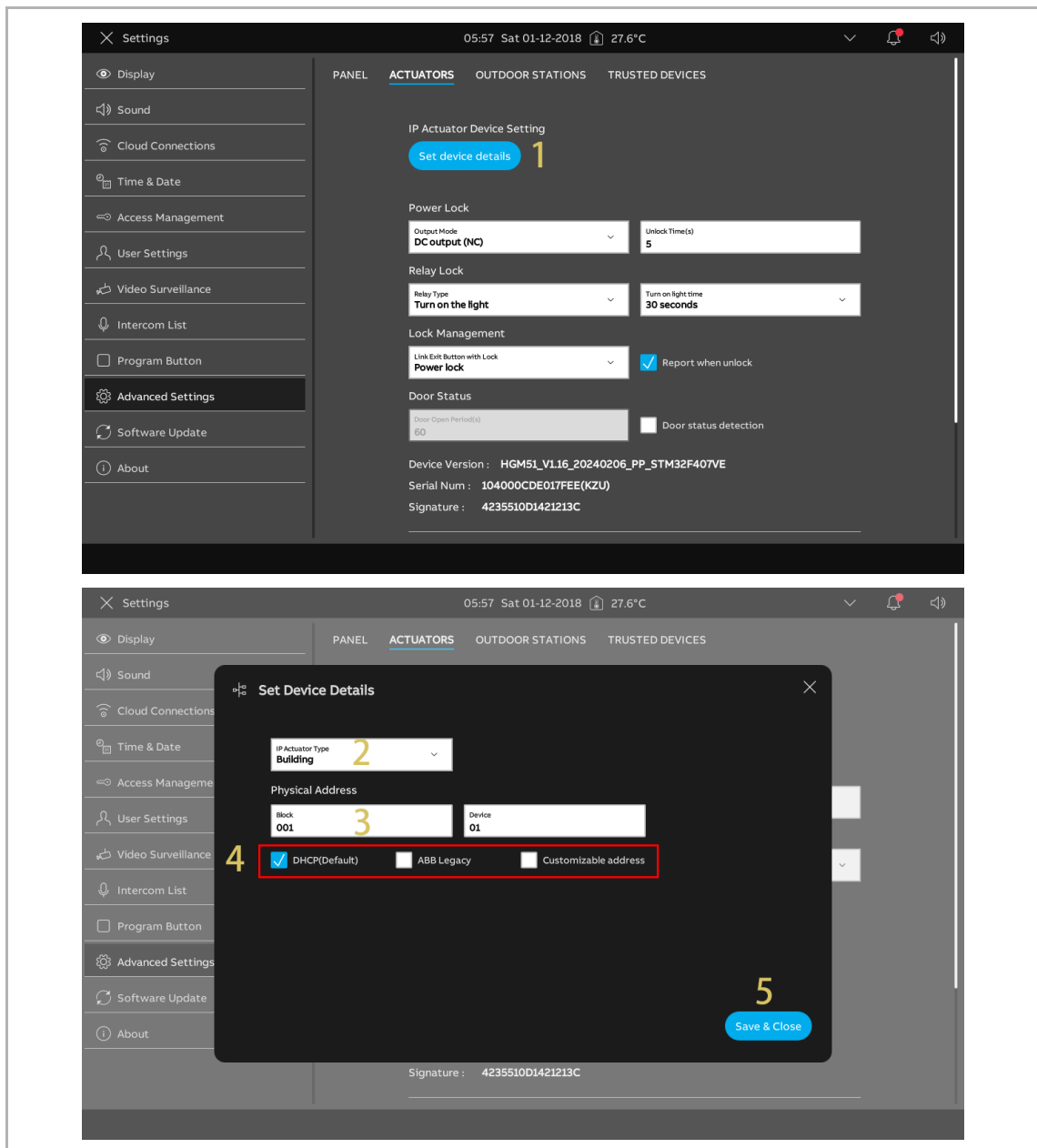
- [1] On the "Actuators" screen, go to the "IP Actuator Device Setting" section, tap "Set device details".
- [2] Select "Network" from the drop-down list.
- [3] Enter the device number (01...32).
- [4] Select the network type, it can set to "DHCP", "Customizable address" or "ABB Legacy".
 - If "ABB Legacy" is selected, IP address will be "10.0.x.x".
- [5] Tap "Save & Close".



2. Configuring the building IP actuator

Please follow the steps below:

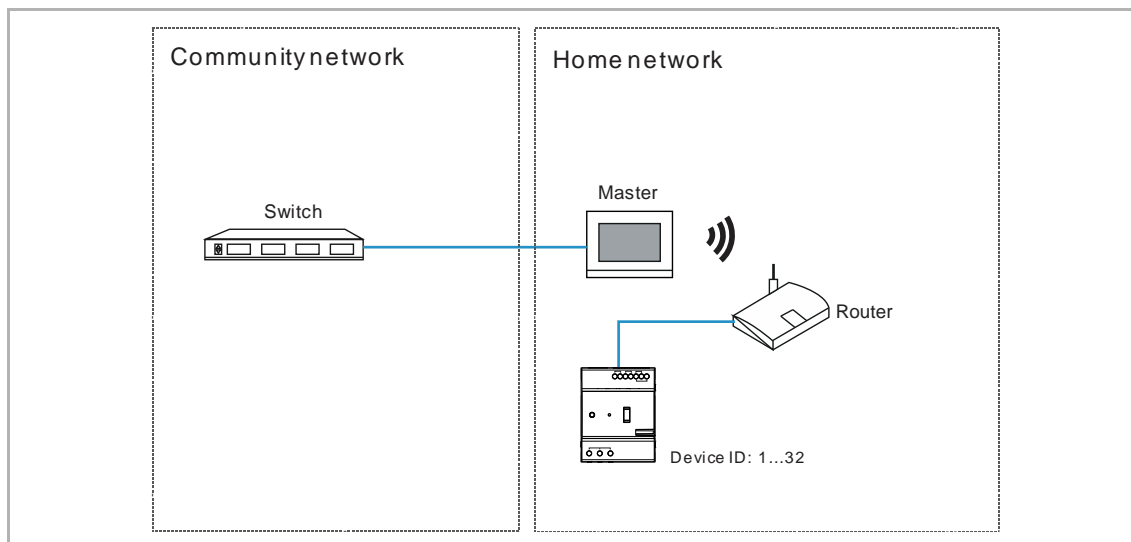
- [1] On the "Actuators" screen, go to the "IP Actuator Device Setting" section, tap "Set device details".
- [2] Select "Building" from the drop-down list.
- [3] Enter the block number (001...999) and the device number (01...32).
- [4] Select the network type, it can set to "DHCP", "Customizable address" or "ABB Legacy".
 - If "ABB Legacy" is selected, IP address will be "10.0.x.x".
- [5] Tap "Save & Close".



3. Configuring the private IP Actuator

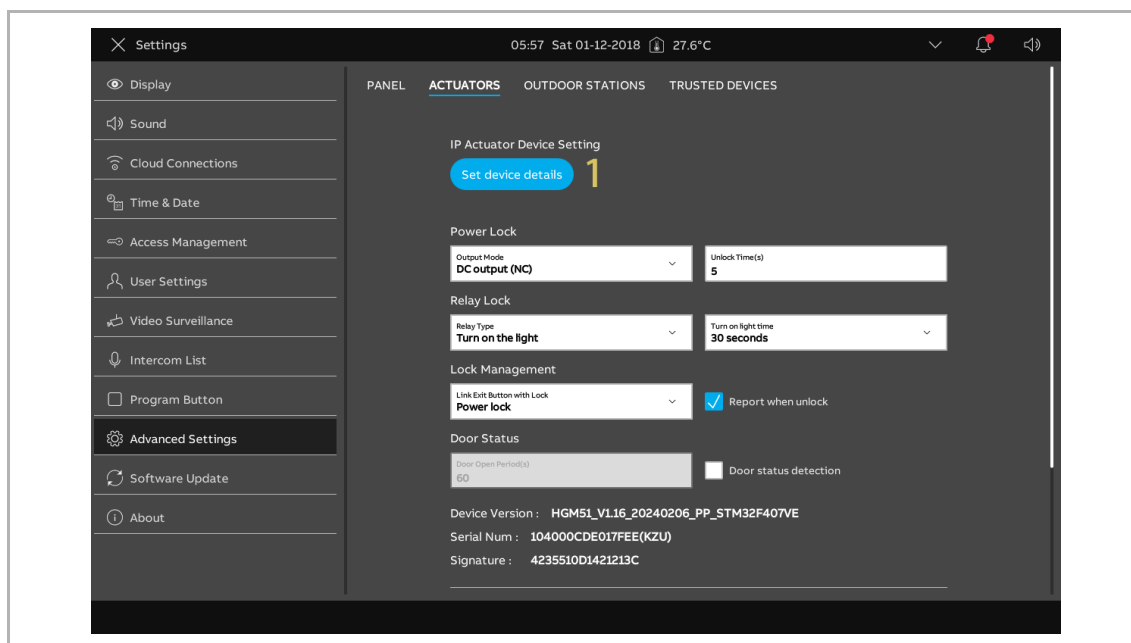
Location of IP Actuator = Internal

In this case, the IP Actuator is connected to the router in the apartment (see the diagram below).

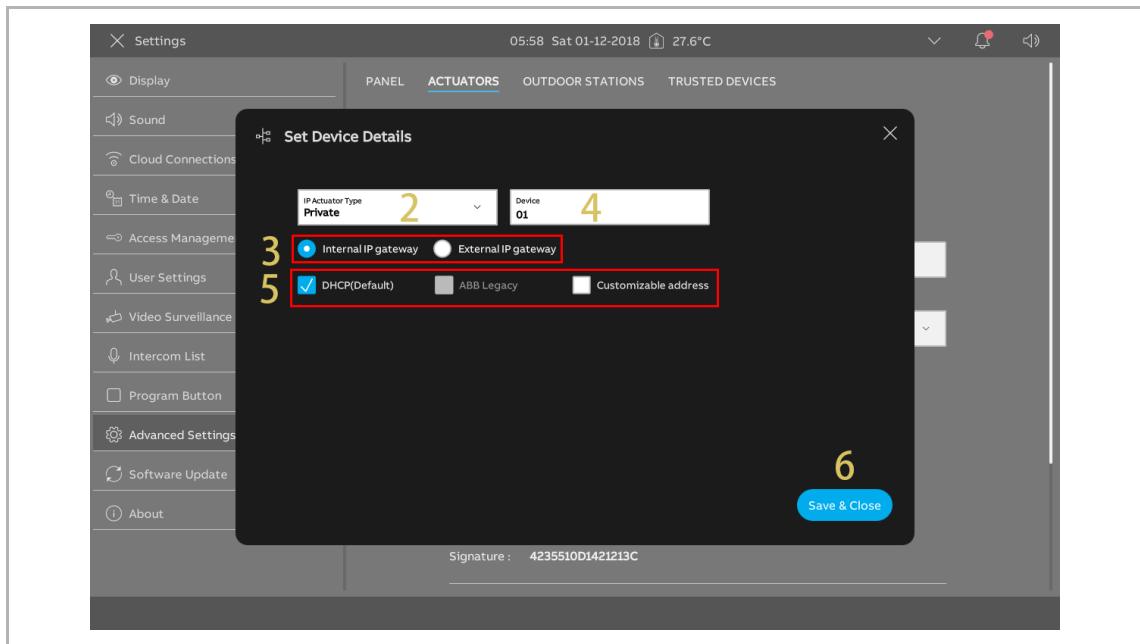


Please follow the steps below:

- [1] On the "Actuators" screen, go to the "IP Actuator Device Setting" section, tap "Set device details".

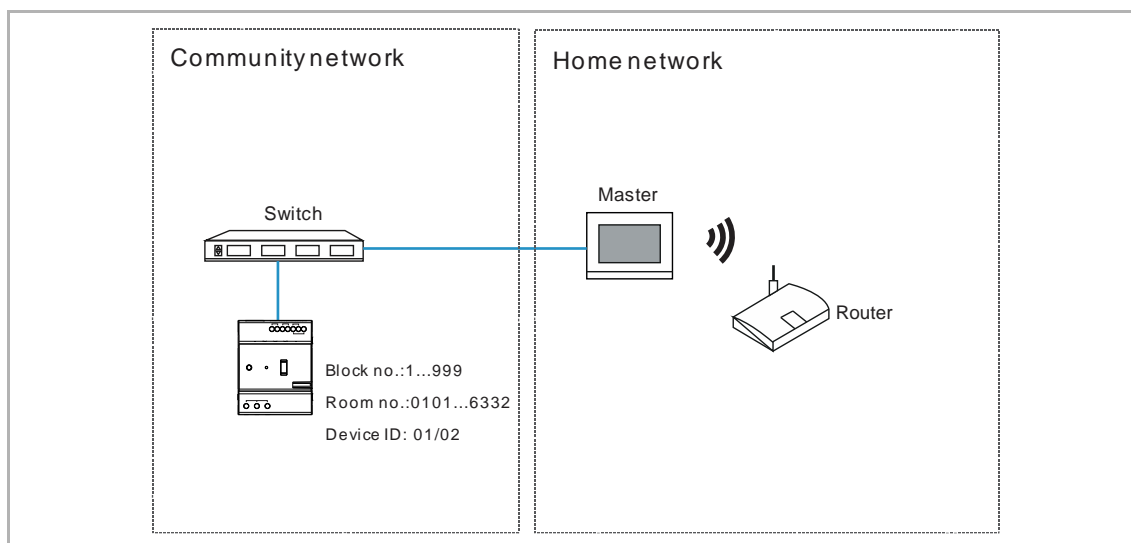


- [2] Select "Private" from the drop-down list.
- [3] Select "Internal IP gateway".
- [4] Enter the device number (01...32).
- [5] Select the network type, it can set to "DHCP", "Customizable address" or "ABB Legacy".
 - If "ABB Legacy" is selected, IP address will be "10.0.x.x".
- [6] Tap "Save & Close".



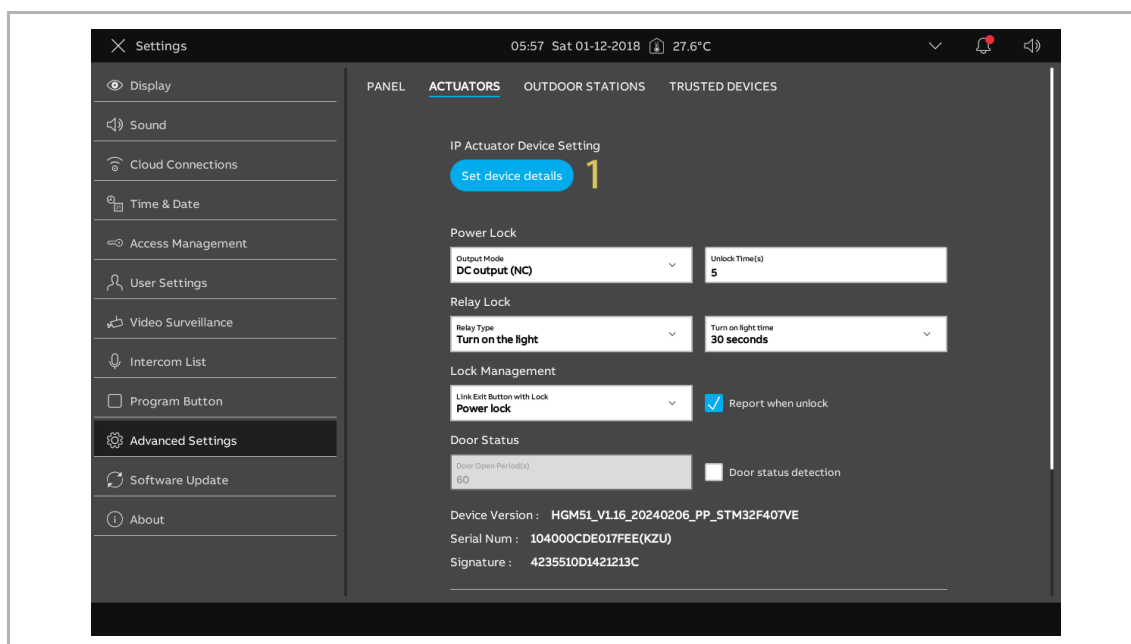
Location of IP Actuator = External

In this case, the IP Actuator is connected to the switch outside the apartment (see the diagram below).

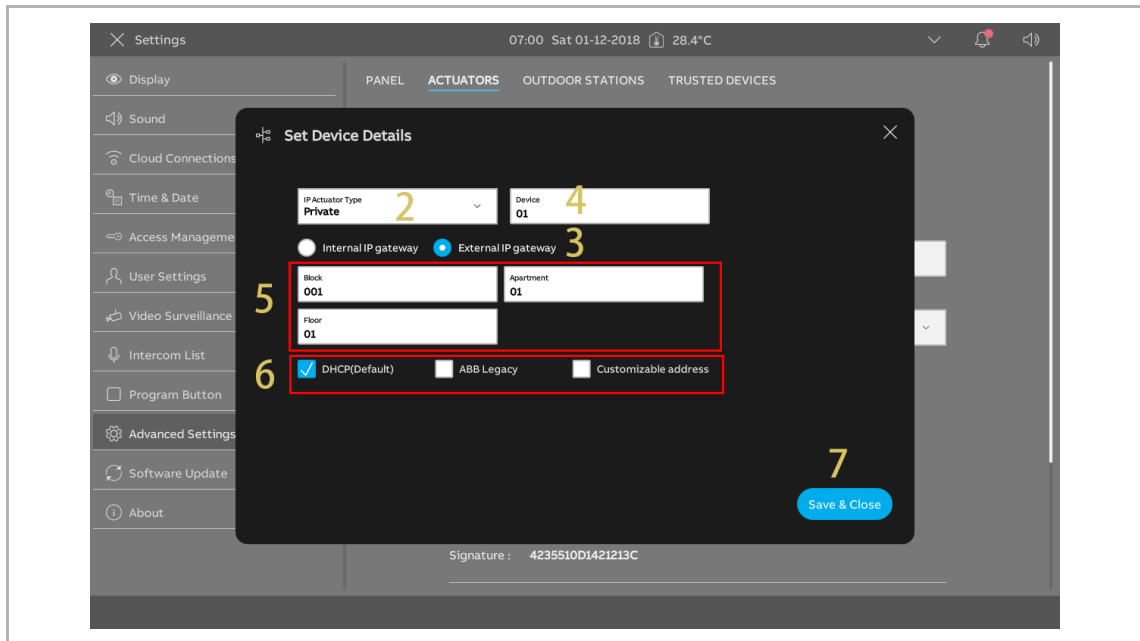


Please follow the steps below:

- [1] On the "Actuators" screen, go to the "IP Actuator Device Setting" section, tap "Set device details".



- [2] Select "Private" from the drop-down list.
- [3] Select "External IP gateway".
- [4] Enter the device number (01...02).
- [5] Enter the block number (001...999), floor number (01...63) and apartment number (01...32).
- [6] Select the network type, it can set to "DHCP", "Customizable address" or "ABB Legacy".
 - If "ABB Legacy" is selected, IP address will be "10.0.x.x".
- [7] Tap "Save & Close".



Note

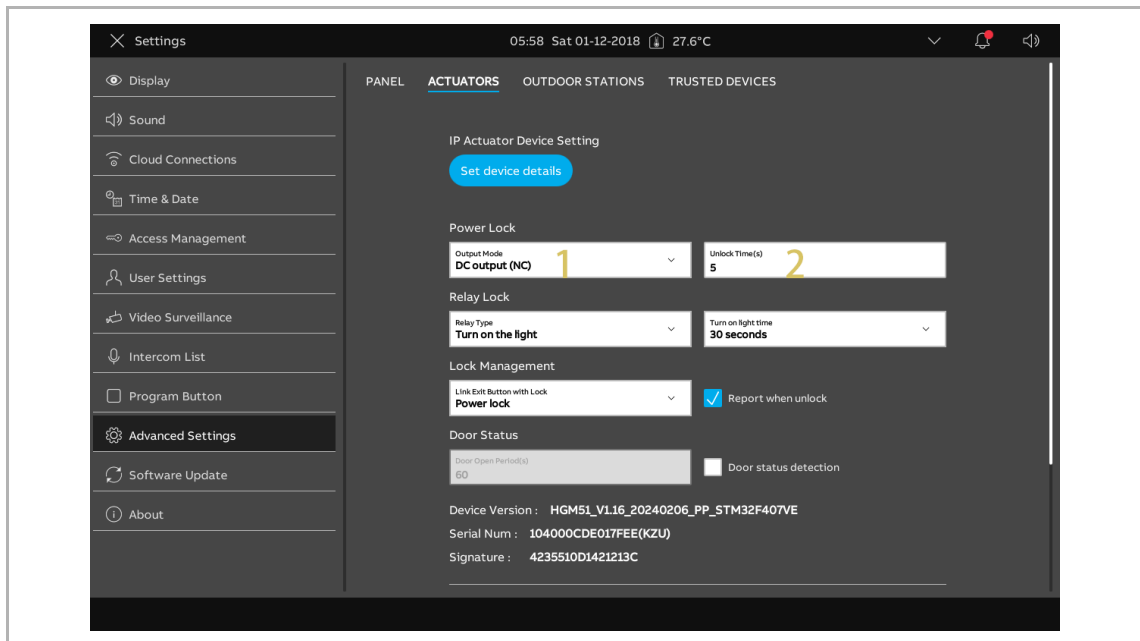
The external and internal types cannot be used in mixed scenarios in the same apartment.

8.1.3 Configuring the lock

Configuring the power lock

Please follow the steps below:

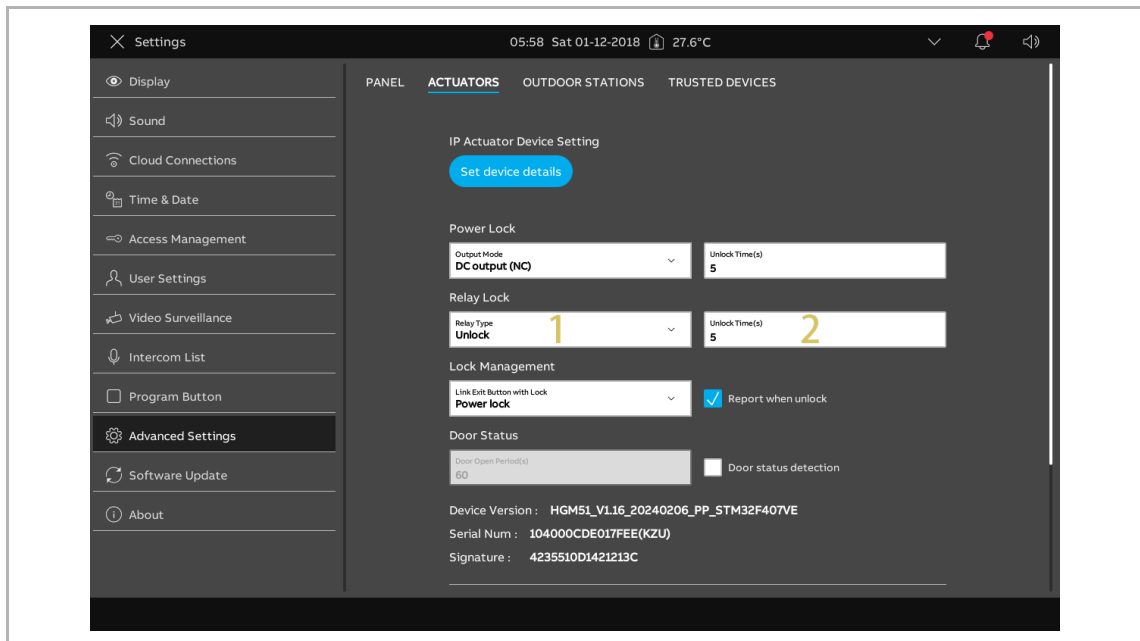
- [1] On the "Actuators" screen, go to the "Power Lock" section, select the output mode from the drop-down list. It can be set to "AC output", "DC output (NC)" or "DC output (NO)".
- [2] Enter the unlock time (default 5 seconds).



Configuring the relay lock

Please follow the steps below:

- [1] On the "Actuators" screen, go to the "Relay Lock" section, select the output mode from the drop-down list. It can be set to "Unlock" (default) or "Turn on the light".
- [2] Enter the unlock time (default 5 seconds) or the time for turning on the light (default 30 seconds).

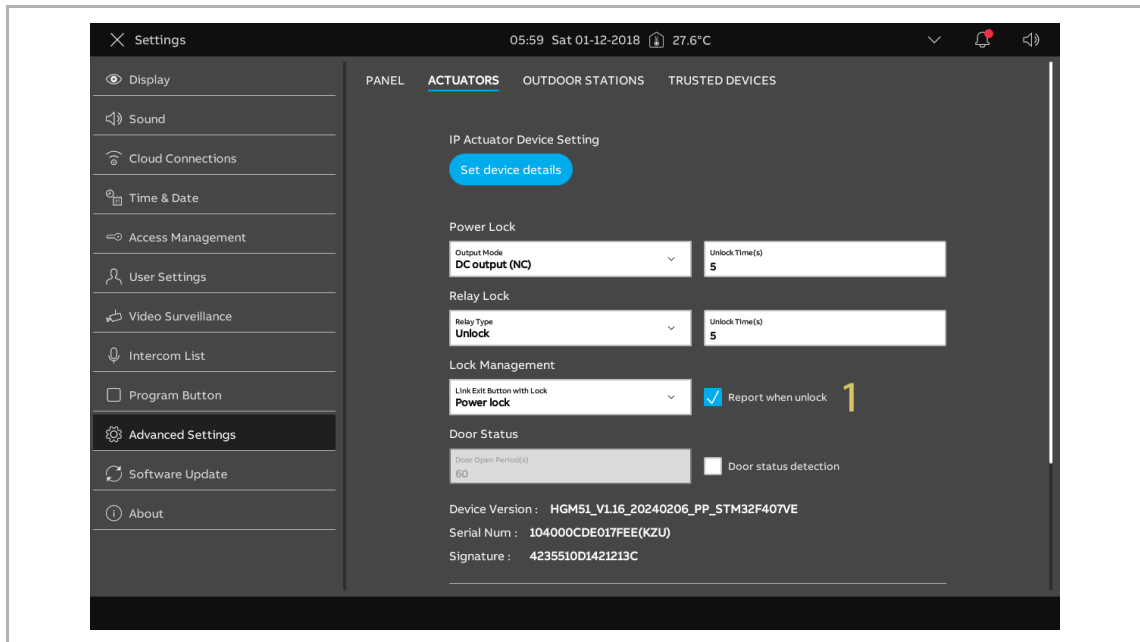


8.1.4 Configuring the "Report when unlock" function

If this function is enabled, each unlock record from the IP Actuator will be sent to SmartAP.

Please follow the steps below:

- [1] On the "Actuators" screen, go to the "Lock management" section, tick the check box to enable the function.

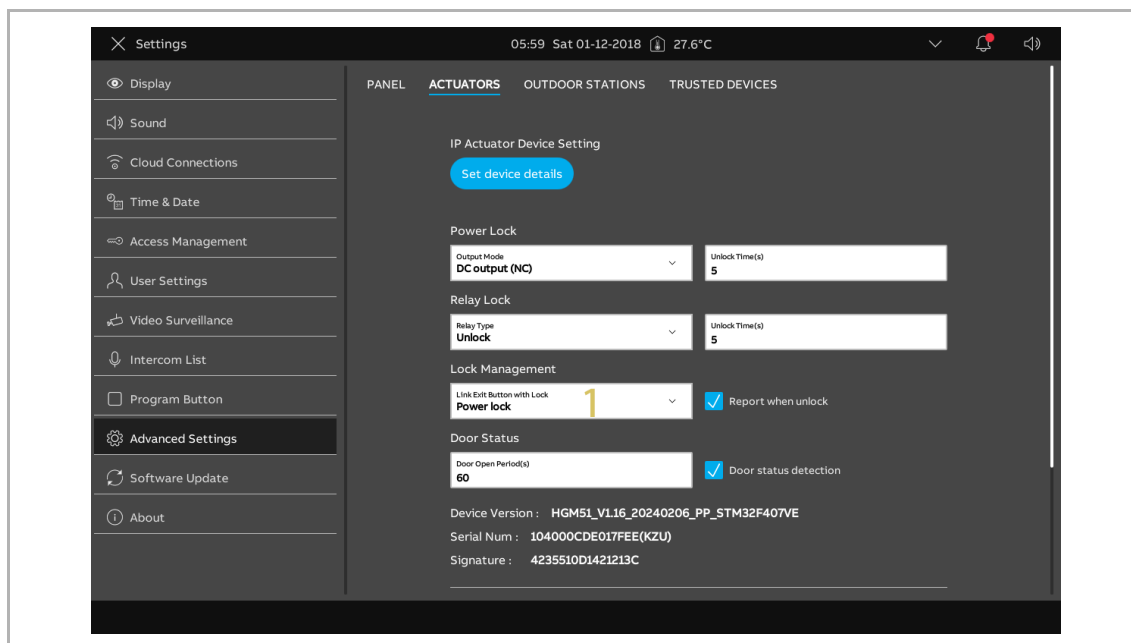


8.1.5 Linking the exit button with the lock

The exit button can be linked with the designated lock of the IP Actuator.

Please follow the steps below:

- [1] On the "Actuators" screen, go to the "Lock Management" section, select the lock type from the drop-down list. It can be set to "Power lock" or "Relay lock".

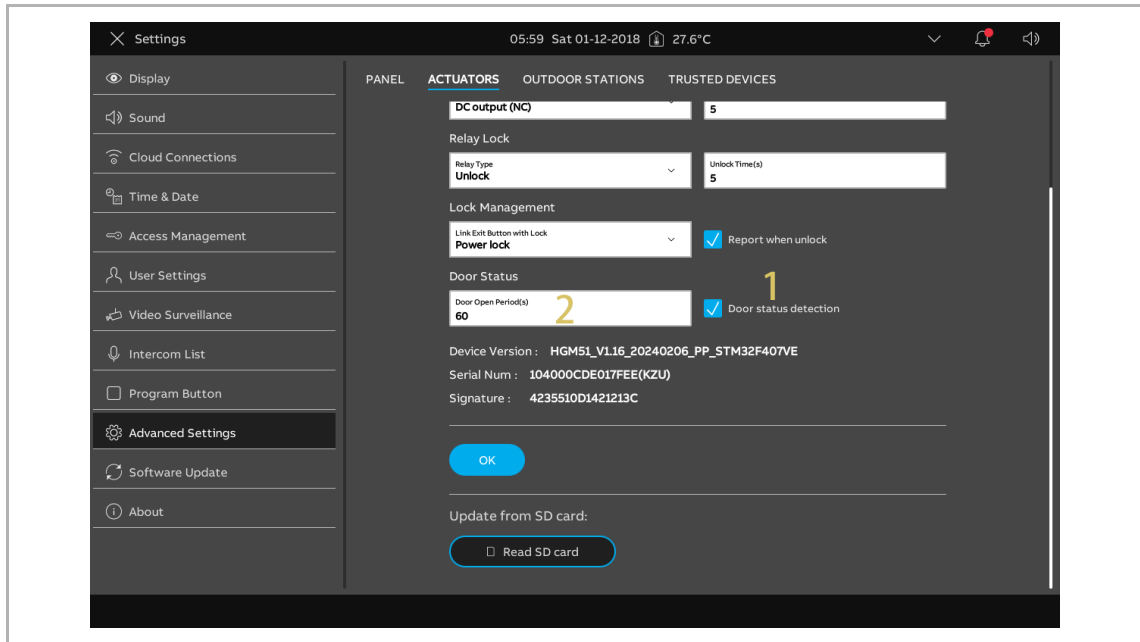


8.1.6 Configuring the "Door status detection" function

If this function is enabled, when the door is open longer than the setting value, the IP actuator will send an alarm to the SmartAP (a sensor should first be connected to the IP actuator).

Please follow the steps below:

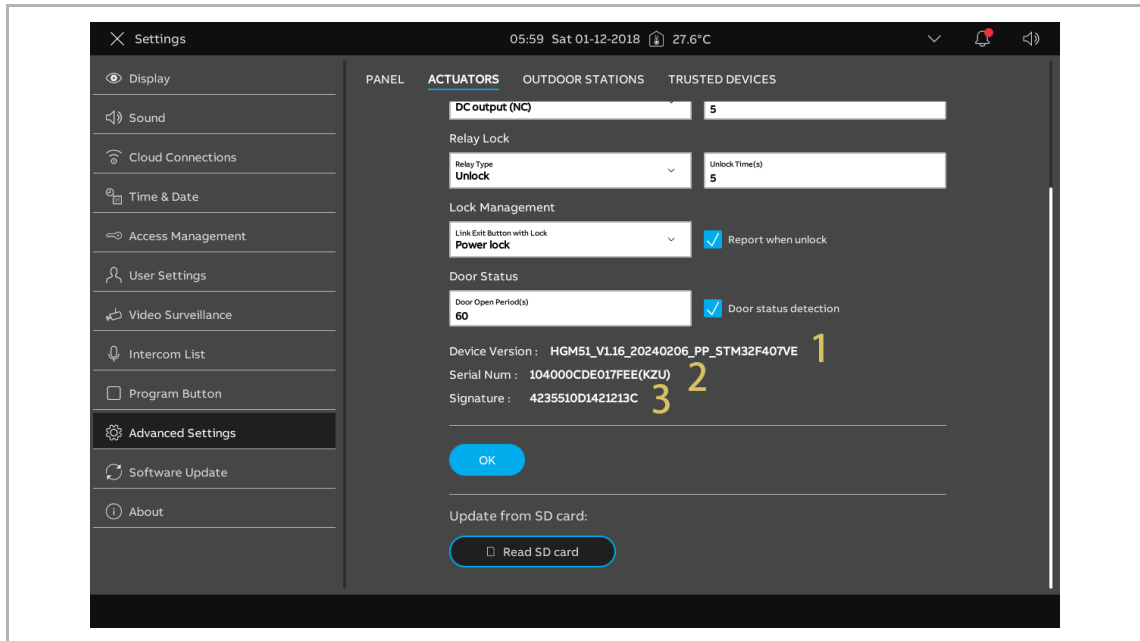
- [1] On the "Actuators" screen, go to the "Door Status" section, tick the check box to enable the function.
- [2] Enter the door open period (60 seconds default).



8.1.7 Viewing the information

Please follow the steps below:

[1] On the "Actuators" screen, scroll down to view the information.



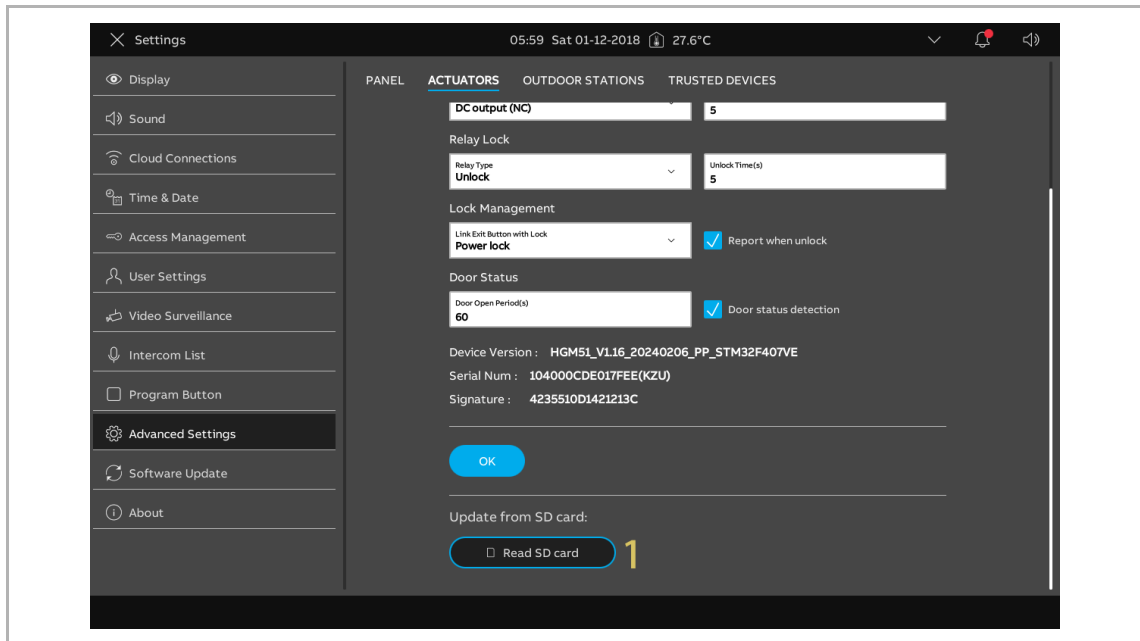
No.	Description
1	Software version
2	Serial number
3	Signature

8.1.8 Updating the firmware

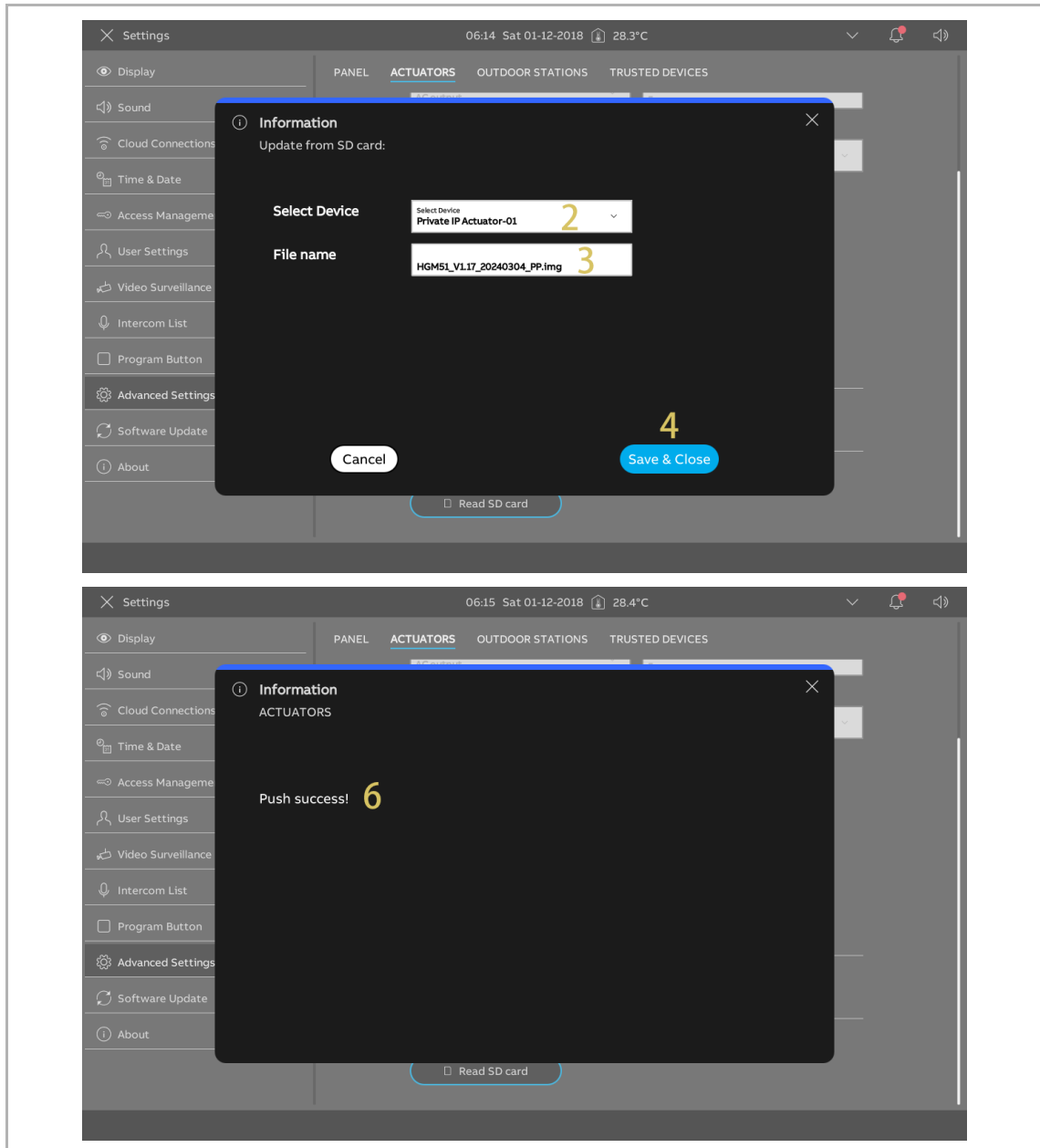
The IP Actuator can update the firmware via the Indoor Station which supports micro SD card. The IP Actuator must exit engineering mode before the firmware is upgraded.

Please follow the steps below:

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



- [2] Select the designated IP Actuator.
- [3] Select the updating file from SD card.
- [4] Tap "Save & Close".
- [5] "Loading..." will be displayed to indicate that the upgrade is in progress.
- [6] "Push success!" will be displayed if the upgrade is successful.



8.2 Configuring the settings on the SmartAP

8.2.1 Adding an IP Actuator



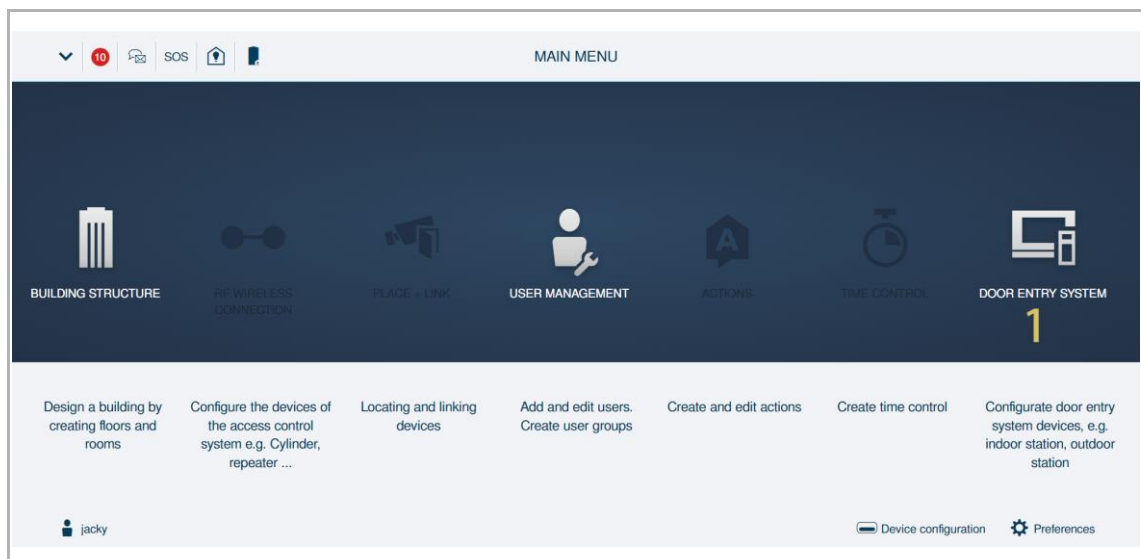
Note

Only an Outdoor Station without a certificate can be added by SmartAP. This Outdoor Station will lose its certificate if its physical address is changed.

The Outdoor Station needs to be powered on before being added.

On the "Main Menu" screen of "Smart Access Point", follow the steps below,

[1] Click "Door Entry System".



- [2] Click "Add device".
- [3] Select the device type from the drop-down list. It could be set to "Network IPA", "Building IPA" or "Private IPA".
- [4] Enter the device address,
- [5] This function is available only when device type is set to "Second-confirm station".
 - If the Outdoor Station is installed in the community network, "Installed in the community network" should be enabled.
- [6] Enter the serial number.
- [7] Click "Save".

The screenshot shows the 'ADD DEVICE' form in the 'DOOR ENTRY SYSTEM' interface. The form is titled 'ADD DEVICE' and is part of the 'OUTDOOR STATIONS' section. It contains the following fields and options:

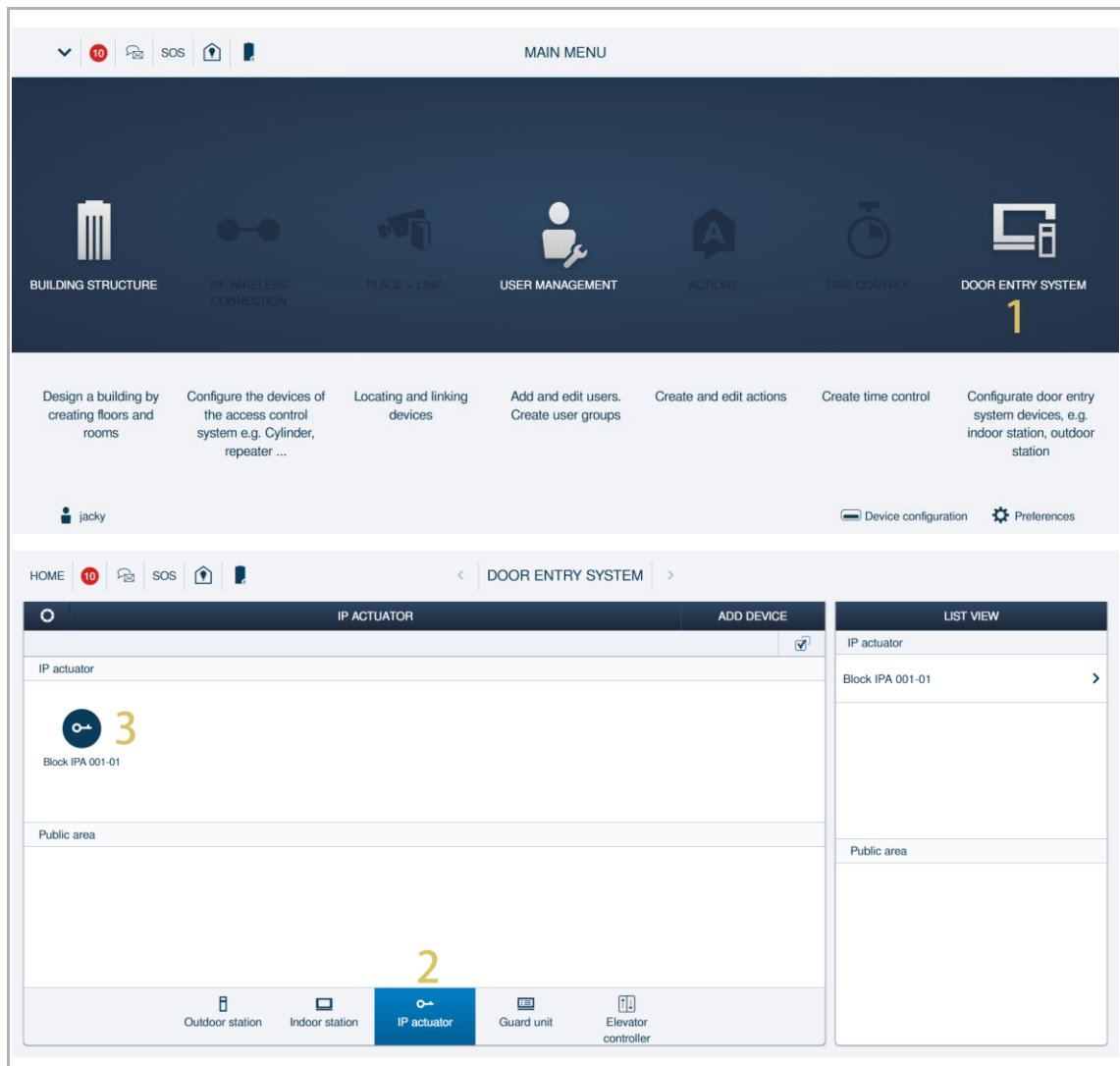
- Device type:** A dropdown menu set to 'Private IPA'.
- Device addr.:** Four input fields, each containing the number '1'.
- Installed in the community network:** A checkbox that is checked.
- Serial No.:** An input field containing the serial number '104000CDE017FEE'.

The form has 'Cancel' and 'Save' buttons at the bottom. The interface also shows a sidebar with 'Outdoor stations' and 'Public area' sections, and a bottom navigation bar with icons for 'Outdoor station', 'Indoor station', 'IP actuator', 'Guard unit', and 'Elevator controller'.

8.2.2 Accessing the designated IP Actuator screen

Please follow the steps below:

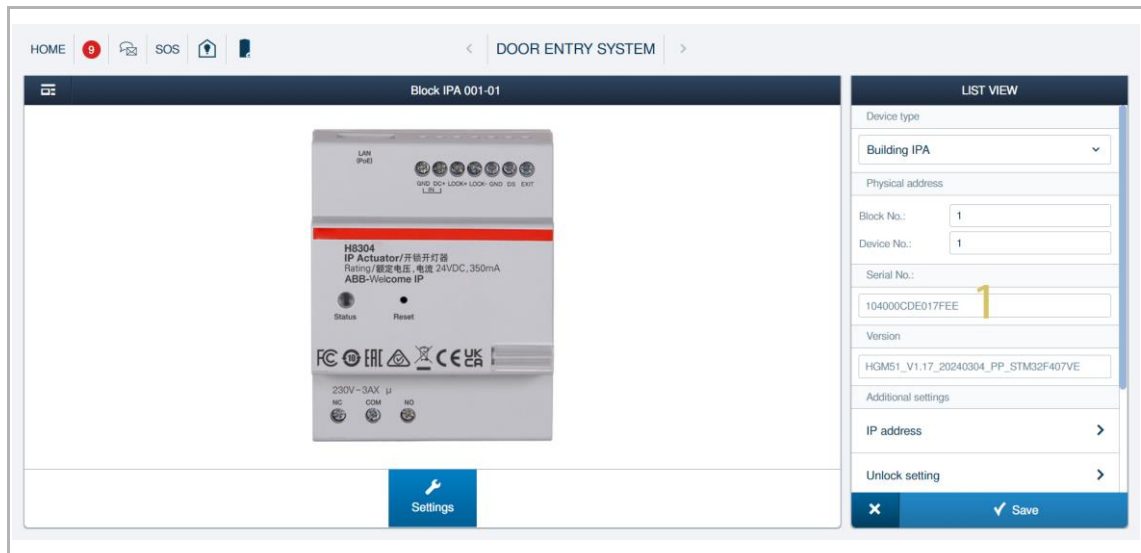
- [1] On the "Main Menu" screen, click "Door Entry System".
- [2] Click "IP Actuator".
- [3] Click the designated IP Actuator to access the corresponding screen.



8.2.3 Viewing the serial number

Please follow the steps below:

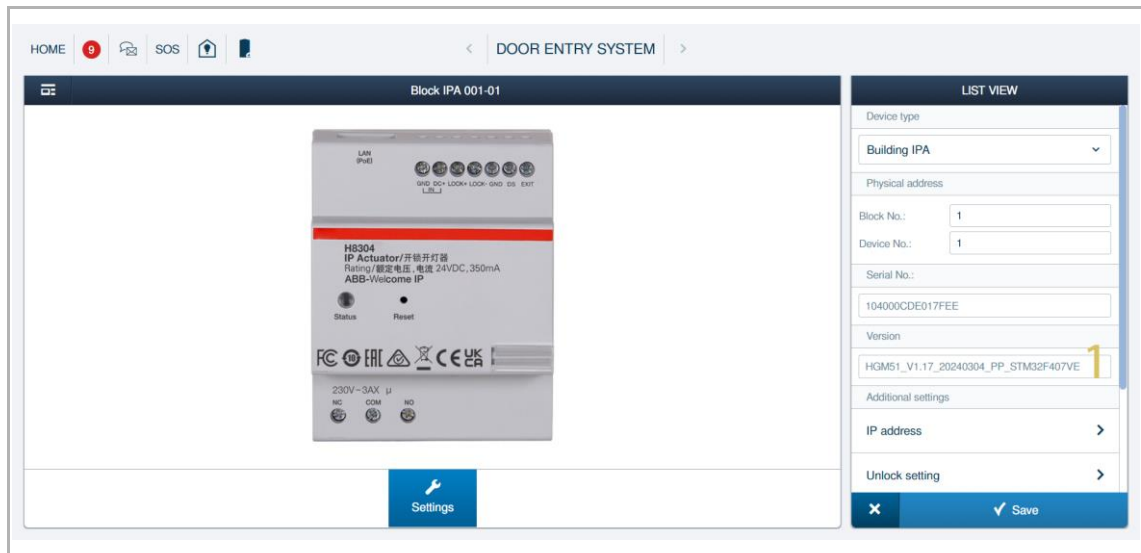
- [1] On the designated IP Actuator screen, go to the "Serial No." section to view the serial number.



8.2.4 Viewing the version

Please follow the steps below:

- [1] On the designated IP Actuator screen, go to the "Version" section to view the firmware version.

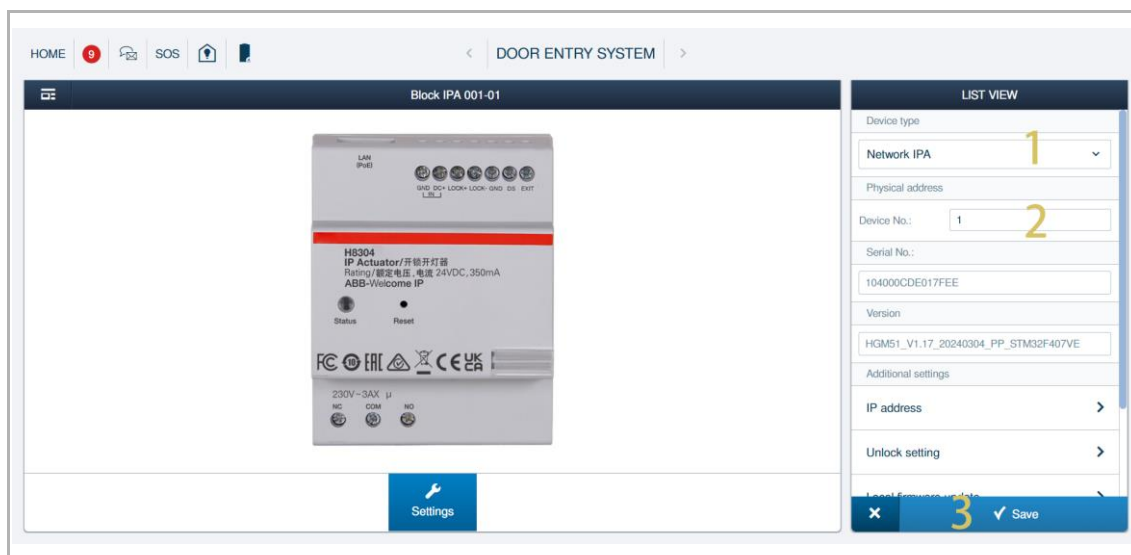


8.2.5 Configuring the physical address

1. Network IPA

Please follow the steps below:

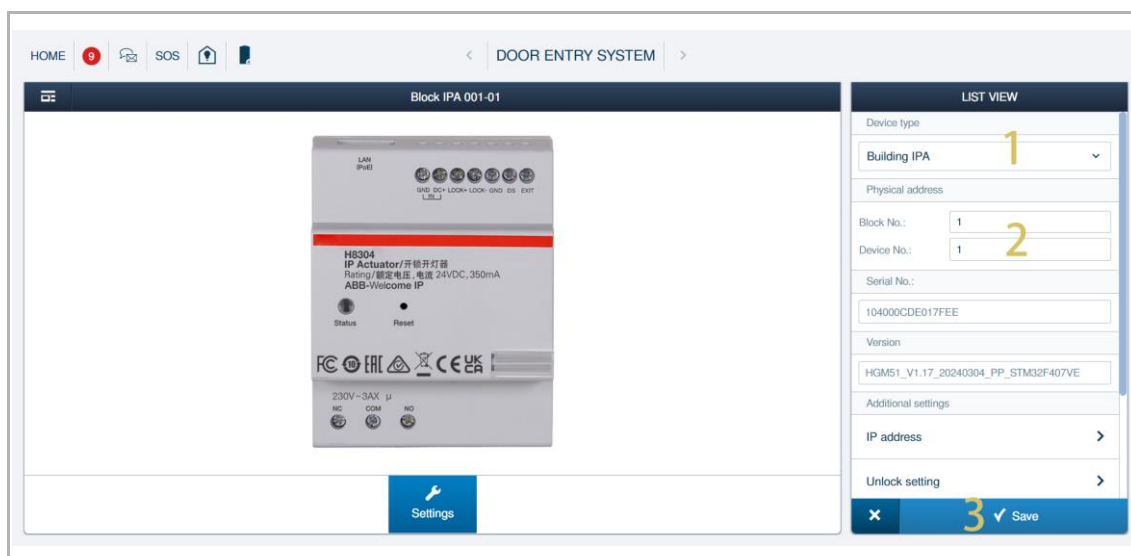
- [1] On the designated IP Actuator screen, go to the "Device type" section, select "Network IPA".
- [2] Go to the "Physical address" section, enter the device number (1...32).
- [3] Click "Save".



2. Building IPA

Please follow the steps below:

- [1] On the designated IP Actuator screen, go to the "Device type" section, select "Building IPA".
- [2] Go to the "Physical address" section, enter the block number (1...999) and the device number (1...32).
- [3] Click "Save".



3. Private IPA

Please follow the steps below:

- [1] On the designated IP Actuator screen, go to the "Device type" section, select "Private IPA".
- [2] Go to the "Physical address" section, enter the physical address:
- [3] Click "Save".

The screenshot displays the configuration interface for the H8304 IP Actuator. The main panel shows a photograph of the device, which is a white rectangular unit with a red stripe and various labels including 'H8304 IP Actuator/开锁开灯器', 'Rating/额定电压, 电流 24VDC, 350mA', and 'ABB-Wiscome IP'. The right sidebar, titled 'LIST VIEW', contains the following configuration fields:

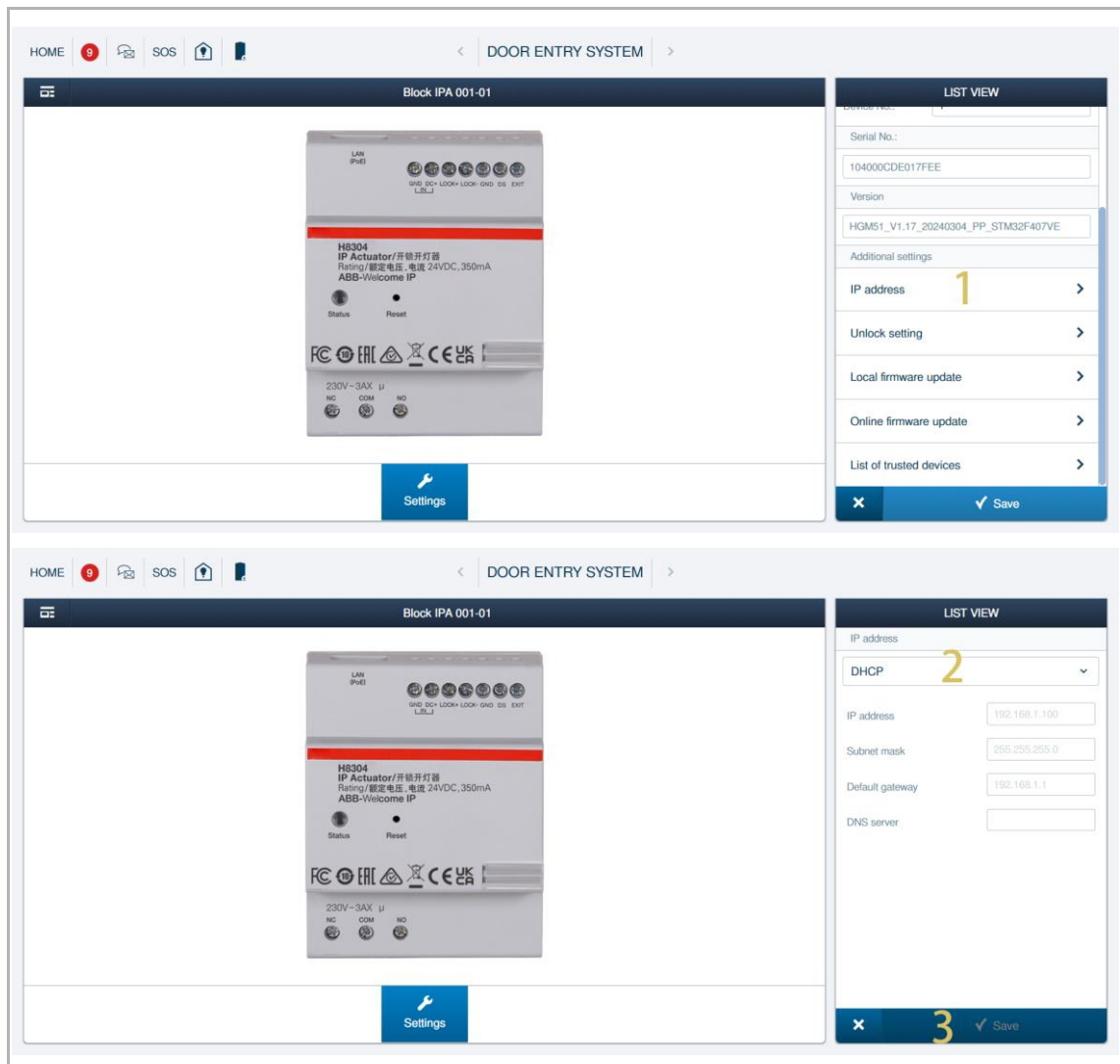
- Device type:** A dropdown menu with 'Private IPA' selected. A yellow '1' is next to it.
- Physical address:** Fields for Block No. (1), Floor No. (0), Room No. (1), and Device No. (1). A yellow '2' is next to the Floor No. field.
- Serial No.:** A text field containing '104000CDE017FEE'.
- Version:** A text field containing 'HGM51_V1.17_20240304_PP_STM32F407VE'.
- Additional settings:** A section with an 'IP address' field and a 'Save' button. A yellow '3' is next to the 'Save' button.

At the bottom of the main panel, there is a blue 'Settings' button.

8.2.6 Configuring the IP address

Please follow the steps below:

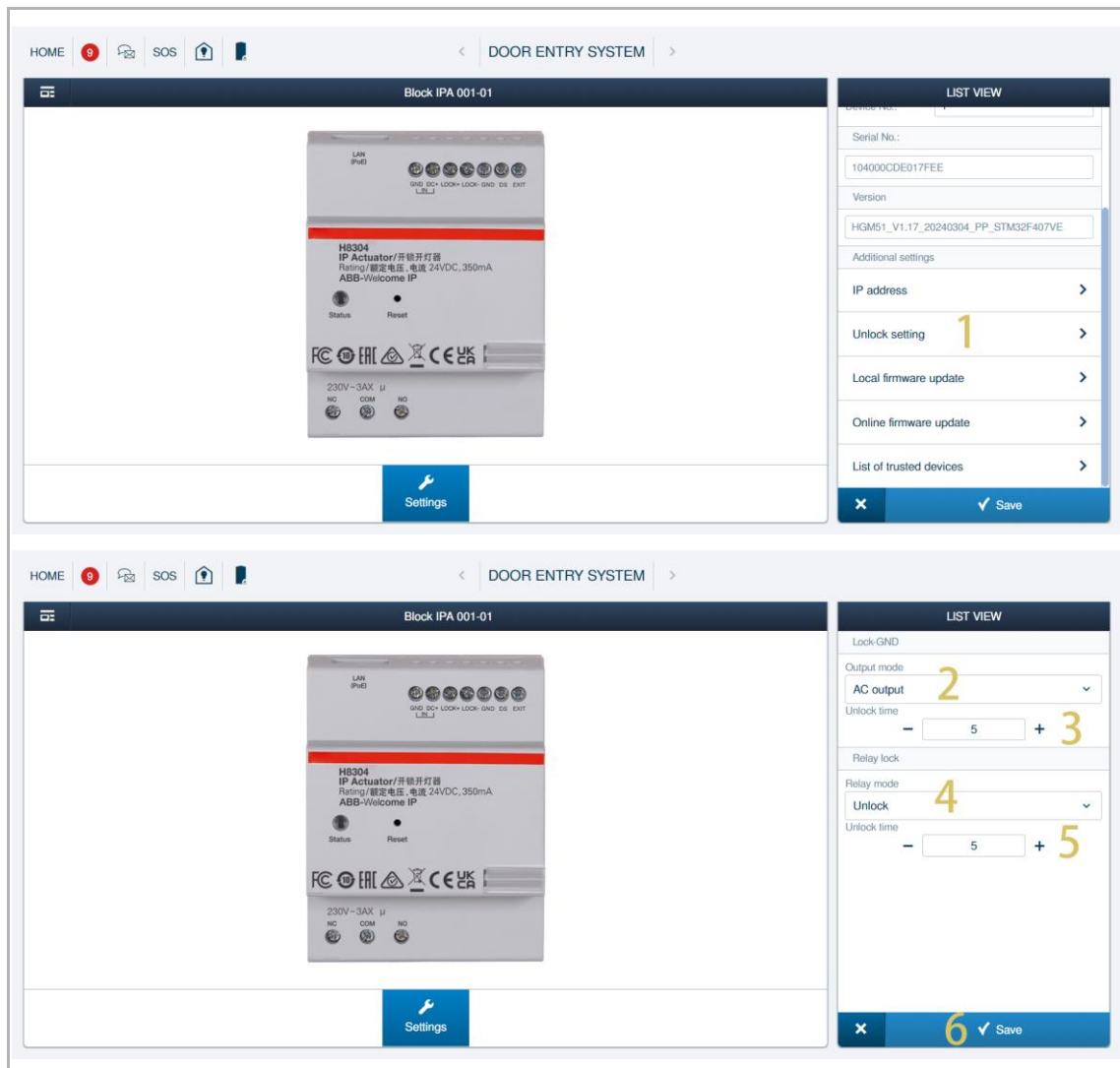
- [1] On the designated IP Actuator screen, go to the "Additional settings" section, click "IP address".
- [2] Select the network type, it can set to "DHCP" or "Static address".
 - If "Static address" is selected, you need to enter the IP address manually.
- [3] Click "Save".



8.2.7 Configuring the lock

Please follow the steps below:

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



8.2.8 Configuring the trusted devices

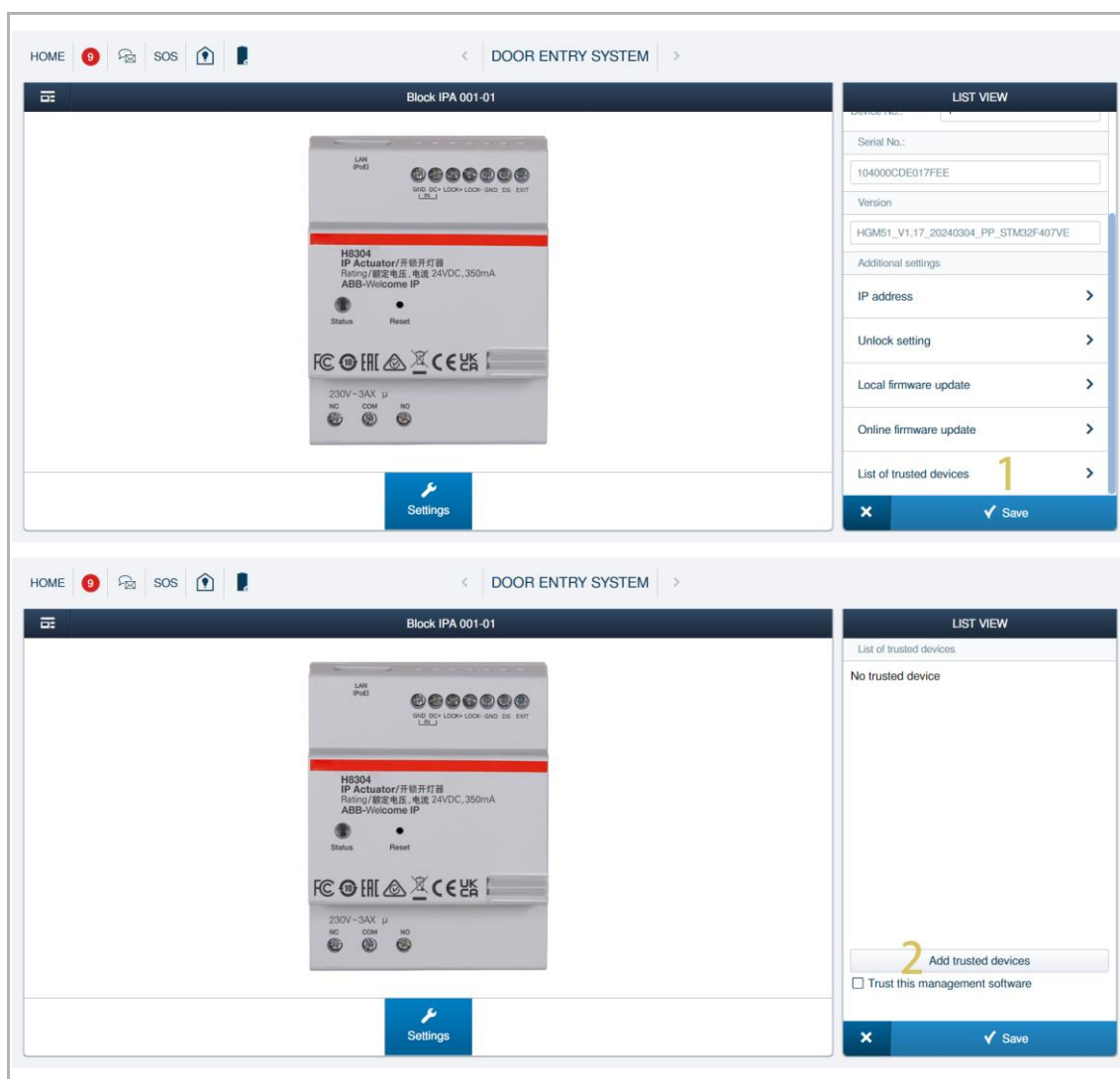
If you want to release the lock on the IP Actuator, you need to check:

- If the Indoor station and the IP Actuator have been signed on "Smart Access Point".
- If the Indoor Station has been added to the trusted list on the IP Actuator.

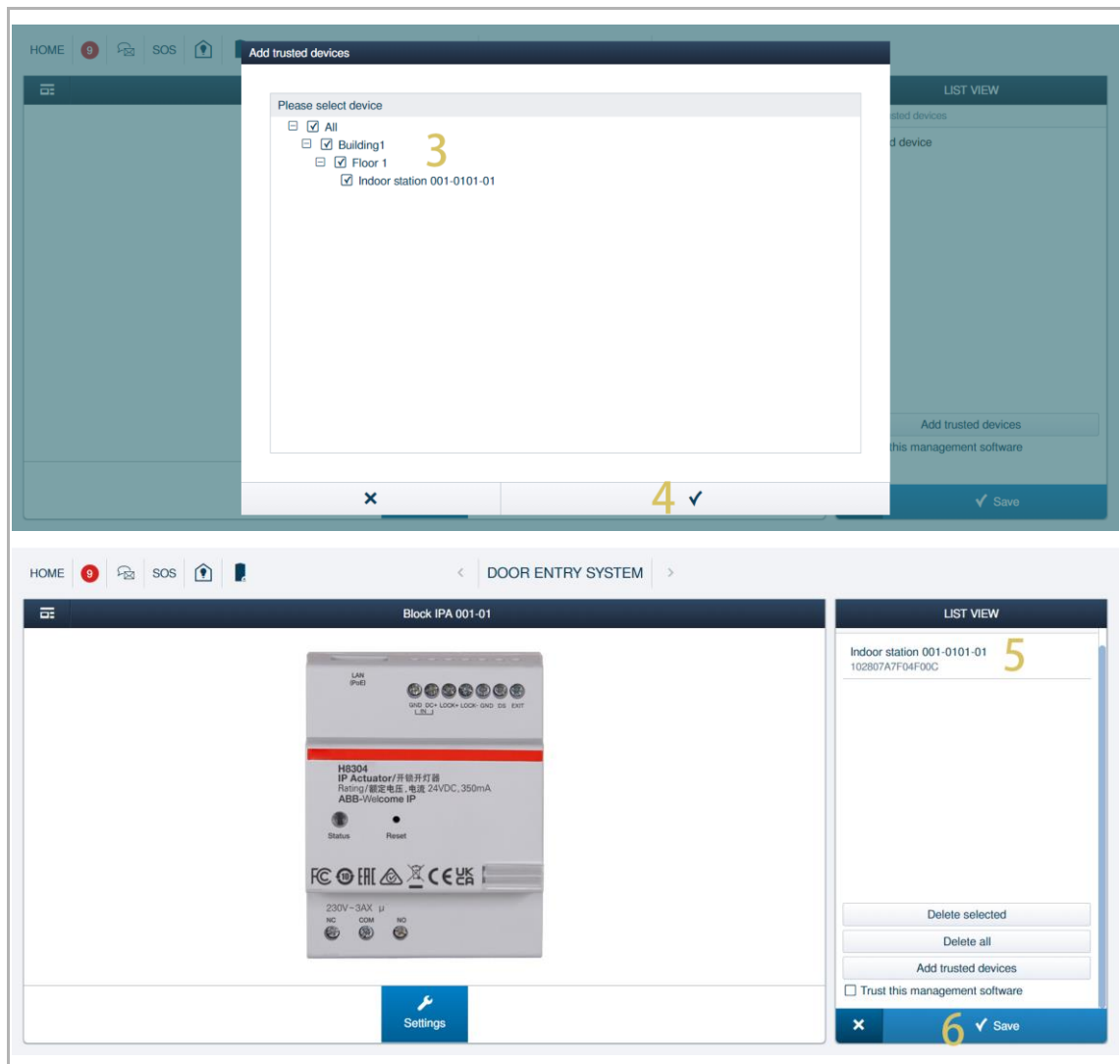
Please follow the steps below:

[1] On the designated IP Actuator screen, click "List of trusted devices".

[2] Click "Add trusted devices".



- [3] Tick the check boxes to select the devices to be trusted.
- [4] Click "✓".
- [5] The result is displayed on the screen.
- [6] Click "Save".

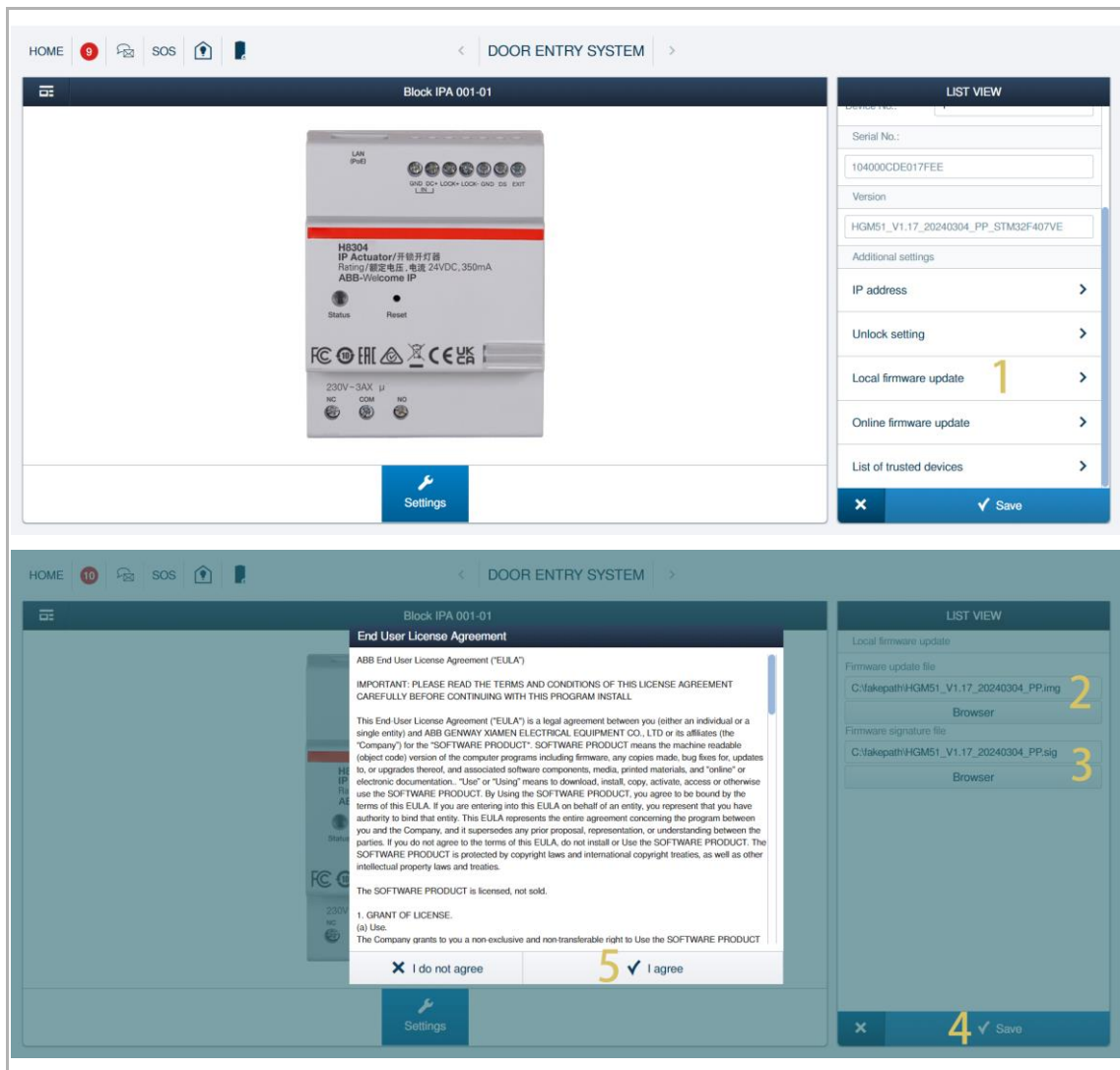


8.2.9 Updating the firmware

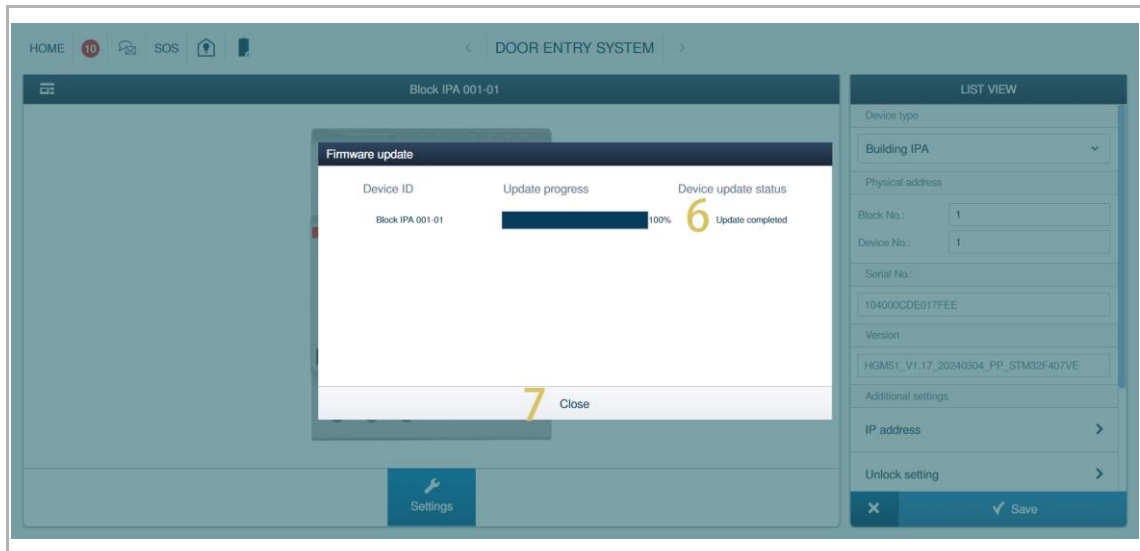
1. Local firmware update

Please follow the steps below:

- [1] On the designated IP Actuator 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.



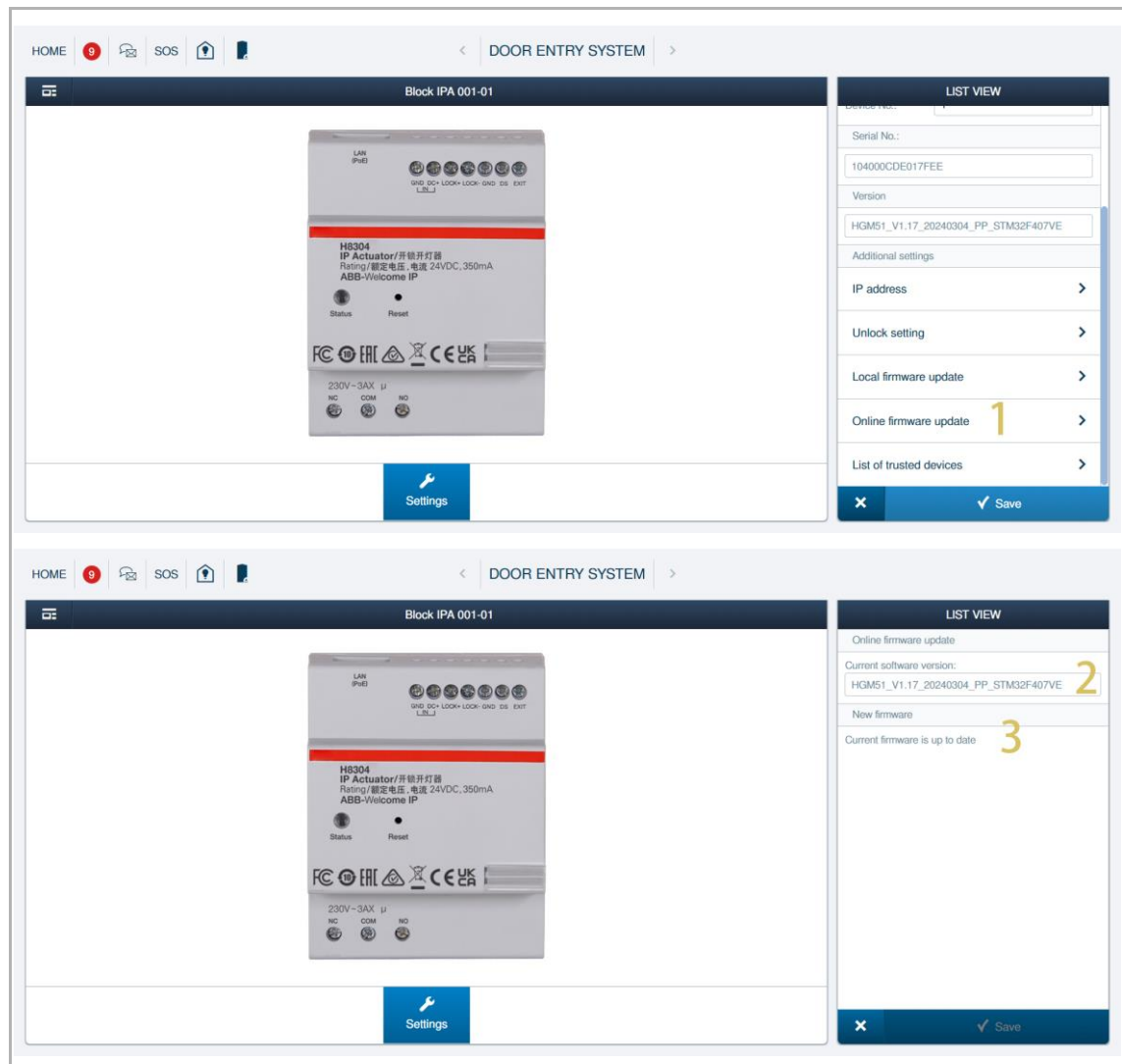
- [6] Update status will be displayed.
- [7] Click "Close" when the update is completed.



2. Online firmware update

Please follow the steps below:

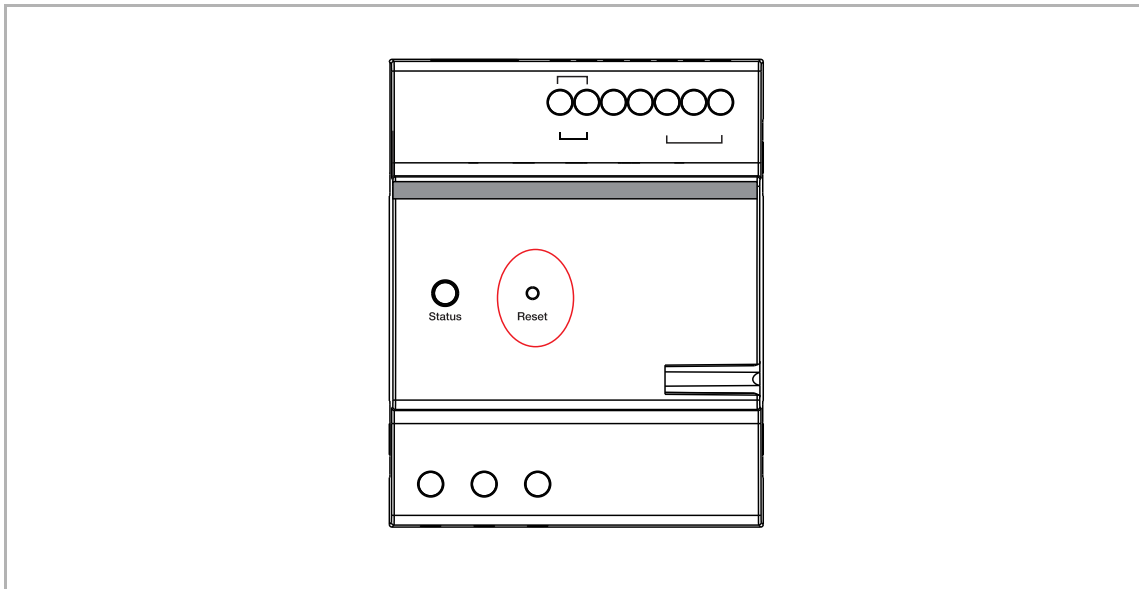
- [1] On the designated IP Actuator screen, click "Online firmware update".
- [2] Current firmware version will be displayed.
- [3] "Current firmware is up to date" will be displayed if no newer version is available.



8.3 Restoring to factory default

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.



9 Cyber security

9.1 Disclaimer

H8304 product is designed to be connected and to communicate information and data via a network interface, which should be connected to a secure network. It is customer's sole responsibility to provide and continuously ensure a secure connection between the product and customer's network or any other network (as the case may be) and to establish and maintain appropriate measures (such as but not limited to the installation of firewalls, application of authentication measures, encryption of data, installation of antivirus programs, etc.) to protect the H8304 product, the network, its system and interfaces against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. Busch-Jaeger Ltd and its affiliates are not liable for damages and/or losses related to such security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information.

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

9.2 Performance and service

Network performance

Type	Value
Ethernet	6 Mbps (8,928 packets/sec)
ARP	40 packets/sec
ICMP	1 Mbps (1,488 packets/sec)
IP	20 packets/sec

Port and service

Port		
7777	TCP	To be used for device management
8887	TCP	To be used for firmware update
10777	TLS	Secure channel for device management

9.3 Deployment guideline

All devices need to work in security mode by default and. all devices on one system are to be signed by a public CA at commissioning stage; normally the management software acts as CA.

It is suggested that compatible mode is only used when the device needs to communicate with previous generation products. In this mode, data transmission between devices is not encrypted, may lead to data leaks and involves a risk of attacks.

When user decide to remove the device from system, user shall reset the device to factory setting in order to remove all the configuration data and sensitive data in the device. This will prevent sensitive data leak.

It is recommended to apply "MAC filter" and "Rate limiter" in the switch to prevent DOS attack.

9.4 Upgrading

The device supports firmware updates via the management software, where a signature file is used to verify the authentication and integrity of the firmware.

9.5 Backup/restore

None

9.6 Malware prevention solution

The device H8304 is not susceptible to malware, because custom code cannot be executed on the system. The only way to update the software is by firmware upgrading. Only firmware signed by Busch-Jaeger can be accepted.

9.7 Password rule

None

10 Notice

We reserve the right to at all times make technical changes as well as changes to the contents of this document without prior notice.

The detailed specifications agreed to at the time of ordering apply to all orders. Busch-Jaeger accepts no responsibility for possible errors or incompleteness in this document.

We reserve all rights to this document and the topics and illustrations contained therein. The document and its contents, or excerpts thereof, must not be reproduced, transmitted or reused by third parties without prior written consent by Busch-Jaeger.

Service

ABB AG – BUSCH-JAEGER
Freisenbergstr. 2, DE-58513 Lüdenscheid

BUSCH-JAEGER.de
go.abb/contact