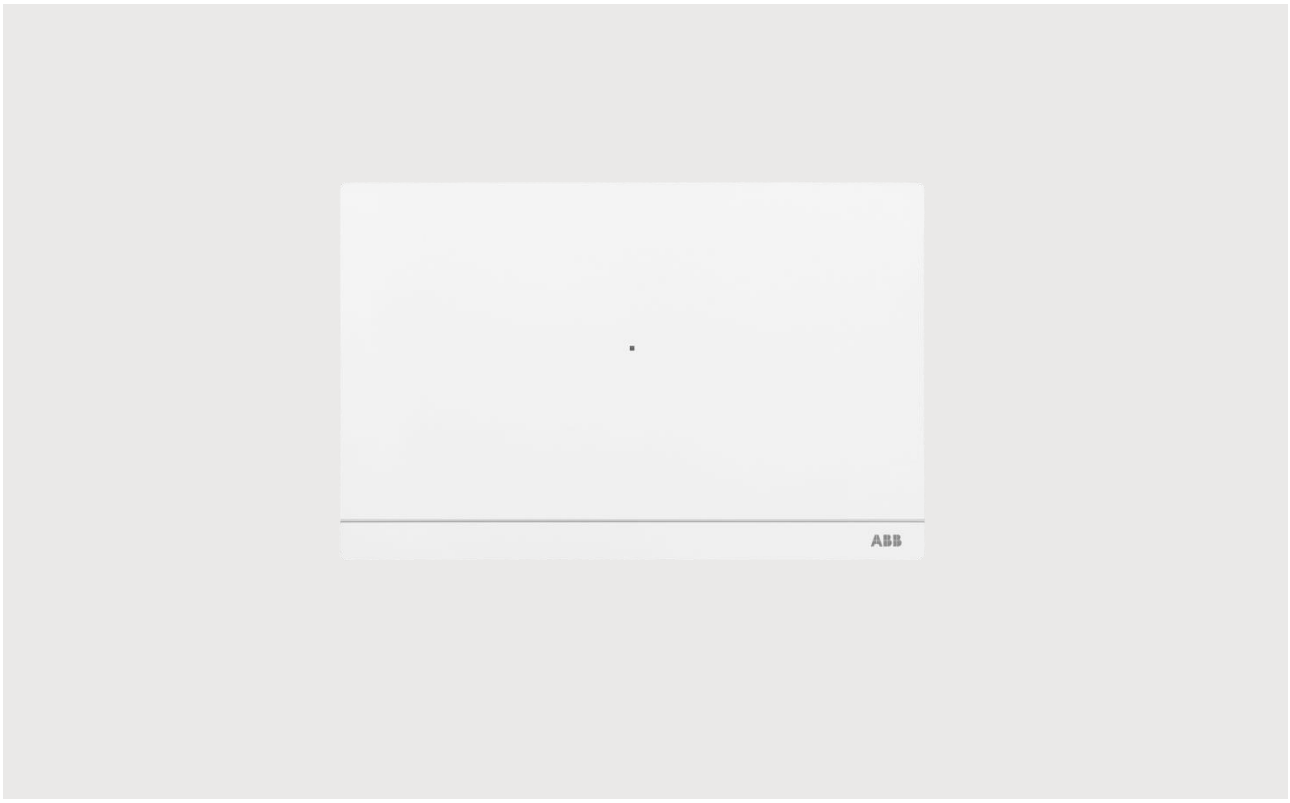
2TMD041800D0088 | 28.11.2024

Producthandboek
ABB-Welcome IP
ABB-AccessControl

D04011 Smart Access Point Pro



1 Over de handleiding 6
2 Veiligheid 6
3 Beoogd gebruik 6
4 Milieu 7
4.1 ABB-apparaten 7
5 Productbeschrijving 8
5.1 Apparaattype 8
5.2 Terminalbeschrijving 9
6 Technische gegevens 11
7 Montage/installatie 12
7.1 Eis voor de installateur 12
7.2 Montage 13
8 Ingebruikname 15
8.1 Systeemvereisten 15
8.2 Toegang tot SmartAP via UPnP 18
8.3 Eerste configuratie 19
8.4 Inlogscherm 31
8.5 Configuratiescherm 32
8.6 Besturingsscherm 33
8.7 Instellingen 34
8.7.1 Snelle instellingen openen 34
8.7.2 Instellingen: algemeen openen 35
8.7.3 Versie-informatie 36
8.7.4 Disclaimer informatie 37
8.7.5 Netwerkinstellingen 38
8.7.6 Taal 39
8.7.7 Tijdinstellingen 40
8.7.8 MyBuildings-instellingen 43
8.7.9 Instellingen APP-modus 45
8.7.10 Instellingen Externe bevoegdheid 46
8.7.11 Onvif IPC-instellingen 48
8.7.12 Alarm-meldingsinstellingen 51
9 Door Entry system-apparaten bedienen 55
9.1 Topologie buiten-/binnenpost 55
9.2 Apparaatbeheer 58
9.2.1 Apparaten automatisch toevoegen 59
9.2.2 Apparaten handmatig toevoegen 62
9.3 Vertrouwde apparaten beheren 64
9.3.1 Vertrouwde apparaten voor de buitenpost beheren 64
9.3.2 Vertrouwde apparaten voor de IP-aktor beheren 69

9.3.3 Vertrouwde apparaten voor "Smart Access Point" beheren ... 74
9.3.4 Nooddeblokkering ... 78
9.4 Binnenpost configureren ... 80
9.4.1 Taal wijzigen ... 81
9.4.2 Apparaat een andere naam geven ... 82
9.4.3 Serienummer bekijken ... 83
9.4.4 Fysiek adres beheren ... 84
9.4.5 Logisch adres beheren ... 89
9.4.6 Screensaver beheren ... 90
9.4.7 Etageplattegrond beheren ... 91
9.4.8 Instellingen kopiëren ... 92
9.5 Buitenpost configureren ... 93
9.5.1 Taal wijzigen ... 94
9.5.2 Fysiek adres beheren ... 95
9.5.3 Ontgrendelinstelling ... 98
9.5.4 Tijdsynchronisatie ... 100
9.5.5 Liftbesturing beheren ... 101
9.5.6 Oproep initiëren via fysiek adres ... 102
9.5.7 Oproep initiëren via logisch adres ... 103
9.5.8 Oproep initiëren via namenlijst ... 111
9.5.9 Welkomstbericht beheren ... 118
9.5.10 Gegevens ontwikkelaar beheren ... 119
9.5.11 Bulletin beheren ... 120
9.5.12 QR-code voor deblokkering beheren ... 121
9.5.13 Firmware updaten ... 123
9.6 Portiercentrale configureren ... 124
9.6.1 Apparaatnummer instellen ... 125
9.6.2 Serienummer bekijken ... 126
9.6.3 Firmware updaten ... 127
9.7 IP-aktor configureren ... 128
9.7.1 Serienummer bekijken ... 129
9.7.2 Fysiek adres beheren ... 130
9.7.3 Ontgrendelinstelling ... 132
9.7.4 Vertrouwde apparaten beheren ... 133
9.7.5 Aan buitenpost gerelateerde IP-aktor deblokkeren ... 134
9.8 Apparaten verwijderen ... 137
9.8.1 Apparaten één voor één verwijderen ... 137
9.8.2 Apparaten in batches verwijderen ... 138

10 AccessControl-apparaten bedienen ... 139
10.1 AccessControl-topologie ... 139
10.2 Een gebouw maken ... 145
10.2.1 Een gebouw maken via "Smart Access Point" ... 145
10.2.2 Een gebouw maken via de Welcome-app ... 150
10.3 Vertrouwde apparaten toevoegen en lokaliseren ... 154
10.3.1 "Smart Access Point" lokaliseren ... 155
10.3.2 Toevoegen en lokaliseren van de "elektronische slotcilinder" ... 156
10.3.3 Toevoegen en lokaliseren van een "RF-repeater" ... 157
10.3.4 Toevoegen en lokaliseren van een "RF/IP-gateway". ... 158
10.4 Apparaten aansluiten ... 159

10.4.1 "RF-repeater aansluiten" ... 161
10.4.2 "Elektronische slotcilinder" verbinden ... 163
10.4.3 AccessControl-apparaat is offline ... 167
10.5 Goedkeuringen toewijzen ... 169
10.5.1 Rechten toewijzen aan een gebruiker ... 169
10.5.2 Rechten toewijzen aan gebruikers ... 174
10.5.3 Offline-dag instellen ... 175
10.5.4 Noodkaarten beheren ... 176
10.6 Apparaten configureren ... 178
10.6.1 "Elektronische slotcilinder" configureren ... 178
10.6.2 "RF-repeater" configureren ... 179
10.6.3 "RF/IP-gateway" configureren ... 180
10.6.4 Kantoormodus ... 185
10.7 Apparaten besturen via het "Smart Access Point" ... 191
10.7.1 Apparaten besturen via de plattegrond ... 193
10.7.2 Apparaten besturen via matrix ... 201
10.8 Apparaten besturen via Welcome-app ... 202
10.8.1 "Smart Access Point" met Welcome-app koppelen ... 202
10.8.2 Elektronische slotcilinder besturen via Welcome-app ... 208
10.9 Back-up beheren ... 210
10.10 Rechten verwijderen ... 211
10.10.1 Rechten van een gebruiker verwijderen ... 211
10.10.2 Rechten van de gebruikers in een groep verwijderen ... 213
10.11 Apparaten loskoppelen ... 215
10.11.1 "Elektronische slotcilinder" loskoppelen ... 217
10.11.2 "RF-repeater" loskoppelen ... 221
10.12 Apparaten verwijderen ... 224
10.12.1 "Elektronische slotcilinder" verwijderen ... 225
10.12.2 RF-repeater verwijderen ... 226
10.12.3 RF/IP-gateway verwijderen ... 227
10.13 Een defecte "RF Repeater" vervangen ... 228
10.14 Verknoping tussen apparaten beheren ... 232
10.14.1 Verknoping toevoegen ... 233
10.14.2 Verknopingen beheren ... 235
10.14.3 Verknopingen verwijderen ... 236

11 Acties beheren ... 238
11.1 Actie toevoegen ... 239
11.2 Acties beheren ... 243
11.3 De actie verwijderen ... 244

12 Cyberveiligheid ... 245
12.1 Disclaimer ... 245
12.2 Performance and service and network performance ... 245
12.3 Deployment guideline ... 247
12.4 Upgrading ... 247
12.5 Backup/restore ... 247
12.6 Data pursing ... 248

12.7 Malware prevention solution 249
12.8 Default passwords and user accounts 249
12.9 Password rule 249
12.10 Logging 250

13 Bijlage 251
13.1 Een account registreren via het MyBuildings-portal 251
13.2 Wachtwoord voor de eerste beheerder resetten 252
13.3 Gebruikersbeheer 254
13.3.1 Gebruikersrollen 254
13.3.2 Gebruikers toevoegen 257
13.3.3 Gebruikersgroepen toevoegen 263
13.3.4 Gebruikers toewijzen aan een gebruikersgroep 265
13.3.5 Gebruiker configureren 267
13.3.6 Gebruikersgroep configureren 271
13.4 Firmware updaten 272
13.4.1 Firmware updaten voor "Smart Access Point" 272
13.4.2 Firmware updaten voor buiten-/binnenpost 274
13.4.3 Firmware updaten voor AccessControl-apparaten 278
13.5 Back-up beheren 280
13.5.1 Back-up maken 281
13.5.2 Back-up herstellen 282
13.5.3 Back-up verwijderen 283
13.5.4 Back-up naar pc exporteren 284
13.5.5 Back-up vanaf de pc importeren 285
13.6 Voorinstellingen herstellen 286
13.6.1 AccessControl-apparaten herstellen 286
13.6.2 Toegang tot het "Smart Access Point" op afstand 288
13.6.3 Functie "Afstandsbediening" herstellen 291
13.6.4 Alle voorinstellingen herstellen 292
13.7 Melding 293
13.7.1 Melding 294
13.7.2 Alarmrapport 295
13.7.3 Protocollen 296
13.7.4 Meldingen exporteren 297
13.8 Berichtencentrale 298
13.8.1 Een bericht maken en versturen 299
13.8.2 Een bericht bekijken en beantwoorden 300

14 Opmerkingen 301

1 Over de handleiding

Lees deze handleiding aandachtig door en houd rekening met de informatie die deze bevat. Hiermee kunt u letsel en schade aan eigendommen voorkomen en zowel een betrouwbare werking als een lange levensduur van het apparaat garanderen.

Bewaar deze handleiding op een veilige plaats.

Als u het apparaat doorgeeft, geef dan ook deze handleiding door.

ABB aanvaardt geen aansprakelijkheid voor het niet naleven van de instructies in deze handleiding.

2 Veiligheid

GEVAAR

Bij direct of indirect contact met spanningvoerende delen treedt er een gevaarlijke stroomschok in het lichaam op. Elektrische schok, brandwonden of de dood kunnen het gevolg zijn. Bij niet correct uitgevoerde werkzaamheden aan spanningvoerende delen bestaat brandgevaar.

– Voor montage en demontage eerst de netspanning uitschakelen!
– Werkzaamheden aan het 100 … 240V-stroomnet uitsluitend laten uitvoeren door een erkend elektrotechnisch installatiebedrijf.

3 Beoogd gebruik

Als onderdeel van het ABB-Welcome IP -systeem kan dit apparaat alleen worden gebruikt met accessoires van dat systeem.

4 Milieu

Overweeg de bescherming van het milieu!

Gebruikte elektrische en elektronische apparaten mogen niet via het huishoudelijk afval worden weggegooid. Breng uw apparaten naar het afvalstation of kijk online waar u ze kunt inleveren.

– Het apparaat bevat waardevolle grondstoffen die kunnen worden gerecycled. Breng het apparaat daarom naar de juiste inzamelplaats.

4.1 ABB-apparaten

Alle verpakkingsmaterialen en apparaten van ABB dragen de markeringen en testzegels voor een juiste verwijdering. Voer het verpakkingsmateriaal, de elektrische apparaten en de componenten altijd af via een erkend inzamelpunt of verwijderingsbedrijf.

ABB-producten voldoen aan de wettelijke vereisten, met name de wetten betreffende elektronische en elektrische apparaten en de REACH-verordening.

(EU Richtlijn 2012/19/EU AEEA en 2011/65/EU RoHS)

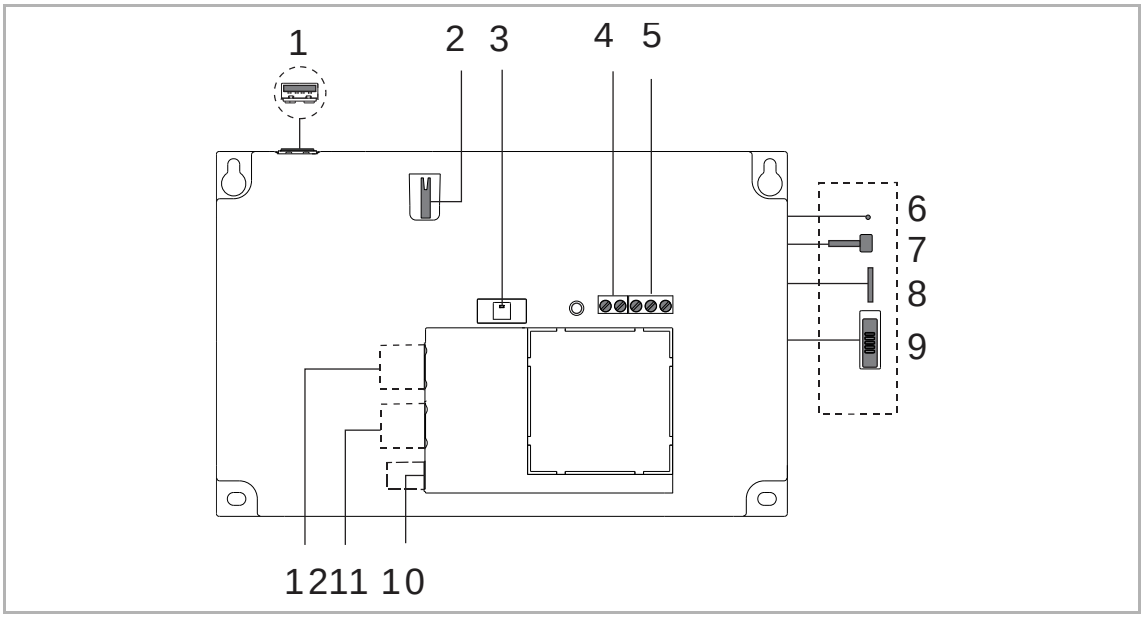
(EU-REACH verordening en wet voor de uitvoering van de verordening (EG) No.1907/2006)

5 Productbeschrijving

5.1 Apparaattype

Artikelnummer	Bestelnummer	Productnaam	Kleur	**Afmetingen (hxbxd)** Eenheid: mm
D04013	2TMA130260W0001	Smart Access Point Lite	Wit	204 x 132 x 32
D04011	2TMA400260W0002	Smart Access Point Pro	Wit	204 x 132 x 32

5.2 Terminalbeschrijving



Nr.	Functie
1	Connector voor USB-stick (gereserveerd)
2	Manipulatieschakelaar Deze wordt gebruikt om te voorkomen dat een indringer in het Smart Access Point inbreekt. Zodra het voorpaneel van het Smart Access Point wordt geopend, klinkt er een sabotagewaarschuwing door de ingebouwde luidspreker van het Smart Access Point. De sabotagewaarschuwing kan ook worden ingesteld als voorwaarde en/of gebeurtenis in de "Actie" functie. Dan kan deze samen met andere acties (bijv. pushmelding) worden geactiveerd.
3	(1) Statusindicatie led
4	Binary input (used to interact with other systems)
5	Binary output (used to interact with other systems)
6	**Resettoets** Houd deze knop 10 s lang ingedrukt om de resetmodus te openen en het wachtwoord van de eerste admin-gebruiker te resetten.
7	**In-/uitschakelen om de WiFi Access Point-modus te activeren/deactiveren** Wanneer de WiFi Access Point modus is geactiveerd, knippert de statusindicatie rood.
8	MicroSD-kaartconnector (gereserveerd)
9	**Veiligheidsschakelaar** Aan = er mogen geen apparaten worden toegevoegd of verwijderd Uit = de apparaten mogen worden toegevoegd of verwijderd (standaard)
10	Connector vermogensingang (DC-JACK-ingang)
11	LAN (PoE)
12	LAN (gereserveerd)

(1) Statusindicatie led

Beschrijving	Blauw	Rood	Groen	Wit	Prioriteit
Resetten naar fabrieksinstellingen				Langzaam knipperen	7 (hoogst)
Alarm (bijv. manipulatiealarm)				Snel knipperen	6
Ingeschakeld of eerste installatie				Aan	5
WiFi Access Point is geactiveerd		Langzaam knipperen			4
Veiligheidsmodus is gedeactiveerd		Aan			3
Deurbel is gedempt	Aan				2
Normale modus			Aan		1

6 Technische gegevens

Aanduiding	Waarde
Spanningswaarde	24 V ⎓
Bedrijfsspanningsbereik	20-27 V ⎓
Nominale stroom	24 V ⎓, 375 mA
PoE standaard	IEEE802.3 af
Draadloze overdrachtfrequentie	**802.11b/g/n:** 2412...2462MHz (voor de VS) 2412...2472MHz (voor Europese landen) **802.11a/n:** 5150…5250MHz 5250…5350MHz 5470…5725MHz 5725…5850MHz (voor de VS)
Draadloos transmissievermogen	Max. 20 dBm@12 Mbps OFDM 2.4 G Max. 20 dBm@12 Mbps OFDM 5.8 G
Draadloze transmissiestandaard	IEEE 802.11 a/b/g/n
Omgevingstemperatuur	-10 °C…+45 °C
Opslagtemperatuur	-25 °C…+70 °C
Productafmetingen	204 mm × 132 mm × 32 mm
IP-level	IP 30
IK-level	IK 05
Relaisuitgang	30 V ⎓, 1 A
Droge contactinvoer	5 V ⎓, 1mA

Bluetooth-gegevens

Bluetooth-standaard	4,2
Frequentieband	2.402…2.480 GHz
TX-vermogen	Maximaal 8 dBm
RX-gevoeligheid	Minimaal -92 dBm

7 Montage/installatie

GEVAAR

Bij direct of indirect contact met spanningvoerende delen treedt er een gevaarlijke stroomschok in het lichaam op. Elektrische schok, brandwonden of de dood kunnen het gevolg zijn. Bij niet correct uitgevoerde werkzaamheden aan spanningvoerende delen bestaat brandgevaar.

– Voor montage en demontage eerst de netspanning uitschakelen!
– Werkzaamheden aan het 100 … 240V-stroomnet uitsluitend laten uitvoeren door een erkend elektrotechnisch installatiebedrijf.

7.1 Eis voor de installateur

Waarschuwing

Elektrische spanning!

Installeer het apparaat alleen als u over de nodige kennis en ervaring op elektrotechnisch gebied beschikt.

– Onjuiste installatie brengt uw leven en dat van de gebruiker van het elektrische systeem in gevaar.
– Onjuiste installatie kan ernstige schade toebrengen aan eigendommen, bijvoorbeeld door brand.

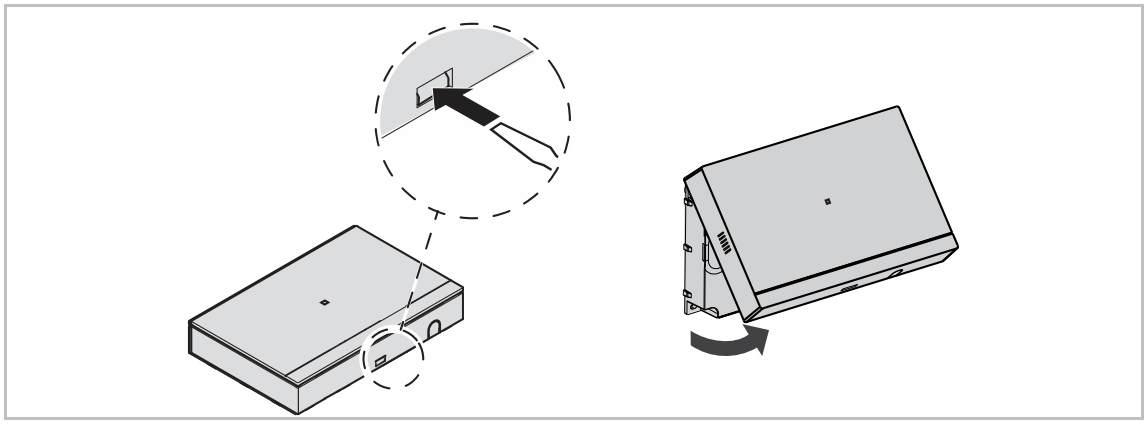
De minimaal noodzakelijke vakkennis en vereisten voor de installatie zijn als volgt:

– Pas de "vijf veiligheidsregels" toe (DIN VDE 0105, EN 50110):
  1. Koppel
  2. Beveilig tegen opnieuw verbonden te zijn
  3. Zorg dat er geen spanning is
  4. Verbind met aarde en kortsluiten
  5. Bedek aangrenzende delen of barricadeer ze.
– Gebruik geschikte persoonlijke beschermkleding.
– Gebruik alleen geschikt gereedschap en meetapparatuur.
– Controleer het type voedingsnet (TN-systeem, IT-systeem, TT-systeem) om de volgende voedingsomstandigheden te garanderen (klassieke verbinding met aarde, beschermende aarding, noodzakelijke aanvullende maatregelen, enz.).

7.2 Montage

1. Demonteren

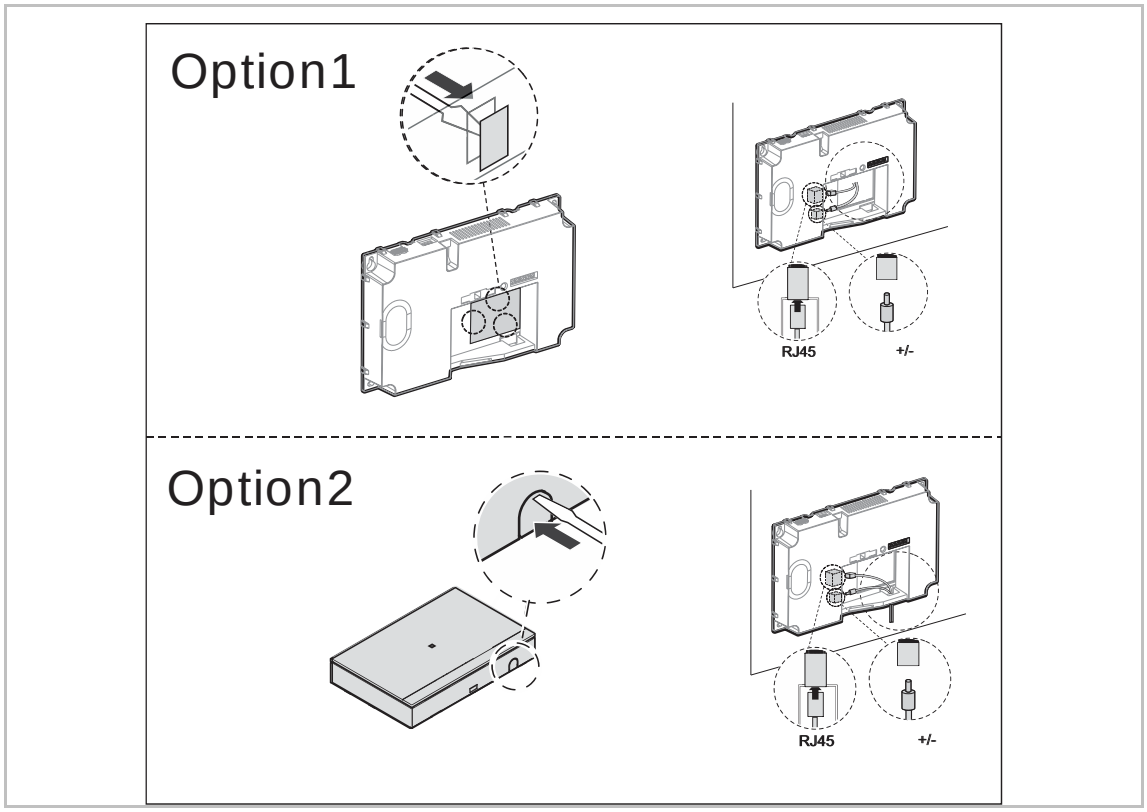
Trek aan de klem aan de onderkant van het apparaat en open vervolgens de voorklep.



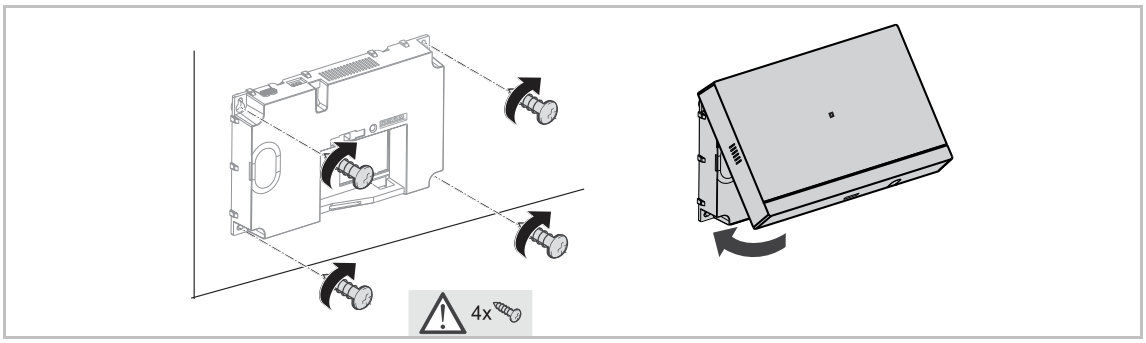
2. Bedrading

Optie 1: bedrading vanaf de achterkant

Optie 2: bedrading vanaf de onderkant



3. Montage



8 Ingebruikname

8.1 Systeemvereisten

Gebruikersinterface

De inbedrijfname wordt altijd uitgevoerd via de webinterface van "Smart Access Point".

Om de webbasis gebruikersinterface te openen, hebt u een computer nodig met een LAN- of WLAN-netwerkadapter en een geïnstalleerde internetbrowser.

Aanbevolen browsers zijn:

- Firefox (vanaf versie 9)
- Google Chrome
- Safari

Welcome-app

Voor de installatie van de Welcome-app hebt u een smartphone of tablet met een besturingssysteem Android (vanaf 4.0) of iOS (vanaf iOS 7) nodig.

Thuisnetwerk

Om tijdens het standaardgebruik tegelijkertijd toegang te hebben tot de Welcome-app en internetdiensten (bijv. e-mail), moet het "Smart Access Point" na inbedrijfname in het bestaande thuisnetwerk geïntegreerd worden. Daarvoor is een router met ethernet- of WLAN-interface nodig.

Gebouwtype

Het "Smart Access Point" ondersteunt twee gebouwtypen voor verschillende toepassingen.

Opmerking
De topologiemodus kan alleen bij de eerste inbedrijfname gekozen worden.

1. Woongebouw

Deze modus wordt gebruikt voor een eengezinswoningen.

In deze modus wordt de "Smart Access Point" gebruikt om de apparaten in de woning te beheren.

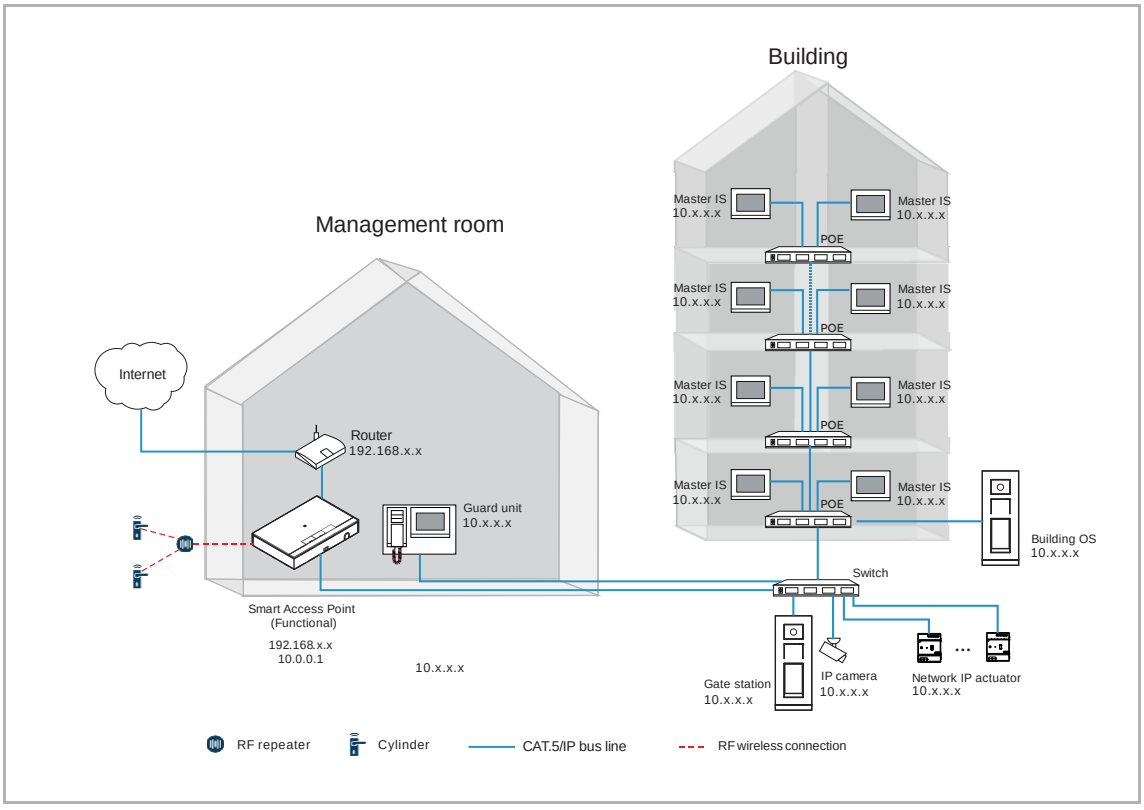
In deze modus kan het "Smart Access Point" alleen communiceren met de andere TCP/IP-apparaten in een netwerksegment; normaal is dat het thuisnetwerk met een statisch IP-adres of het dynamische IP-adres van de DHCP-server.

2. Functioneel gebouw

Deze modus wordt gebruikt voor toepassingen met meerdere appartementen of commerciële toepassingen.

In deze modus kan het "Smart Access Point" alleen communiceren met de andere TCP/IP-apparaten in 2 netwerksegmenten. Eén is het thuisnetwerk in de managementruimte. Het andere is het netwerk van het gebouw. Het IP-adres van "Smart Access Point" is vast ingesteld op 10.0.0.1.

Alle apparaten op het netwerk van het gebouw kunnen het IP-adres automatisch genereren uit hun fysieke adres (bijv. gebouwnummer, etagenummer en ruimtenummer).



MyBuildings-account

Aanbevolen wordt een MyBuildings-account te registreren vóór de eerste inbedrijfname.

1. Voordelen van een MyBuildings-account

- Dit is nodig wanneer u het wachtwoord voor de eerste admin-gebruiker wilt resetten.
- Het is nodig wanneer u zich wilt abonneren op de "afstandsbedieningsservices".
- Het is nodig wanneer u de meldingen via de Welcome-app wilt ontvangen
- Het is nodig wanneer u zich wilt aanmelden via de webinterface van het "Smart Access Point".

Afstandsbedieningsservices

Er zijn 3 soorten "afstandsbedieningsservices":

1. Toegang op afstand en meldingen

Afstandservices voor Welcome IP, AccessControl en VideoControl voor deWelcome-app

- Deuroproepen ontvangen.
- Videobewaking-oproepen naar buitenposten en IP-camera's.
- Op afstand ontgrendelen van digitale deursloten (ondersteuning voor maximaal 8 "elektronische slotcilinders").
- Toegang op afstand tot de webinterface van het lokale Smart Access Point.
- Gebeurtenissengeschiedenis en pushmeldingenservice.
- Per abonnement: toegang op afstand voor 10 mobiele toestellen.

2. Ontgrendeling op afstand

Afstandservices voor AccessControl voor commerciële gebruikssituaties op de Welcome-app:

- Onafhankelijk van het aantal gebruikers (mobiele toestellen).
- Vier verschillende pakketten voor maximaal 600 sloten beschikbaar.
- Op afstand ontgrendelen van digitale deursloten.

3. Video-opslag en streaming

Services voor opslag op afstand voor VideoControl-apparaten (aanvullend pakket voor het pakket "Toegang op afstand en meldingen"):

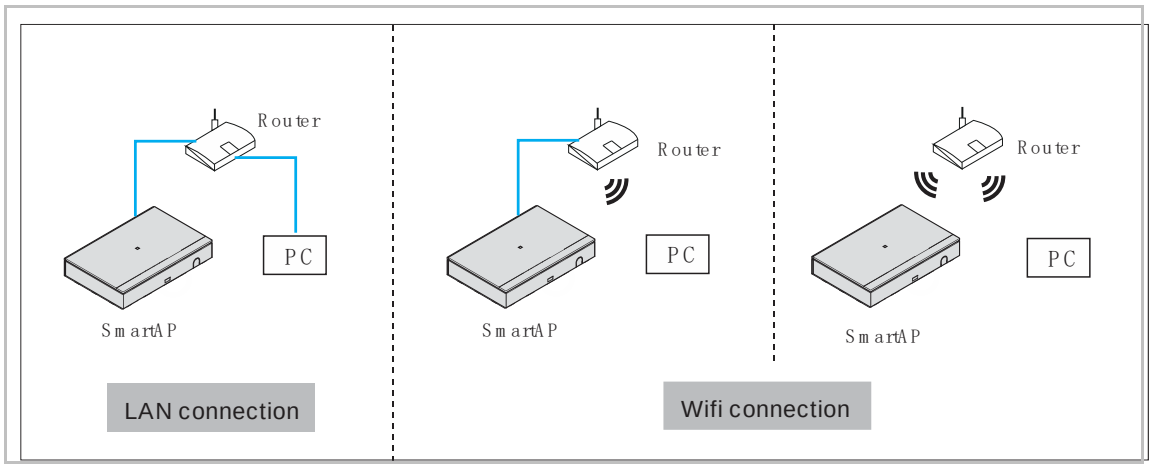
- Opslag- en streamingservices voor gebeurtenisopnamen in de cloud.
- Verschillende pakketten voor cloud-opslag beschikbaar.

4. Hoe registreert u een account op het MyBuildings -portaal?

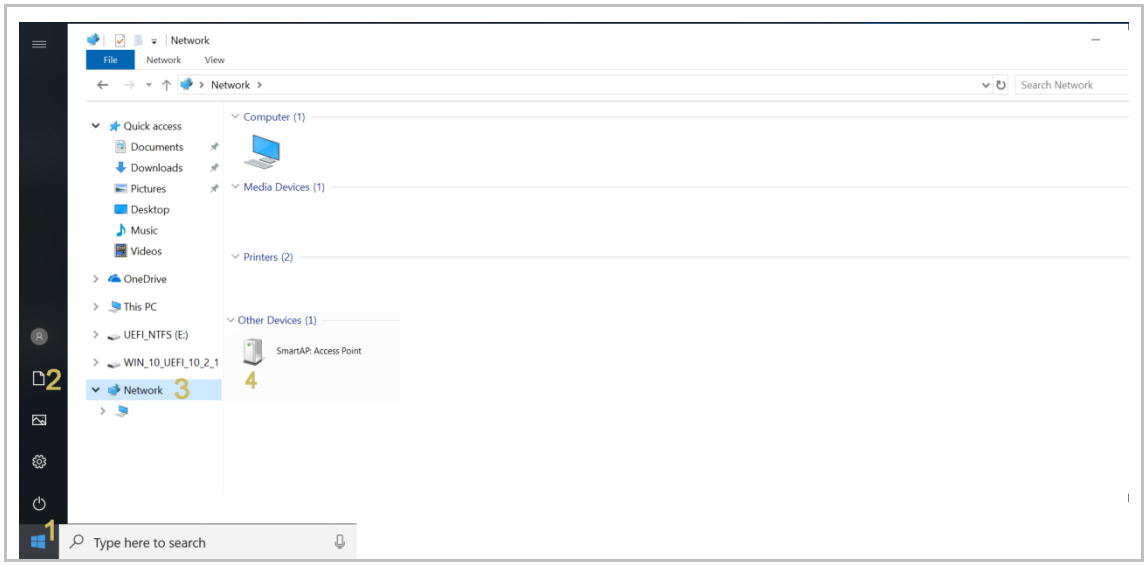
zie hoofdstuk 13.1 “Een account registreren via het MyBuildings-portal“ op pagina 251.

8.2 Toegang tot SmartAP via UPnP

De pc moet eerst verbinding maken met de router.



Volg de onderstaande stappen op de pc:

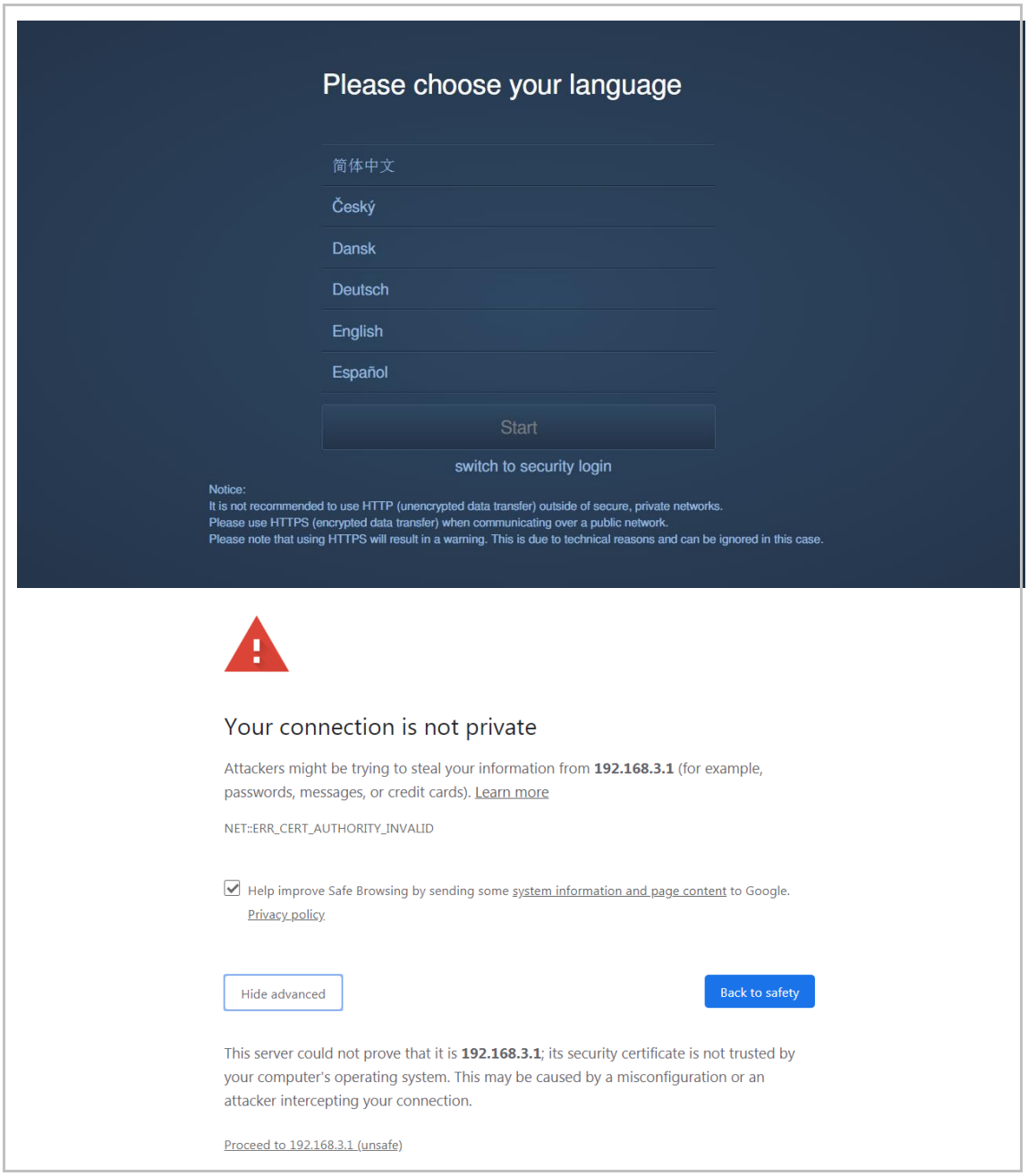


8.3 Eerste configuratie

1. Overschakelen naar veiligheidslogin

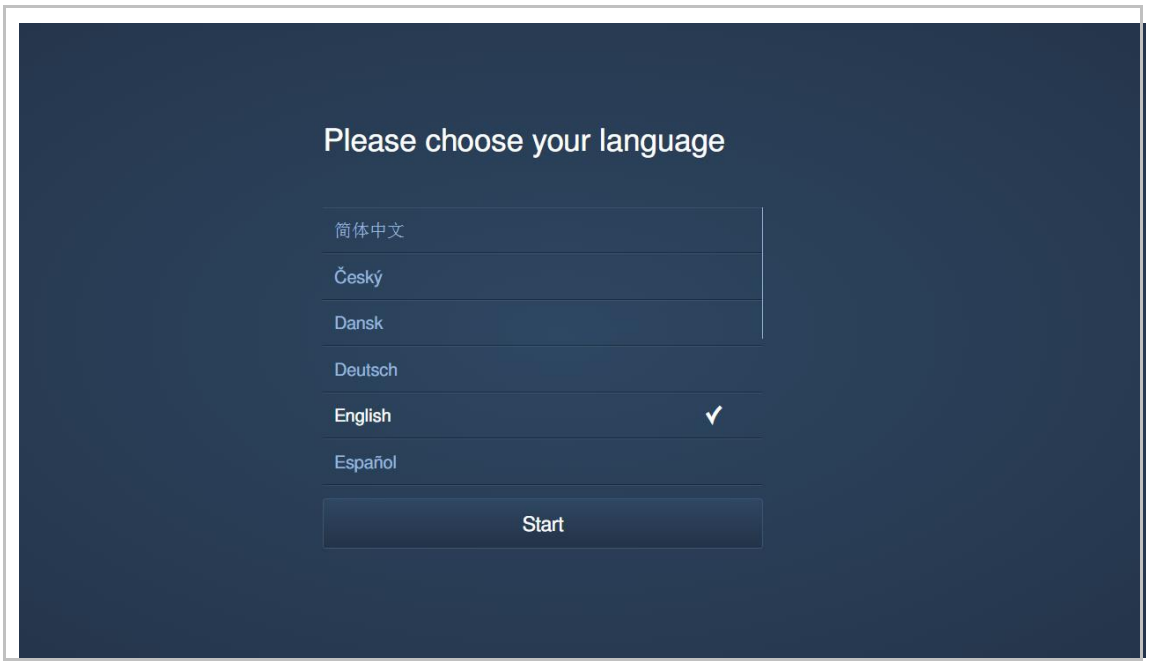
Aanbevolen wordt om HTTPS te gebruiken om gegevens te versleutelen.

Klik op "Overschakelen naar veiligheidslogin" - "Geavanceerd" - "Ga naar ..." om naar het beveiligingsscherm te gaan.

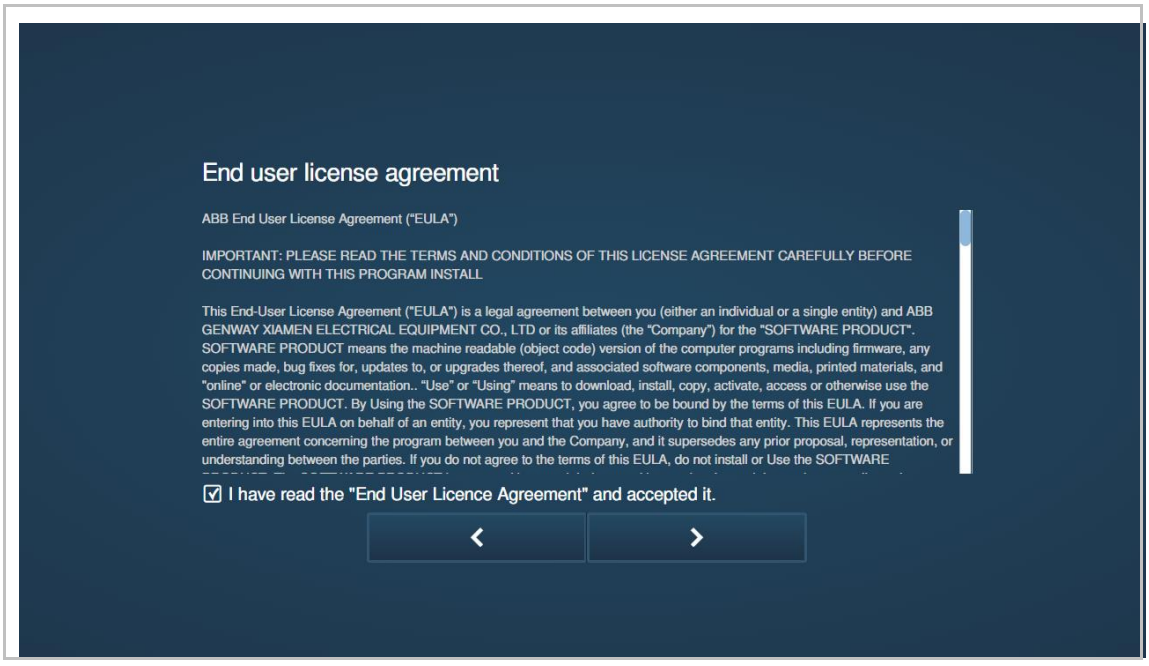


2. Taal selecteren

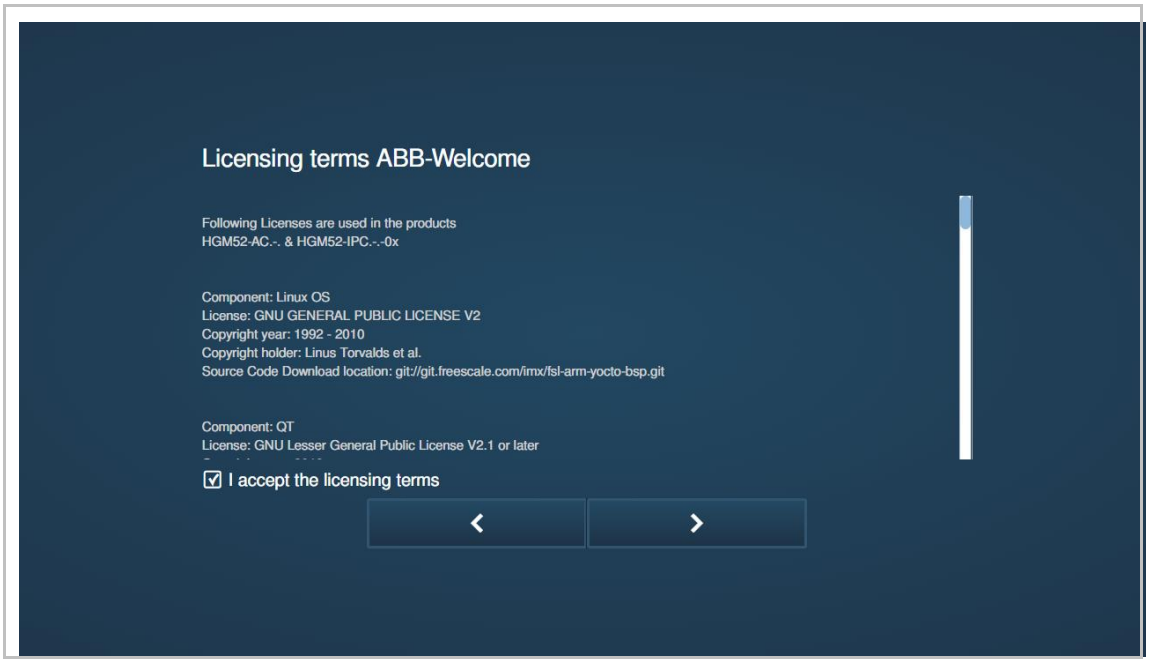
Selecteer de taal uit de keuzelijst.



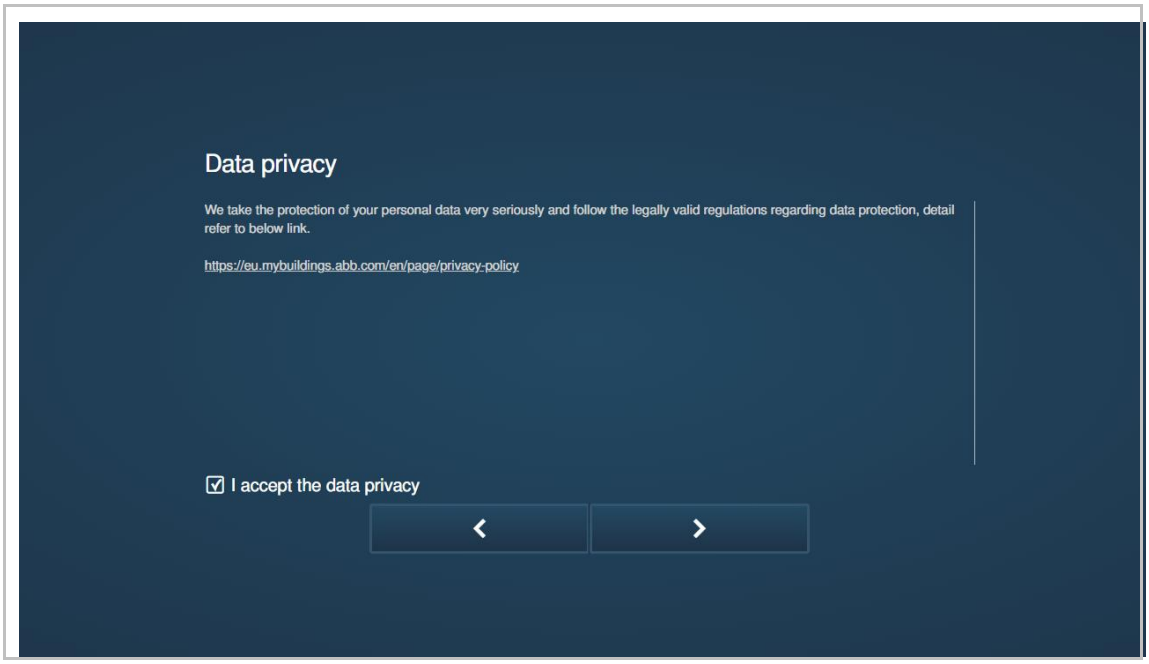
3. Accepteer de eindgebruikerslicentie



4. Accepteer de OSS-licentie

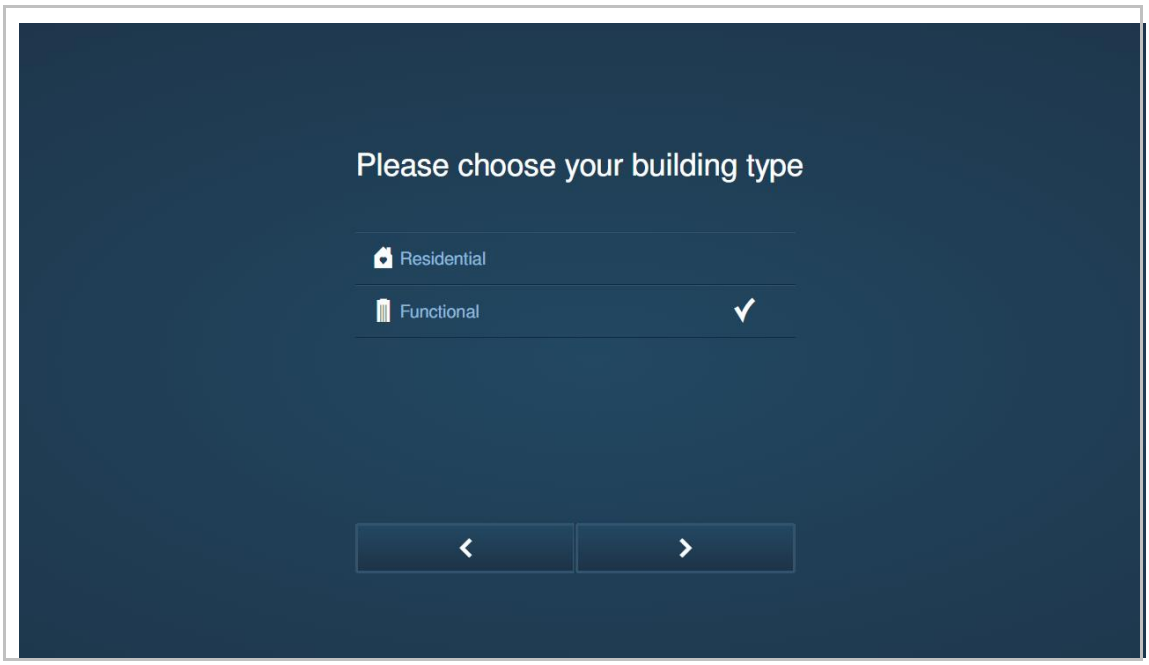


5. Accepteer de privacyverklaring



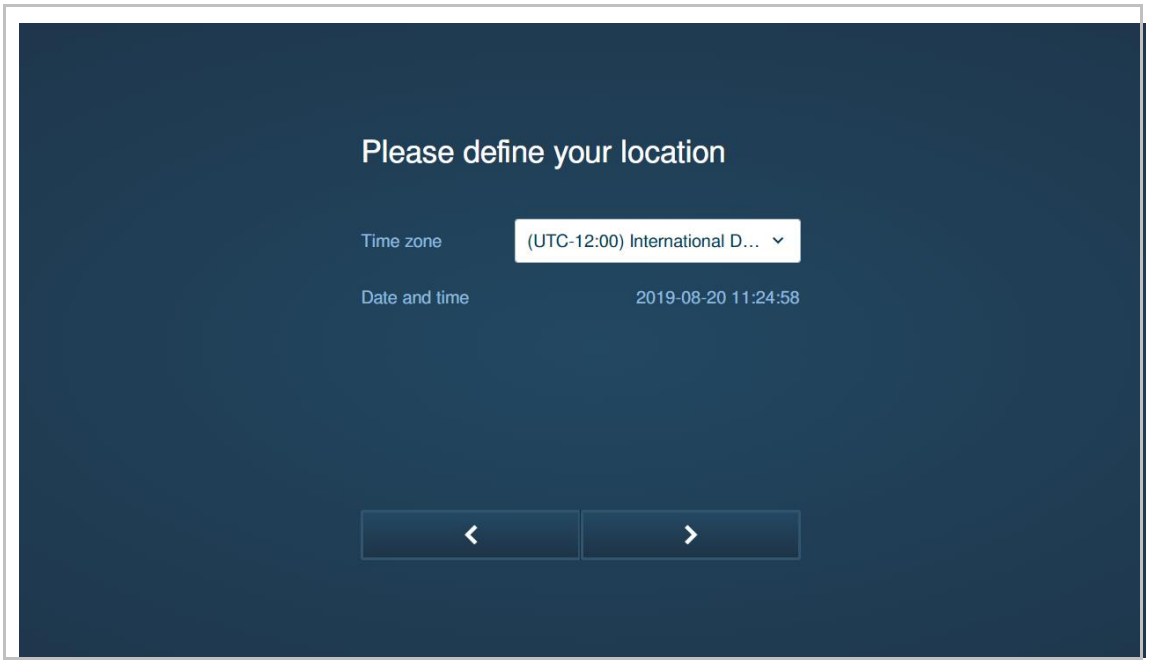
6. Kies het gebouwtype

Meer informatie hierover vindt u in het hoofdstuk "Typische toepassingen".



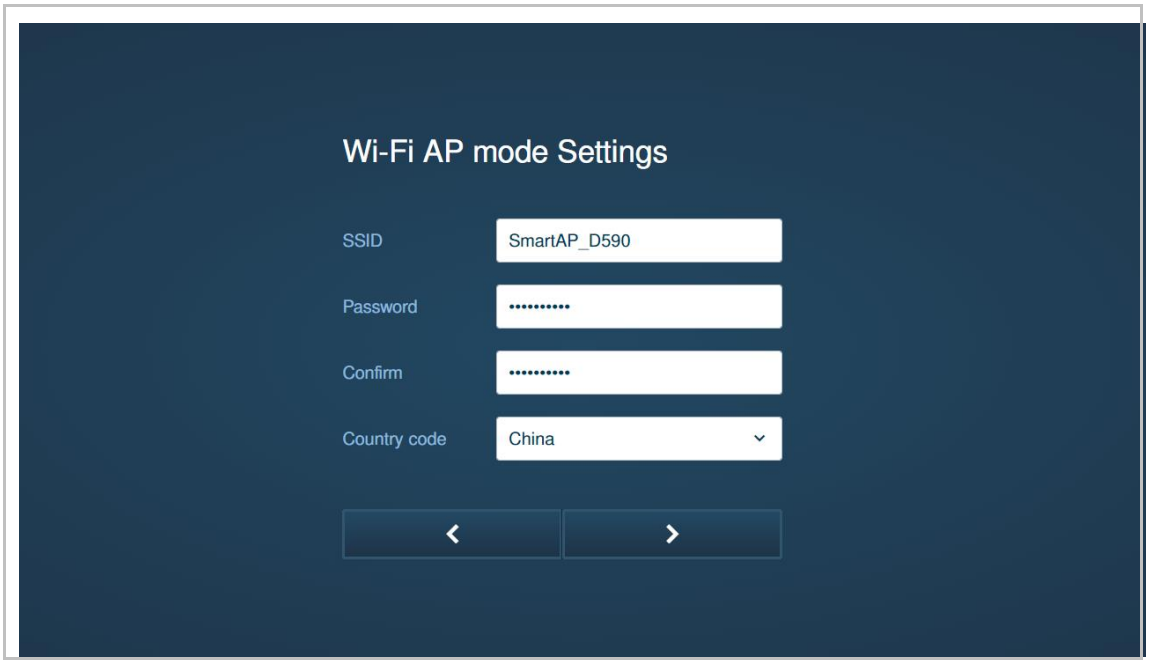
7. Bepaal uw locatie

Selecteer de tijdzone uit de keuzelijst.



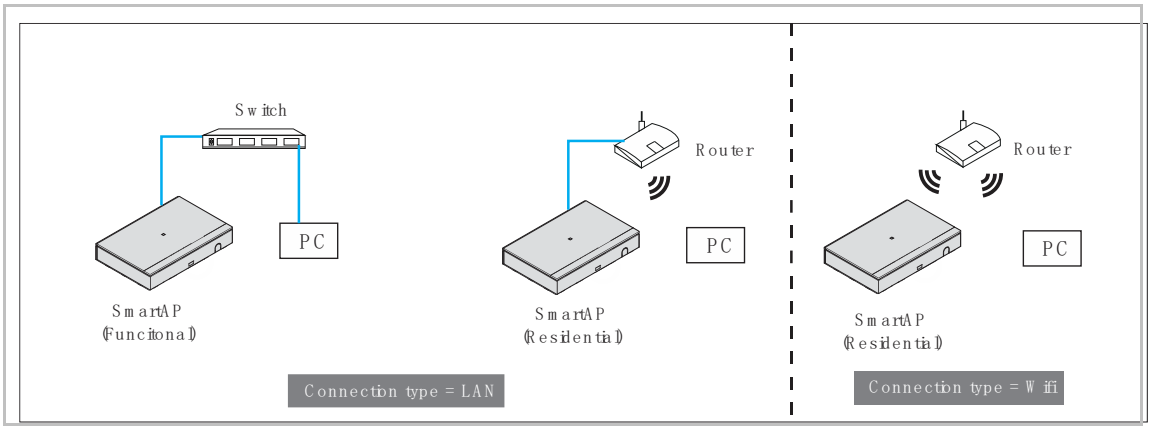
8. Wijzig de AP-modus wifi-instelling en stel de landcode in.

Het is noodzakelijk om de WLAN-naam en het wachtwoord bij de eerste installatie te wijzigen. Aanbevolen wordt om een nieuwe sticker te maken en deze op de afdekking van het apparaat aan te brengen.

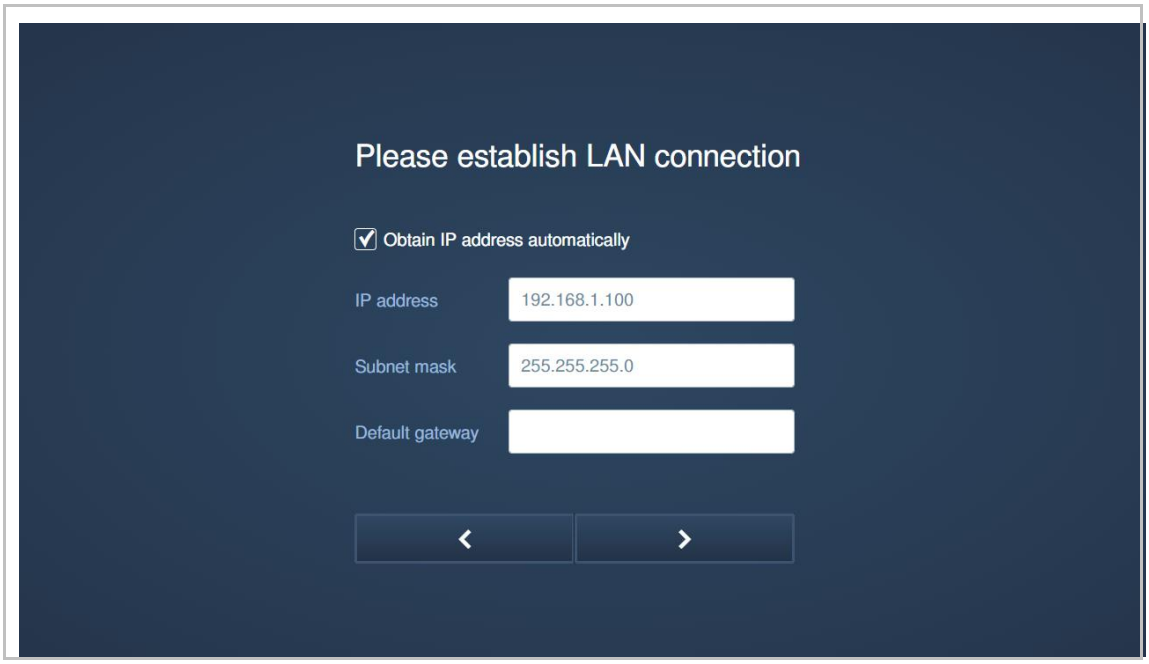


9. Selecteer het type verbinding

Selecteer een verbindingstype volgens onderstaand schema.



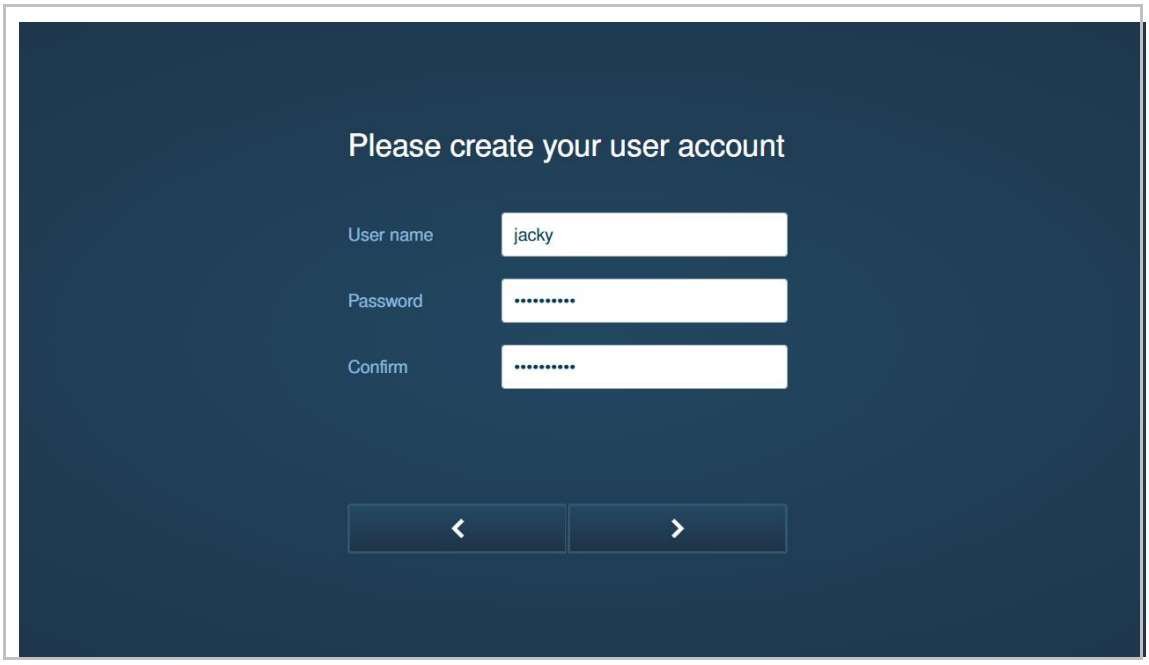
Selectie type = LAN



Selectie type = wifi

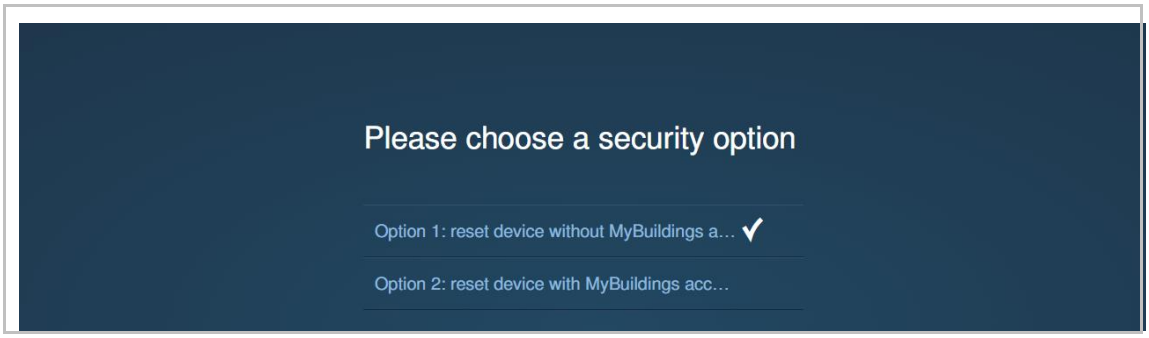
10. Maak de eerste admin-gebruiker aan

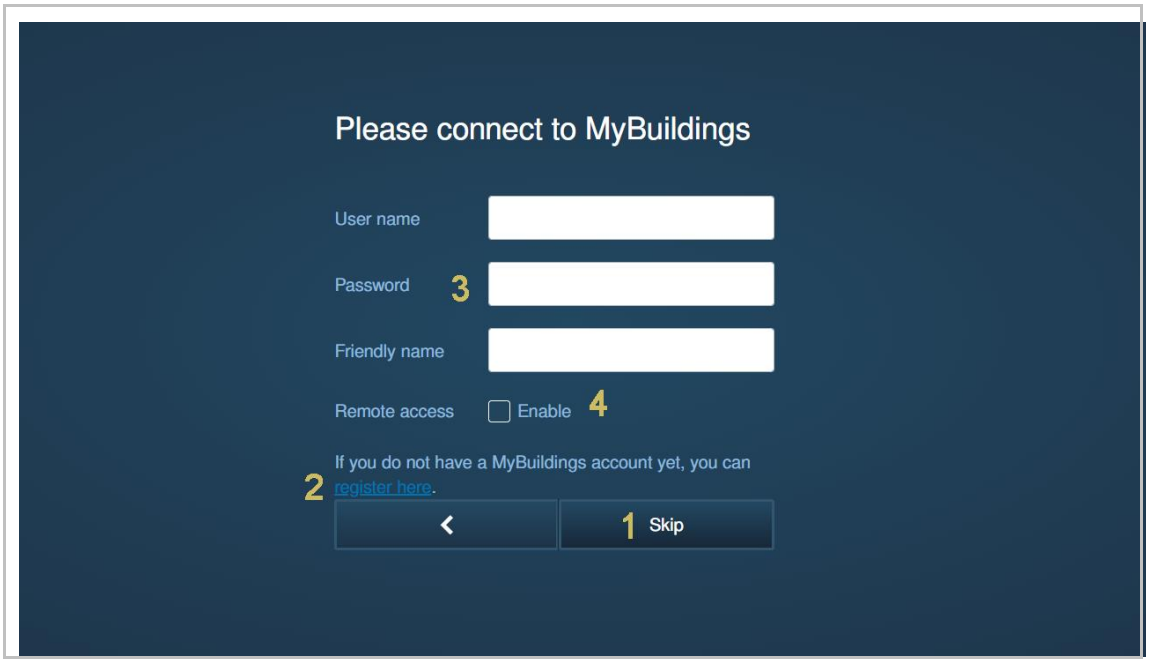
Hier maakt u de eerste admin-gebruiker aan.



11. MyBuildings-login

[1] Beveiligingsniveau 1: stel het wachtwoord voor de eerste admin zonder MyBuildings-account opnieuw in.

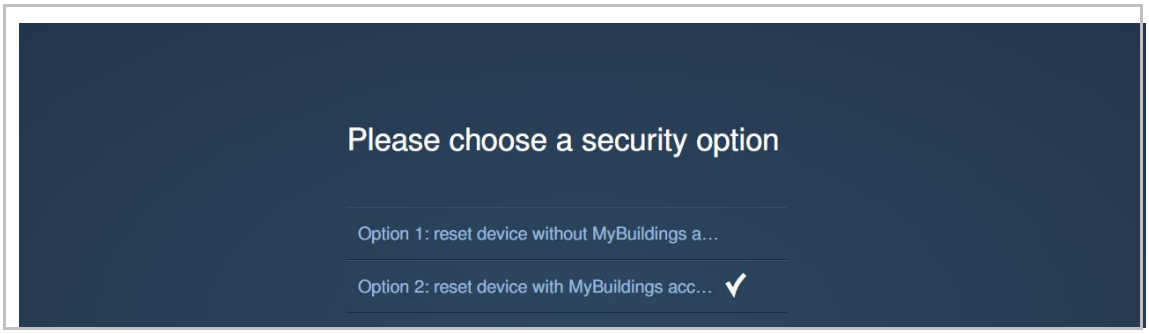


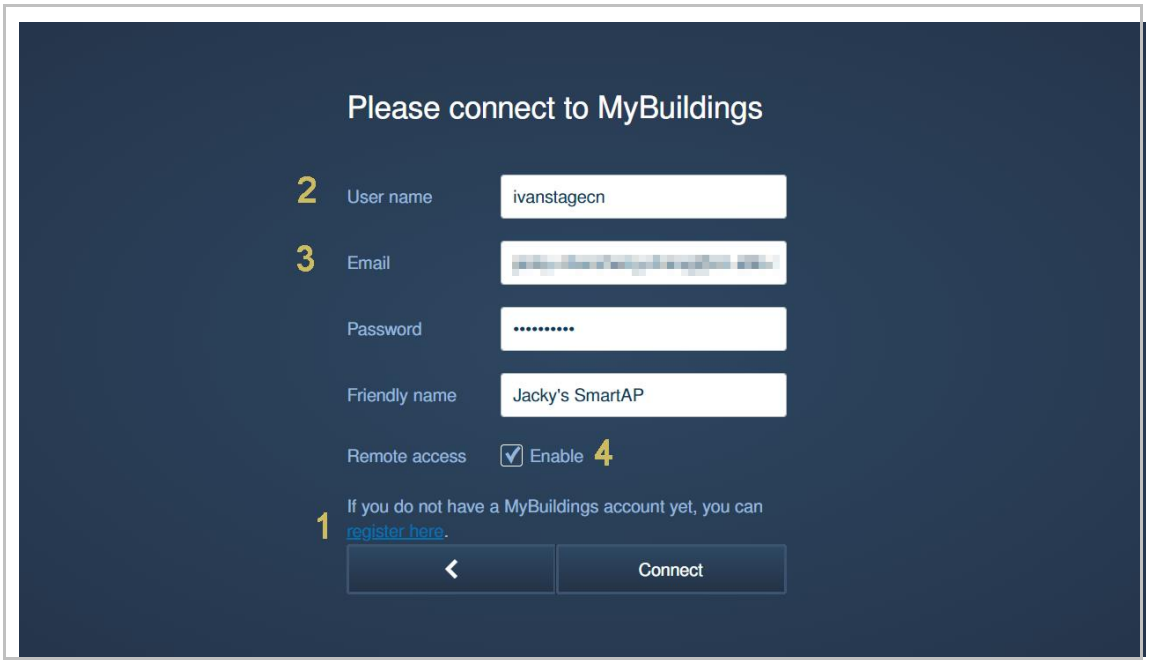


Nr.	Beschrijving
1	Als u in dit scherm geen instellingen aanpast, kunt u op "Overslaan" klikken om naar het volgende scherm te gaan.
2	Als u geen MyBuildings-account heeft, klik dan op "hier registreren" om een account aan te maken.
3	Voer de gebruikersnaam, het wachtwoord en de bijnaam in.
4	Als de functie "Toegang op afstand" is geactiveerd, hebt u toegang tot de SmartAP op het MyBuildings-portaal als u zich op de service op afstand hebt geabonneerd.

Zie het hoofdstuk "Het wachtwoord voor de eerste admin resetten" voor meer informatie.

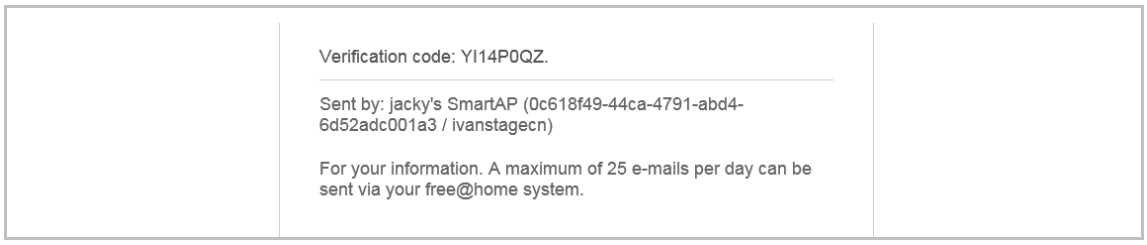
[2] Beveiligingsniveau 2: stel het wachtwoord voor de eerste admin met MyBuildings-account opnieuw in.



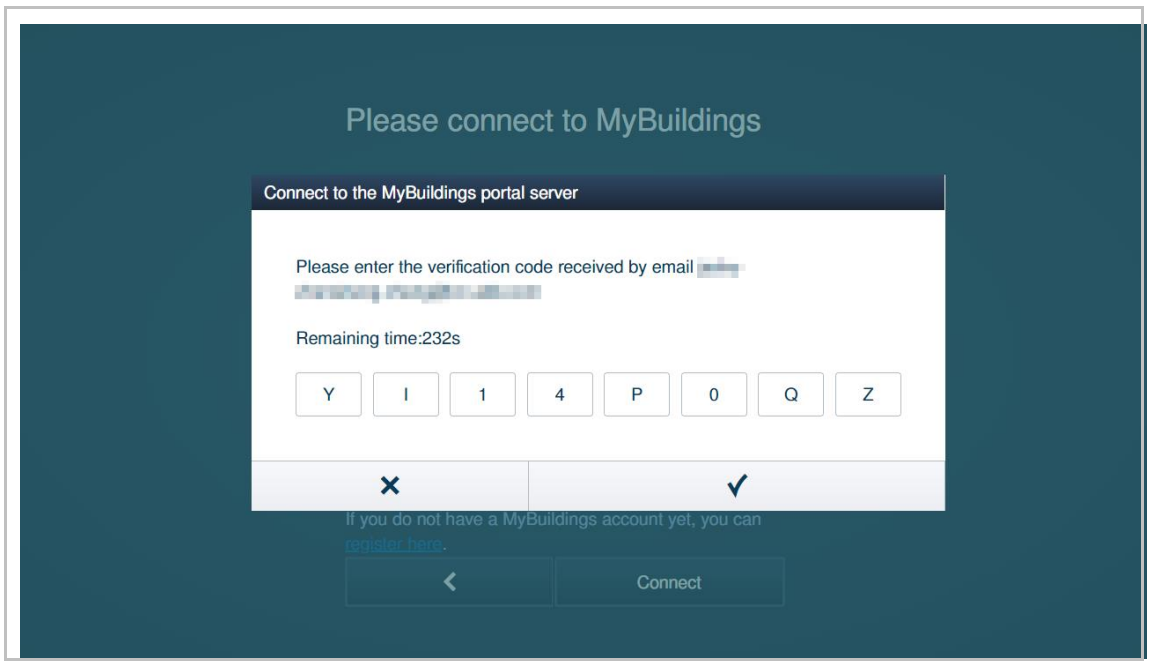


Nr.	Beschrijving
1	Als u geen MyBuildings-account heeft, klik dan op "hier registreren" om een account aan te maken.
2	Voer de gebruikersnaam, het wachtwoord en de bijnaam in.
3	Voer de mail in voor het resetten van het wachtwoord voor de eerste admin.
4	Als de functie "Toegang op afstand" is geactiveerd, hebt u toegang tot de SmartAP op het MyBuildings-portaal als u zich op de service op afstand hebt geabonneerd.

Klik op "Verbinden"; u ontvangt dan een e-mail met de verificatiecode.



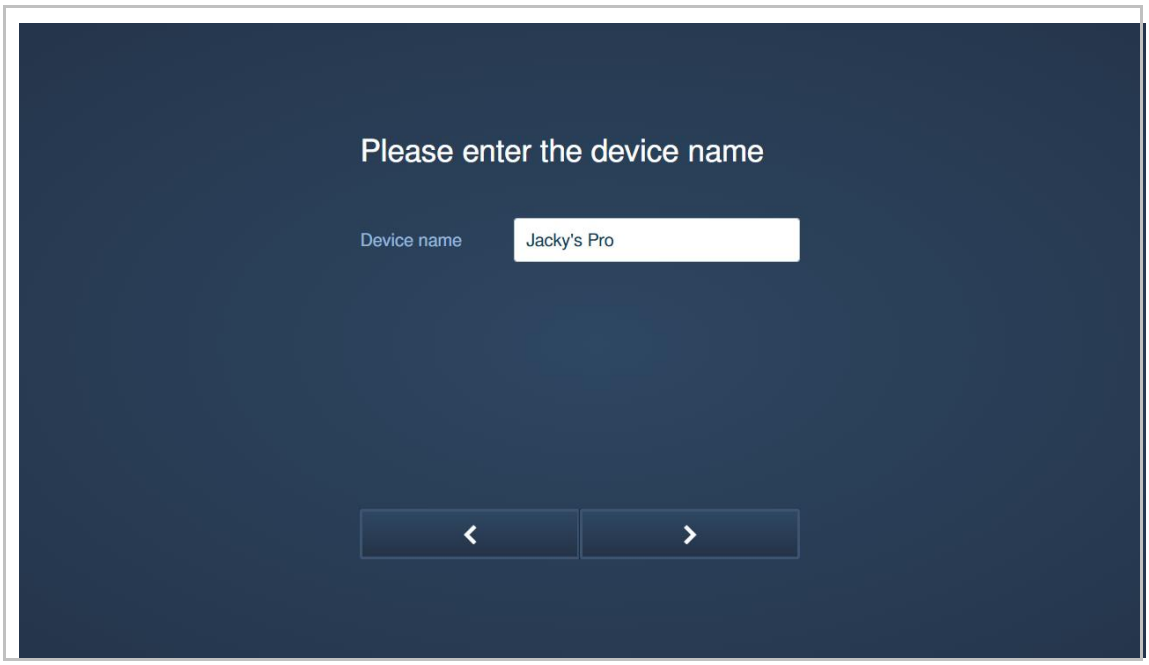
Voer deze verificatiecode in en klik op "√".



Zie het hoofdstuk "Het wachtwoord voor de eerste admin resetten" voor meer informatie.

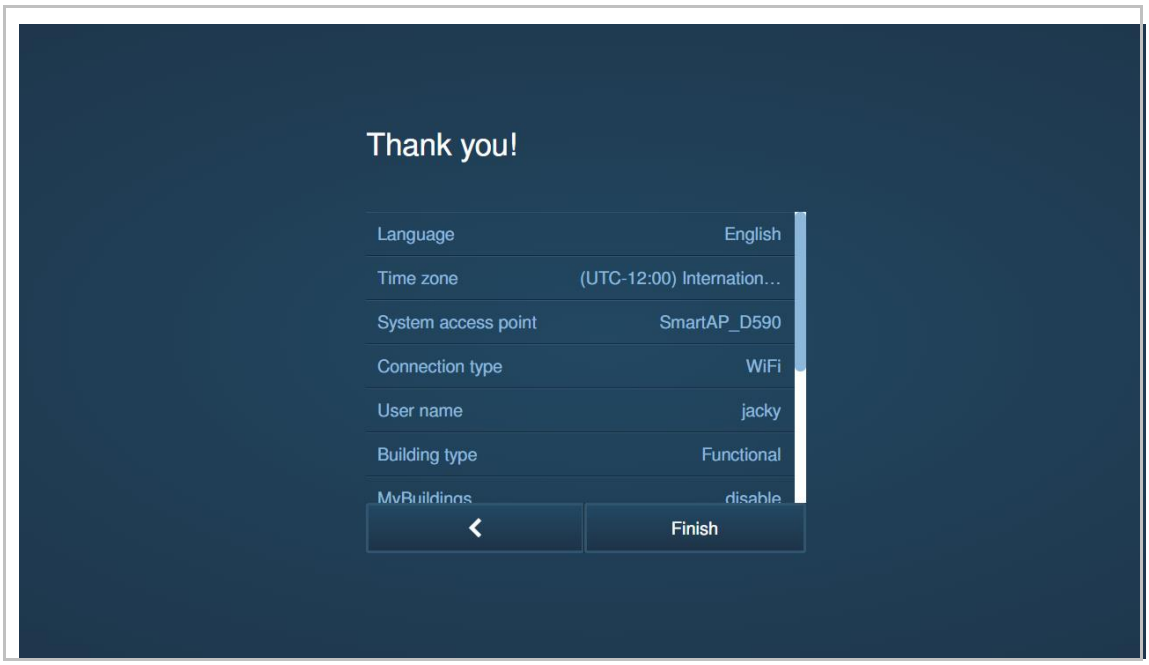
12. Stel de apparaatnaam in

Deze apparaatnaam wordt weergegeven op het inlogscherm.

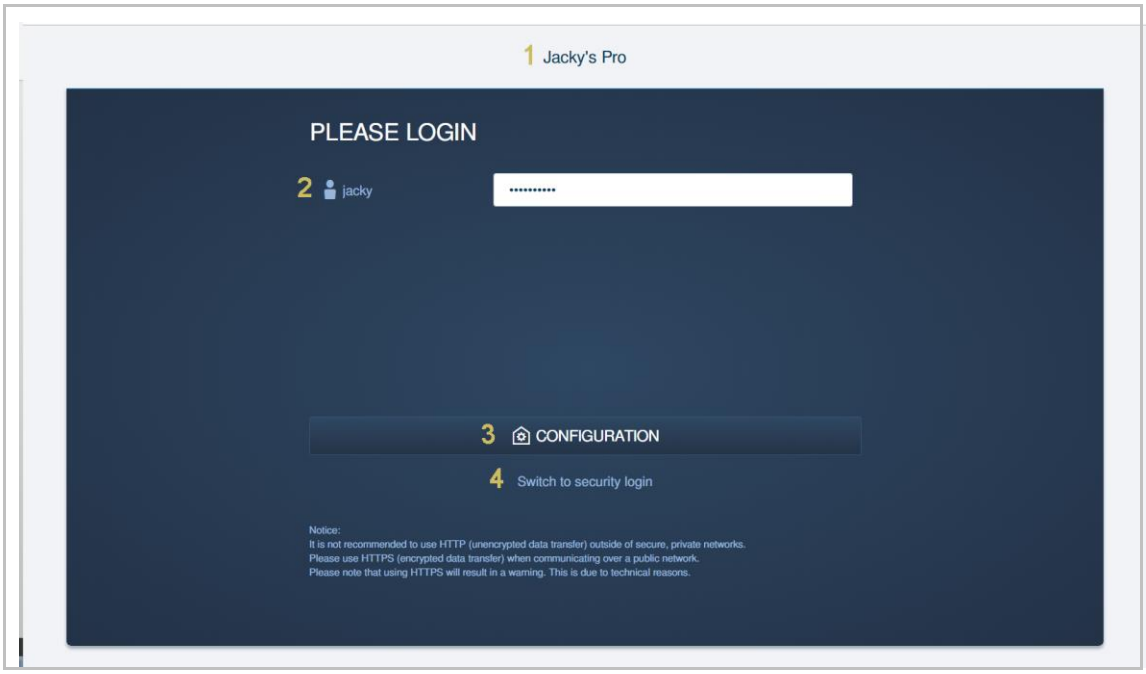


13. Bevestig de instellingen

U kunt alle instellingen zien op het overzichtsscherm. Klik op "Voltooien" als de instellingen in orde zijn.



14. Ga naar het inlogscherm



Nr.	Beschrijving
1	**Apparaatnaam**
2	**Gebruikersnaam en wachtwoord**
3	**Ga naar het configuratiescherm** Deze functie is alleen beschikbaar voor de admin- en master-gebruiker.
4	**Overschakelen naar veiligheidslogin**

zie hoofdstuk 8.1 “Systeemvereisten“ op pagina 15

zie hoofdstuk 13.2 “Wachtwoord voor de eerste beheerder resetten“ op pagina 252

zie hoofdstuk 13.1 “Een account registreren via het MyBuildings-portal“ op pagina 251

zie hoofdstuk 13.1 “Een account registreren via het MyBuildings-portal“ op pagina 251

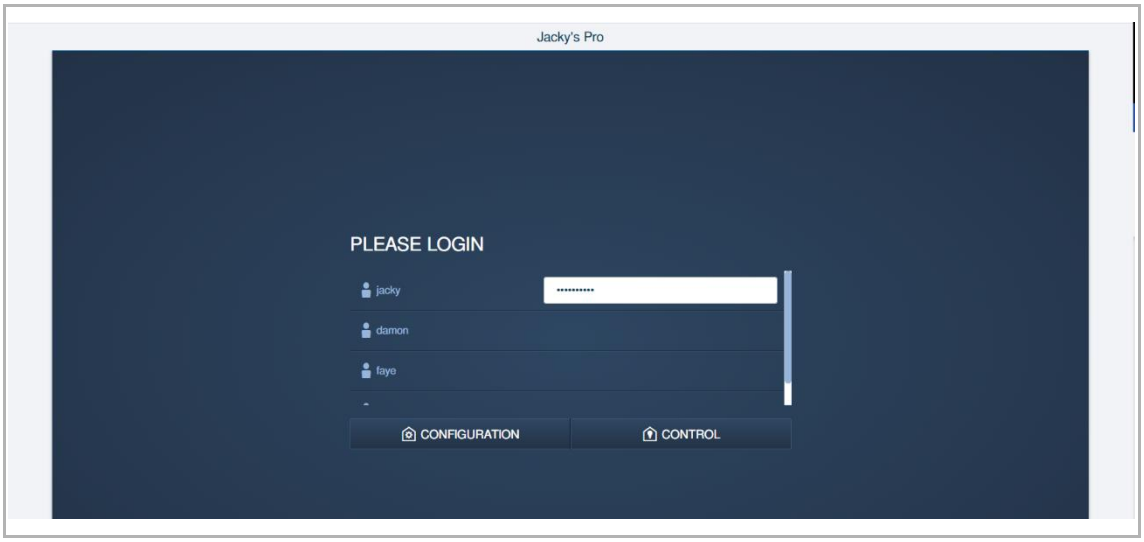
zie hoofdstuk 13.2 “Wachtwoord voor de eerste beheerder resetten“ op pagina 252

8.4 Inlogscherm

Na de eerste installatie kunt u het inlogscherm van "Smart Access Point" openen met de eerste admin-gebruiker. Het inlogscherm verschilt afhankelijk van het aantal gebruikers.

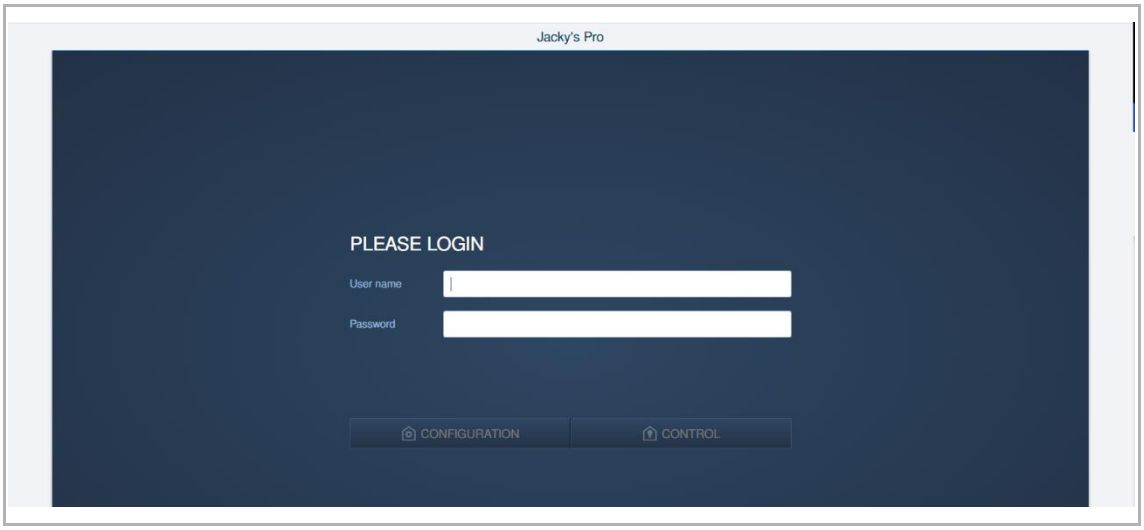
Aantal gebruikers < 6

Als het aantal gebruikers <6 is, wordt er een namenlijst op het scherm weergegeven. Voer het wachtwoord rechts van de gebruikersnaam in om door te gaan.



Aantal gebruikers ≥ 6

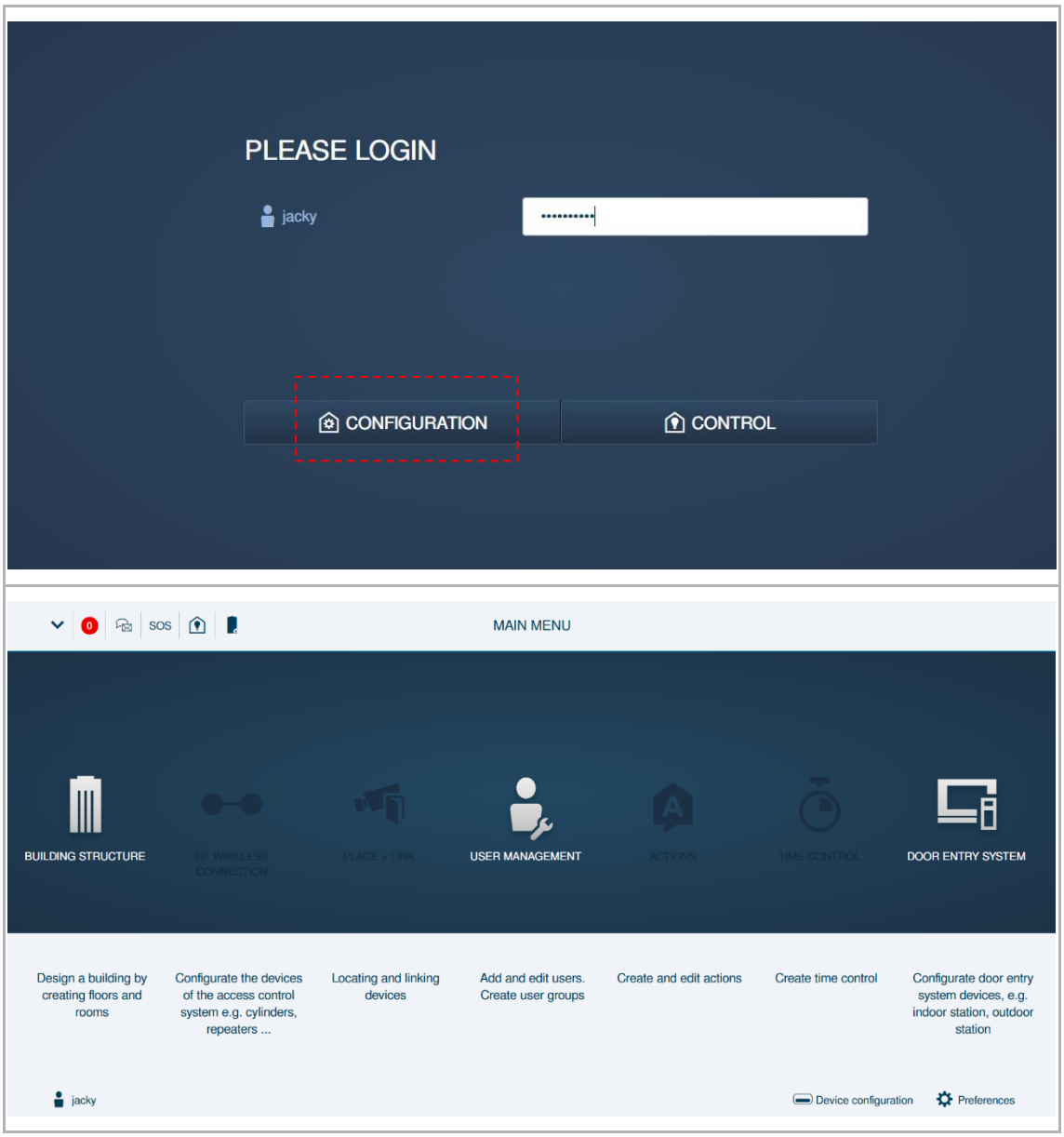
Als het aantal gebruikers ≥ 6 is, wordt er geen namenlijst op het scherm weergegeven. U moet de gebruikersnaam en het wachtwoord invoeren om door te gaan.



8.5 Configuratiescherm

Het configuratiescherm wordt gebruikt om alle apparaten en gebruikers toe te voegen en te configureren.

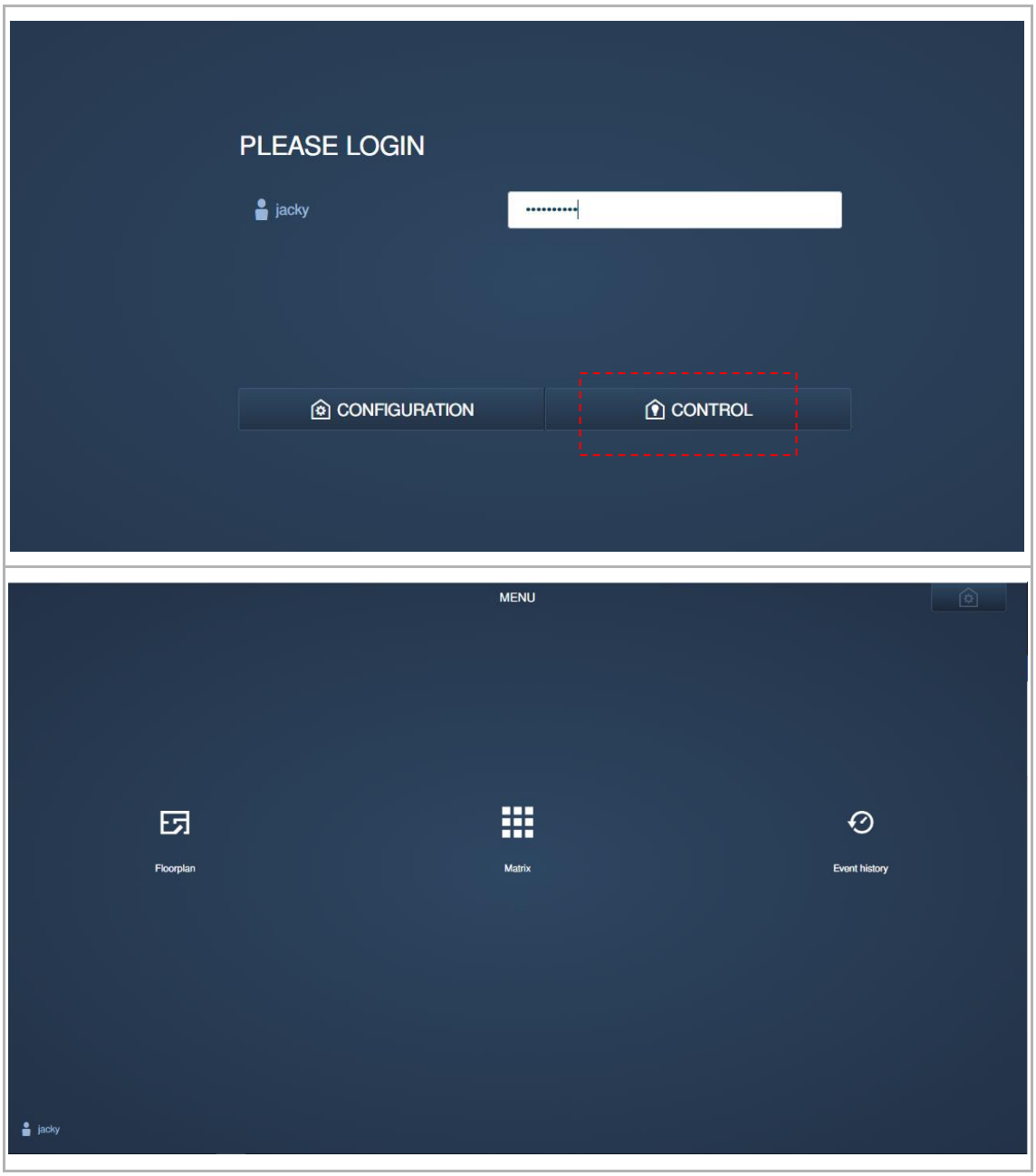
Voer op het inlogscherm het wachtwoord in en klik op "Configuratie" om toegang te krijgen tot het configuratiescherm.



8.6 Besturingsscherm

Het controlescherm wordt gebruikt om de Accescontroleapparaten te bedienen.

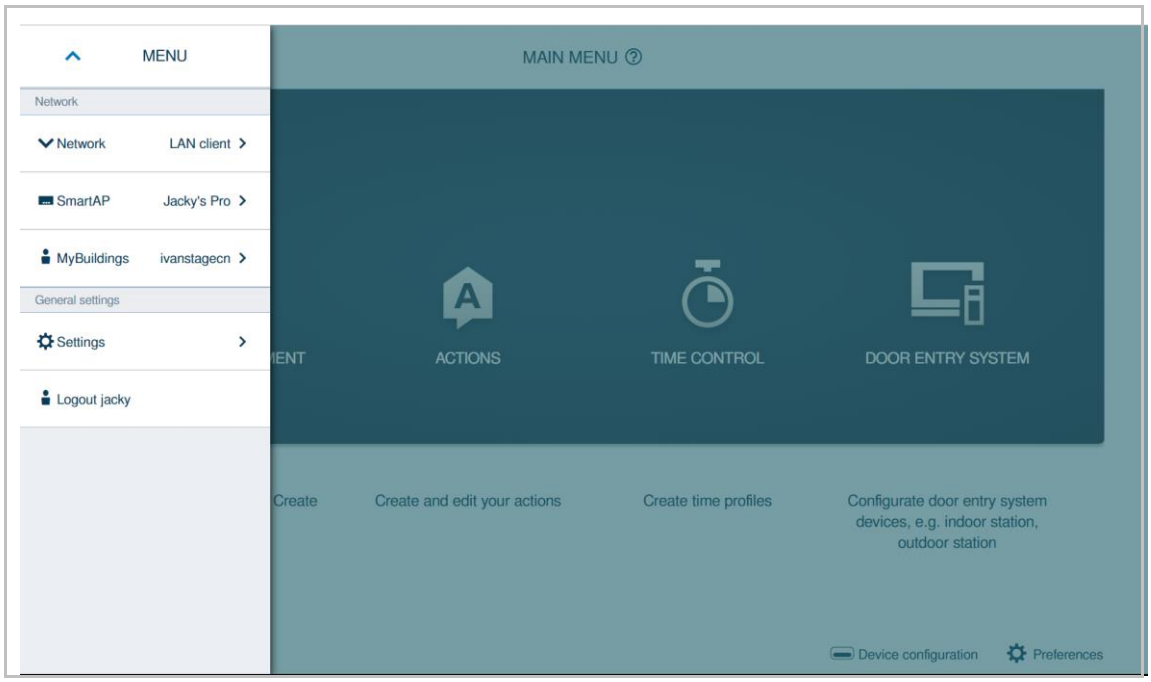
Op het aanmeldscherm, voer het wachtwoord in en klik op "Control" om toegang te krijgen tot het controlescherm.



8.7 Instellingen

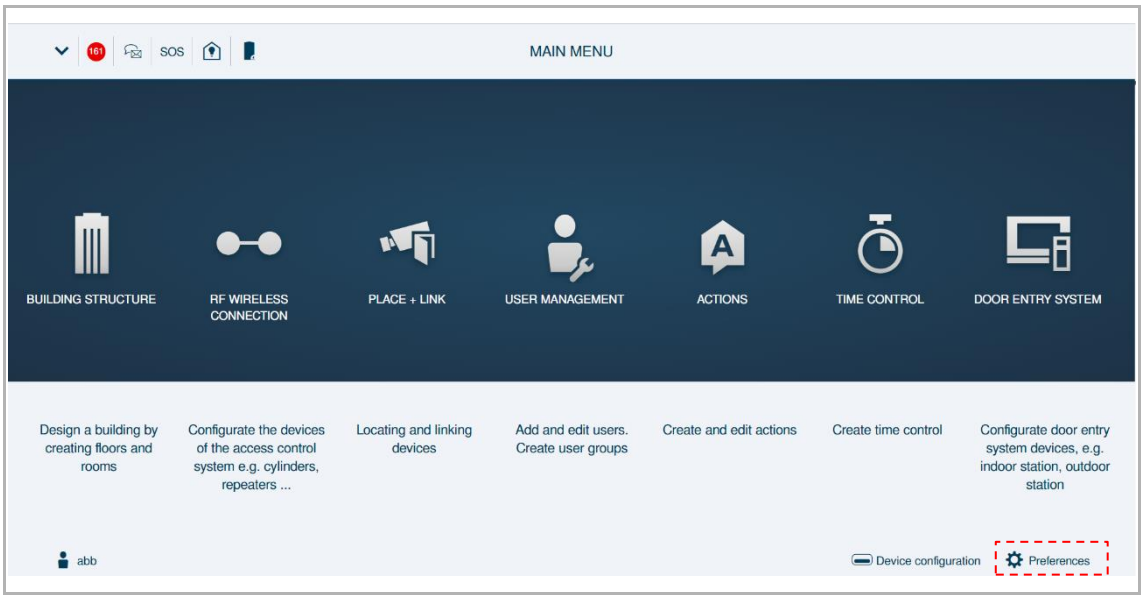
8.7.1 Snelle instellingen openen

Klik in het configuratiescherm op "V" om de snelle instellingen te openen.



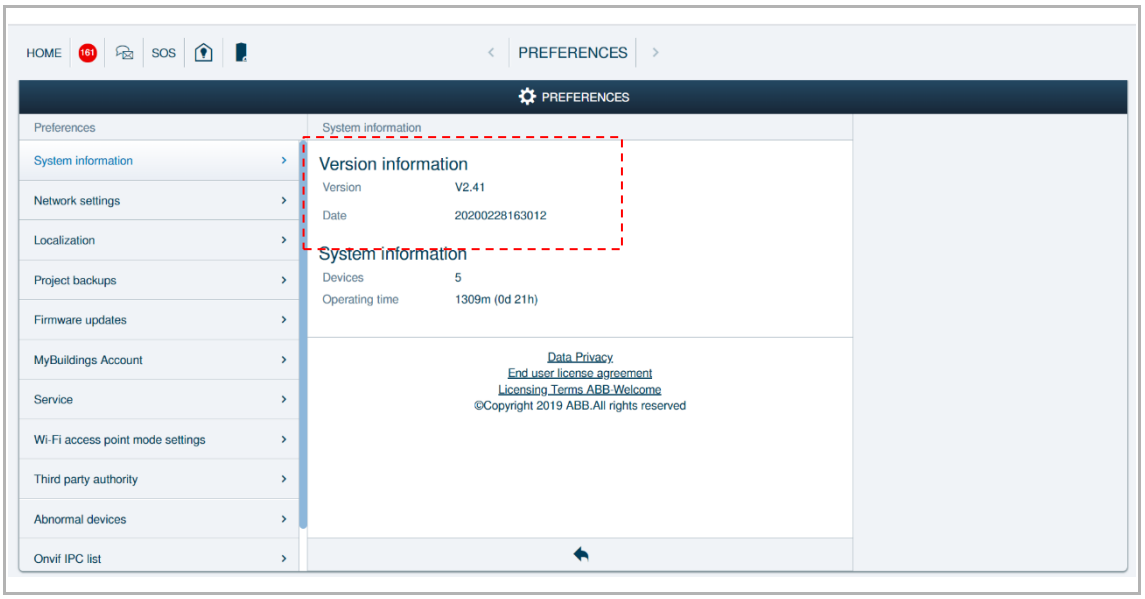
8.7.2 Instellingen: algemeen openen

Klik in het configuratiescherm op "Instellingen" om het bijbehorende scherm te openen.



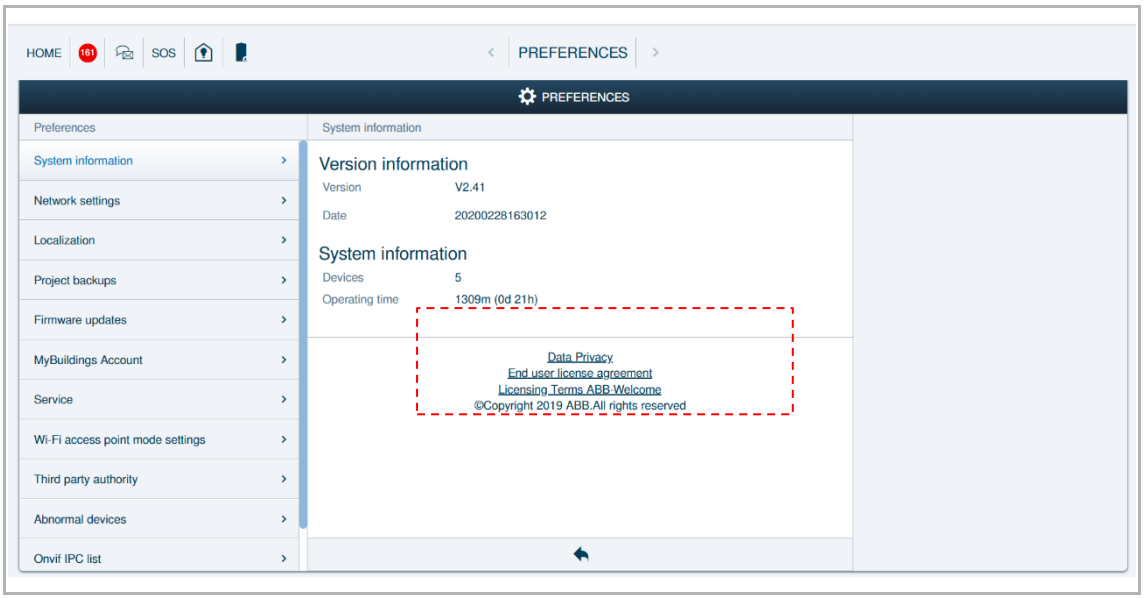
8.7.3 Versie-informatie

Op het scherm "Instellingen", "Systeeminformatie", kunt u de versie-informatie bekijken.



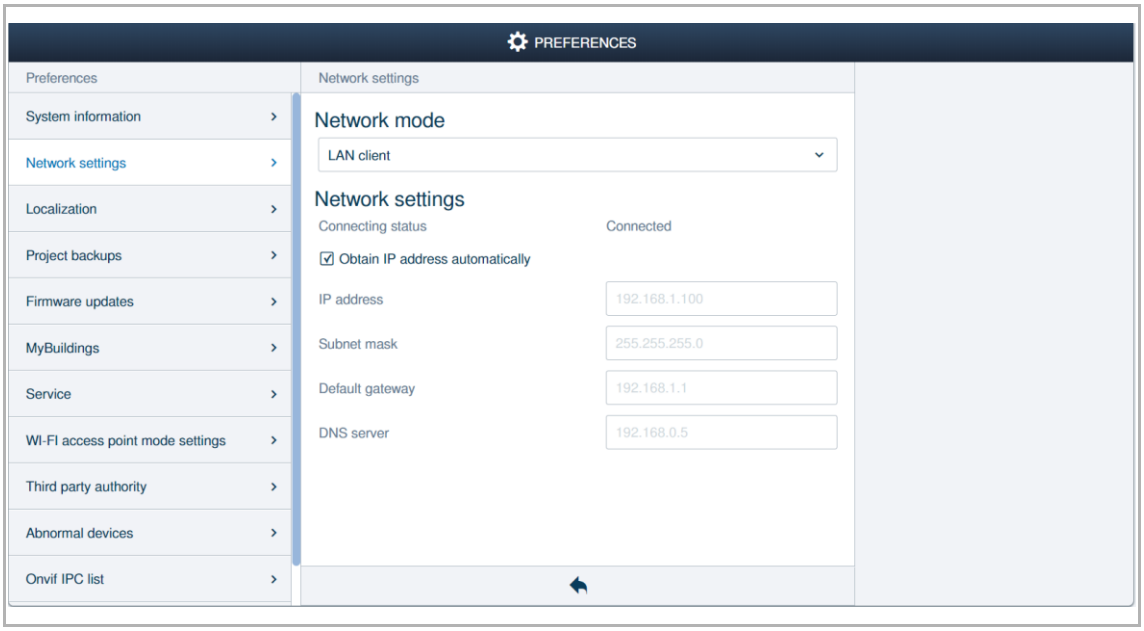
8.7.4 Disclaimer informatie

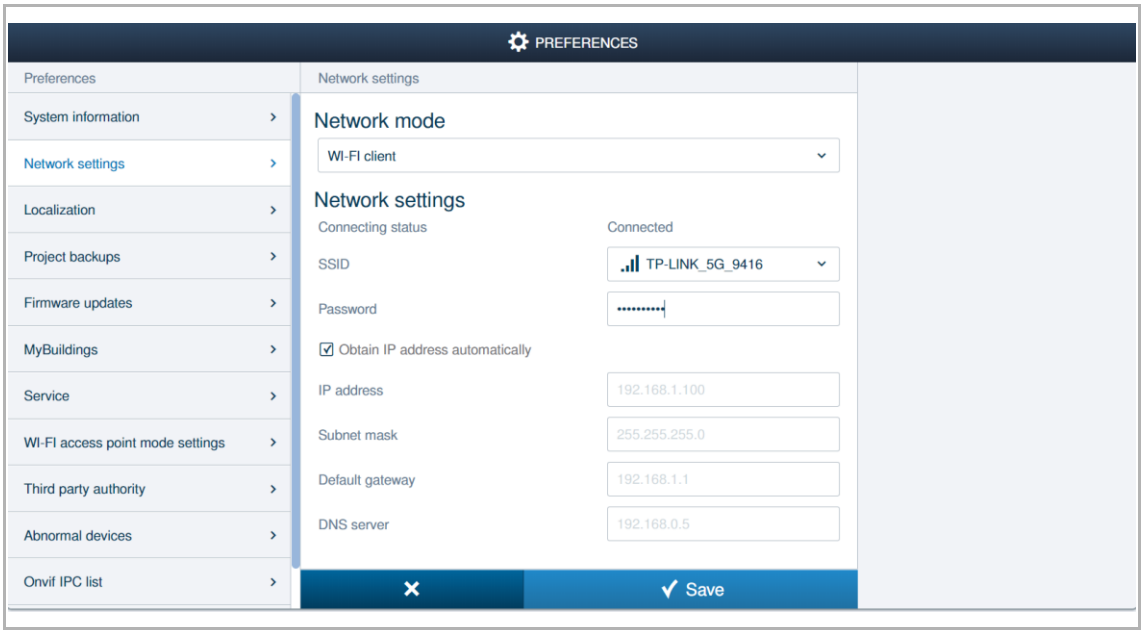
Op het scherm "Instellingen", "Systeeminformatie", kunt u de disclaimer-informatie bekijken.



8.7.5 Netwerkinstellingen

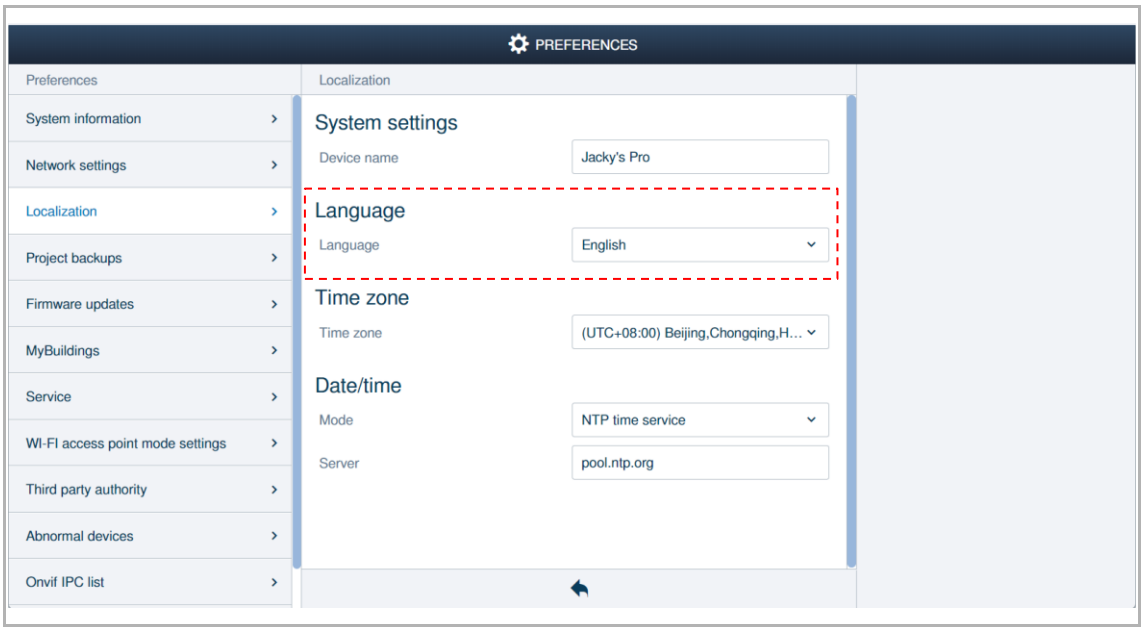
In het scherm "Instellingen", "Netwerkinstellingen" kunt u de netwerkinstellingen wijzigen. zie hoofdstuk 8.3 “Eerste configuratie“ op pagina 19





8.7.6 Taal

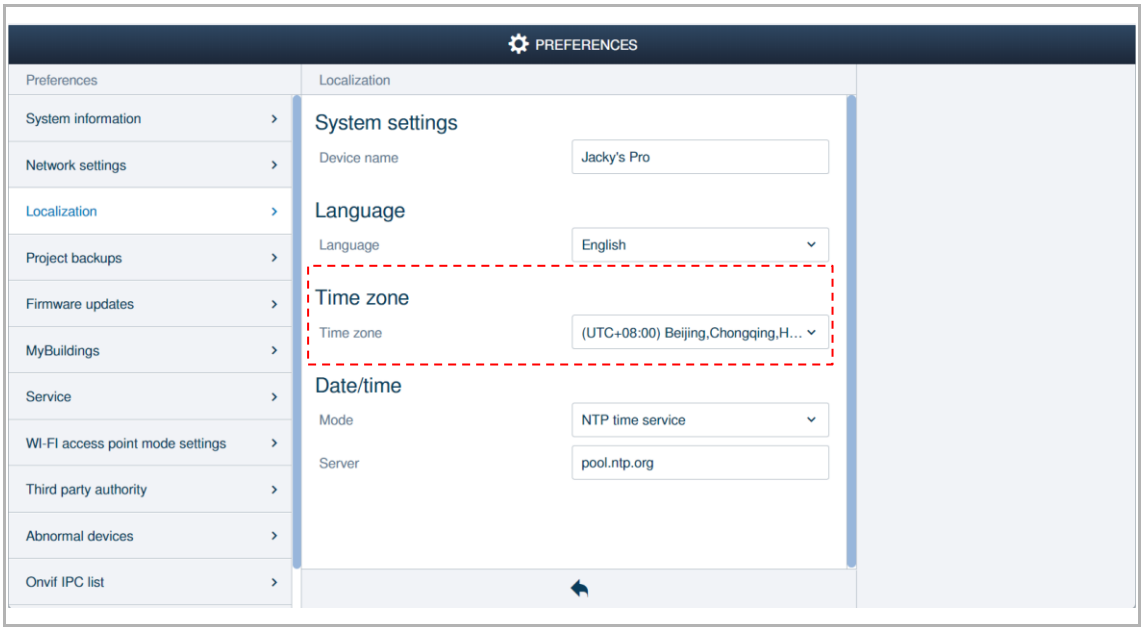
In het scherm "Instellingen", "Lokalisatie", selecteert u de taal in de keuzelijst.



8.7.7 Tijdinstellingen

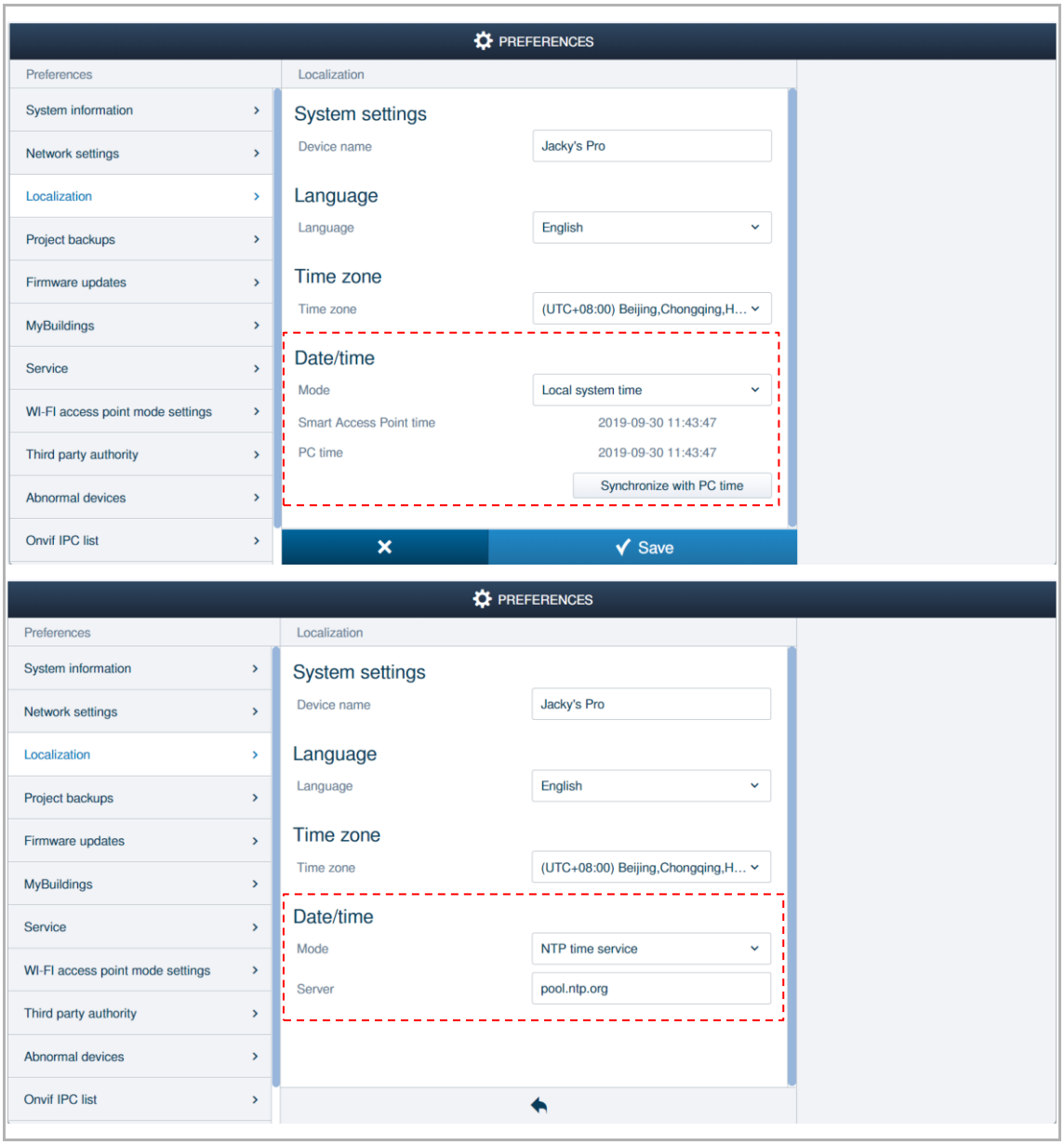
Tijdzone-instelling

In het scherm "Instellingen", "Lokalisatie", selecteert u de tijdzone in de keuzelijst.



Smart Access Point-tijd synchroniseren via lokaal systeem of NTP-server

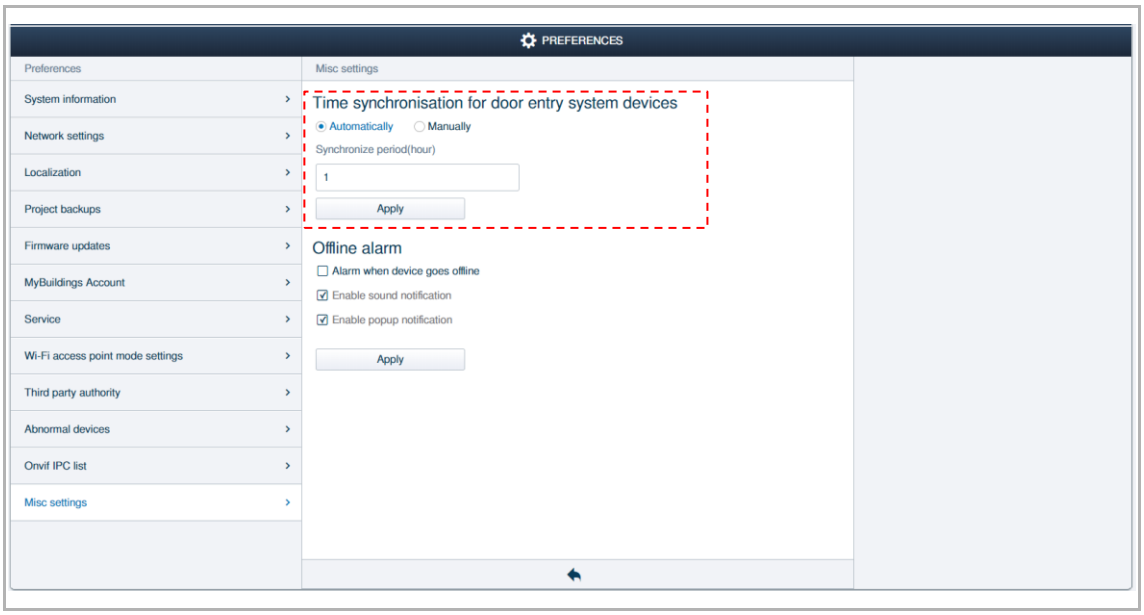
In het scherm "Instellingen", "Lokalisatie", kan de Smart Access Point-tijd worden ingesteld om te synchroniseren vanuit "Lokale systeemtijd" of vanuit " NTP-tijddienst".



Smart Access Point-tijd synchroniseren met andere apparaten in het systeem

Opmerking
Deze functie wordt alleen gebruikt voor apparaten van de buiten-/binnenpost.

In het scherm "Instellingen", "Verschillende instellingen", kunt u "Automatisch" selecteren om de Smart Access Point-tijd regelmatig met andere apparaten in het systeem te synchroniseren. U moet op "Toepassen" klikken voordat de wijziging van kracht wordt.

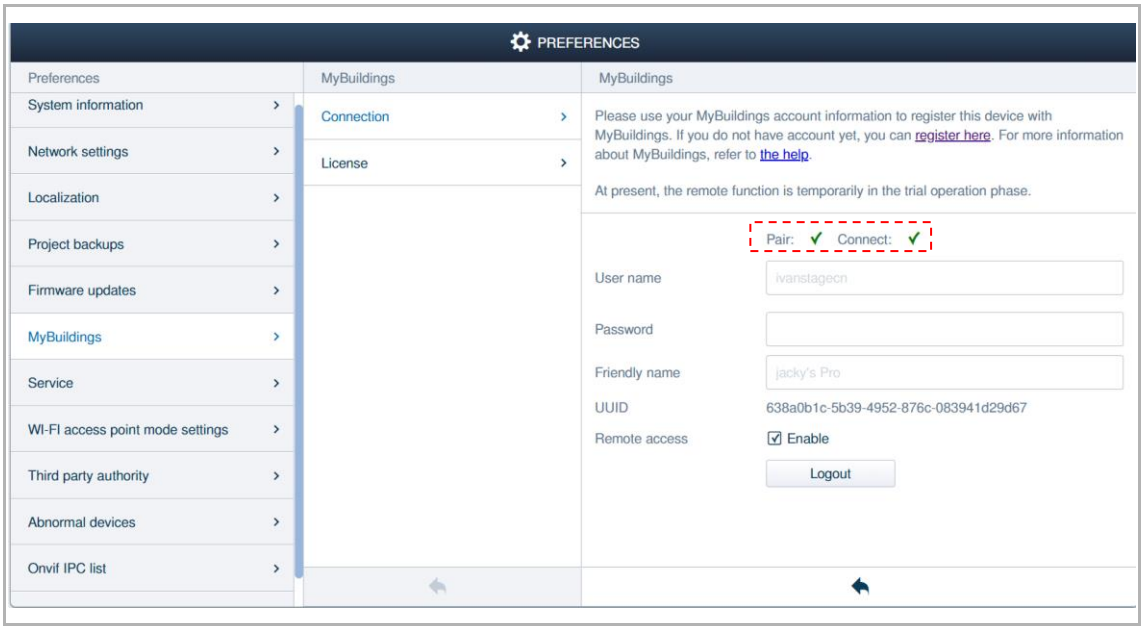


8.7.8 MyBuildings-instellingen

"Paar" wordt weergegeven wanneer account en wachtwoord correct zijn.

"Verbinden" wordt weergegeven wanneer Smart Access Point succesvol is verbonden met het MyBuildings-portaal.

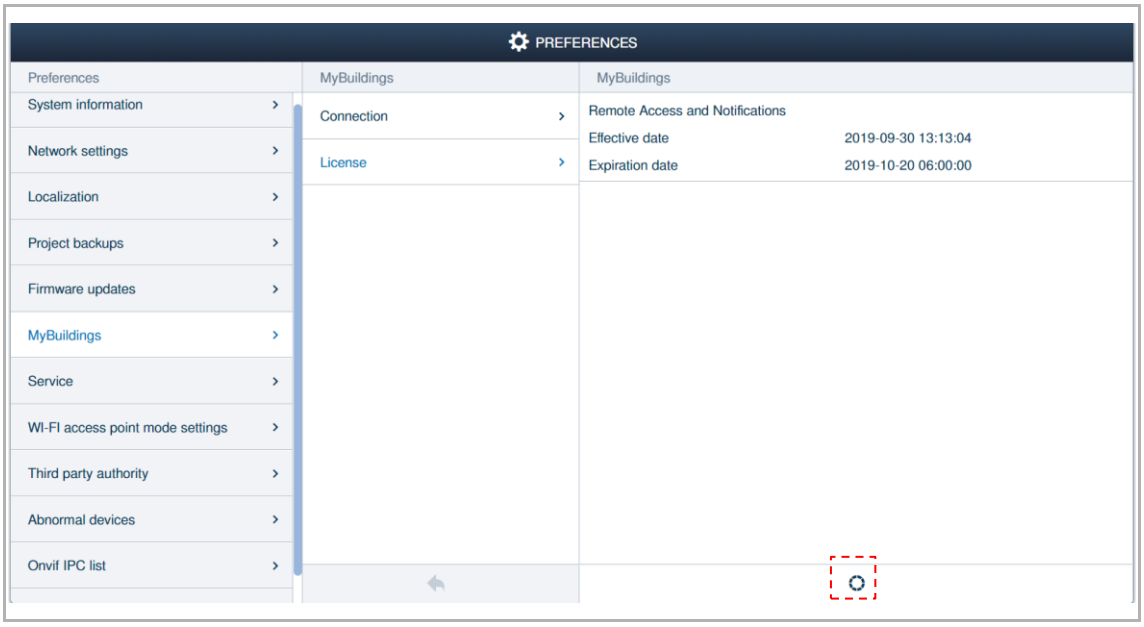
Als "Toegang op afstand" is geactiveerd, hebt u toegang tot "Smart Access Point" op het MyBuildings-portaal. U moet zich echter wel abonneren op de service "Toegang op afstand" op het MyBuildings-portaal voordat deze functie wordt gebruikt.



Licentie vernieuwen

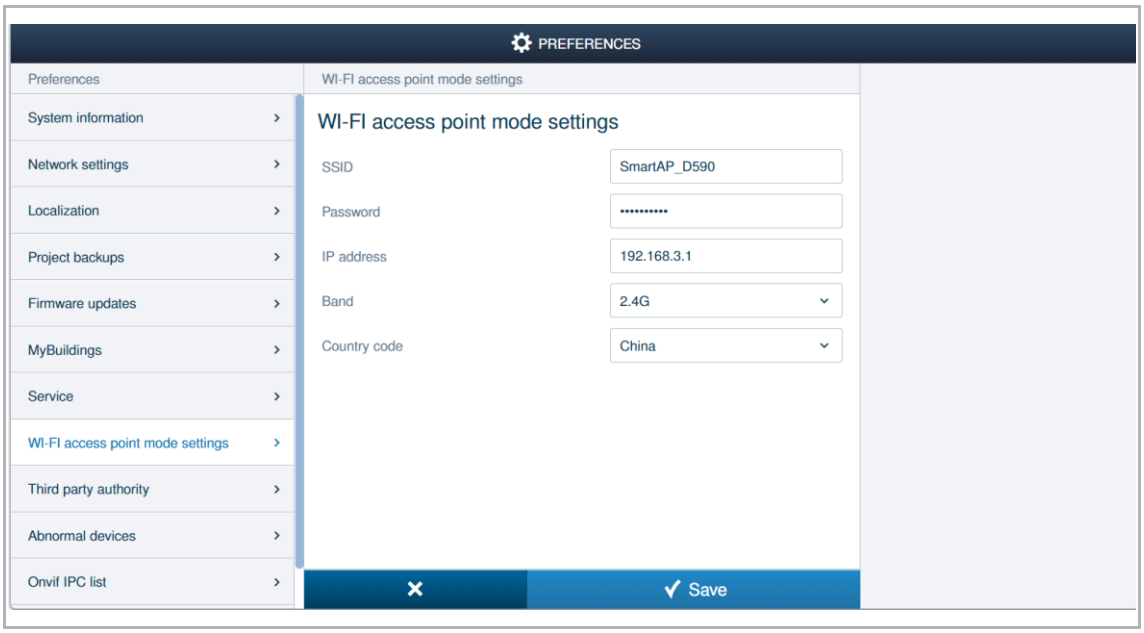
U kunt de licentie vernieuwen nadat u zich op de service op afstand hebt geabonneerd.

In het scherm "Instellingen", "MyBuildings", "Licentie", klikt u op "○" om de licentie te vernieuwen.



8.7.9 Instellingen APP-modus

In het scherm "Instellingen", "Instellingen Wifi Access Point-modus" kunt u de instellingen voor de WiFi Access Point-modus wijzigen.

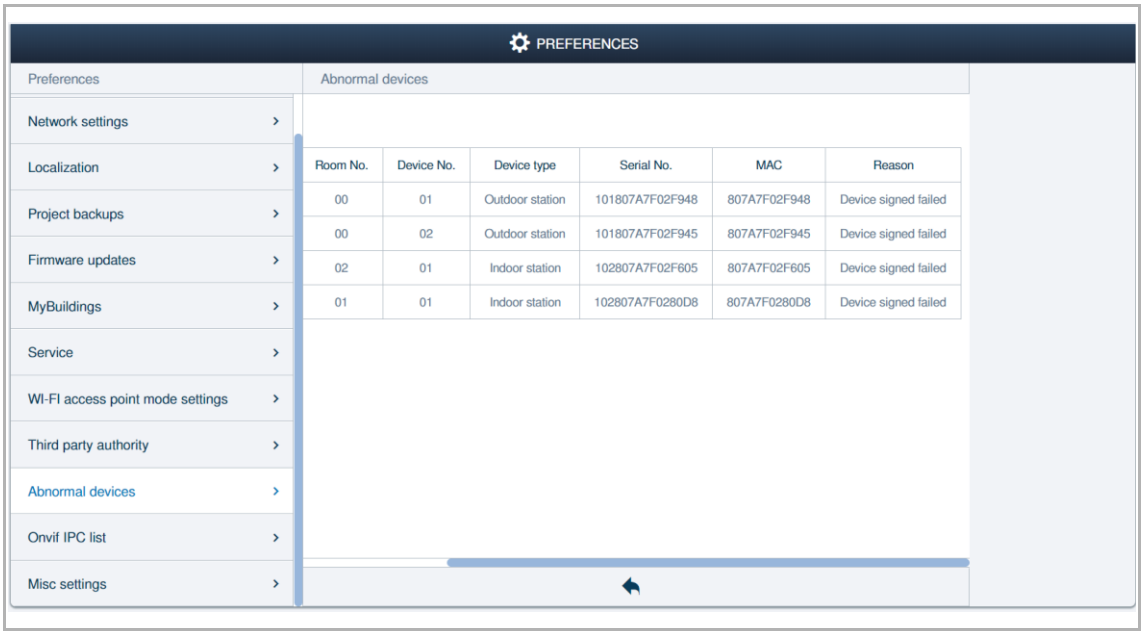


8.7.10 Instellingen Externe bevoegdheid

Een apparaat van een andere fabrikant kan de gegevens voor de buiten-/binnenpost (bijv. ontgrendelingsinformatie) verkrijgen via het "Smart Access Point" door het instellen van het aangewezen IP-adres en de poort van het apparaat van de andere fabrikant.

In het scherm "Instellingen", "Externe bevoegdheid", klikt u op "Toevoegen", voert u het IP-adres en het IP-nummer in en klikt u vervolgens op "Toegepast" om de instelling toe te passen.

Op het scherm "Instellingen", "Niet geïnt. app.", kunt u de details van niet geïntegreerde apparaten bekijken (bijv. apparaat ondertekend mislukt, communicatie mislukt, enz.).



U kunt het apparaat controleren wanneer "Apparaat ondertekend mislukt" in de lijst met niet geïntegreerde apparaten verschijnt.

- Is het apparaat eerder ondertekend?
- Werkt het apparaat in de veiligheidsmodus?
- Is er een conflict met het IP-adres van het apparaat en dat van andere apparaten?

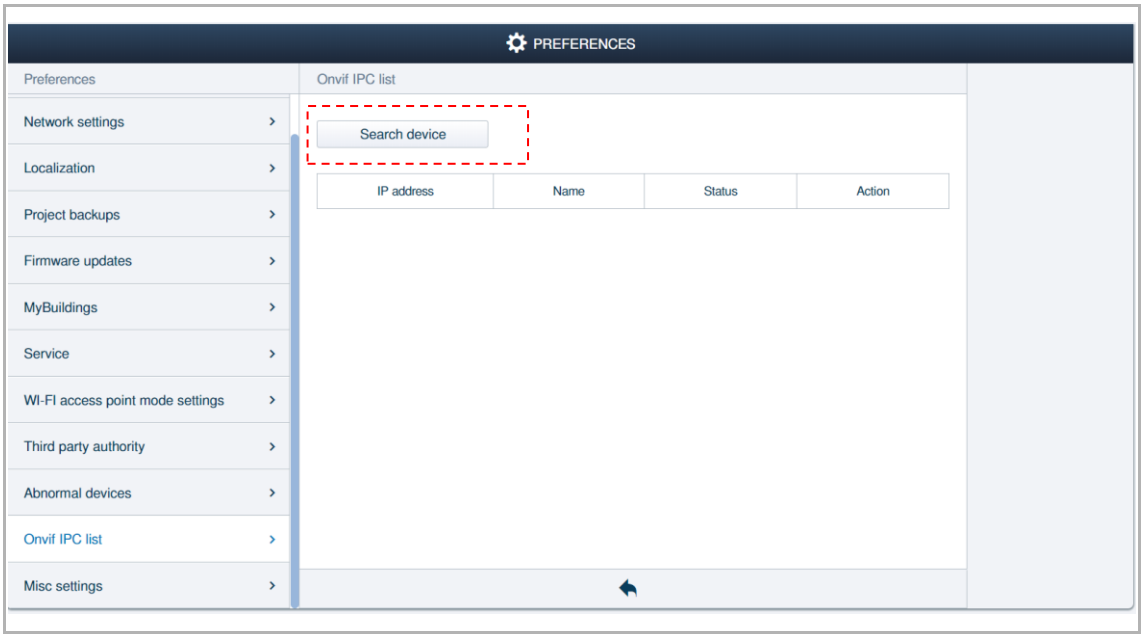
8.7.11 Onvif IPC-instellingen

Een binnenpost kan de functie "Community monitor" niet gebruiken voordat de IPC-camera's hier zijn ingesteld.

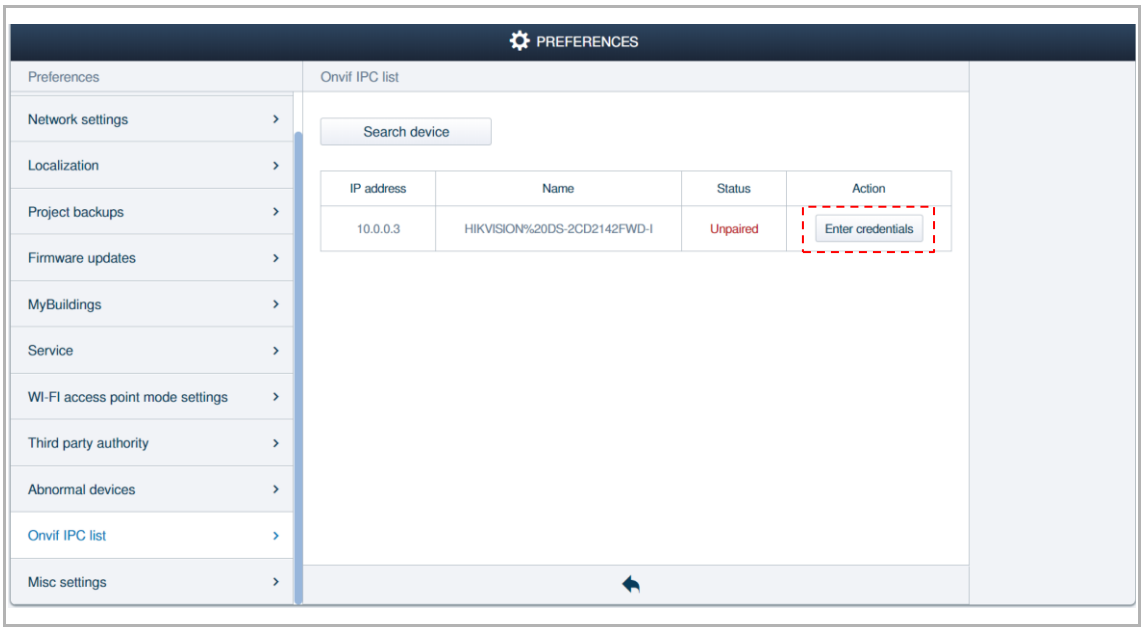
Protocol	Stel als "ONVIF" of "ONVIF Profiel S"
Type codering van video	Stel als "H.264"
Resolutie	Set to max. 1920x1080 (1080p)

Voor IP-camera's kunnen de volgende adressen worden toegewezen in het gemeenschap/functioneel netwerk: -10.0.3.1 -server-8230; 10.0.3.254.In dit adresbereik kunnen ook andere apparaten, zoals een computer, de 10-type adressen gebruiken zonder in conflict te komen met het ABB-Welcome IP-adresbereik.

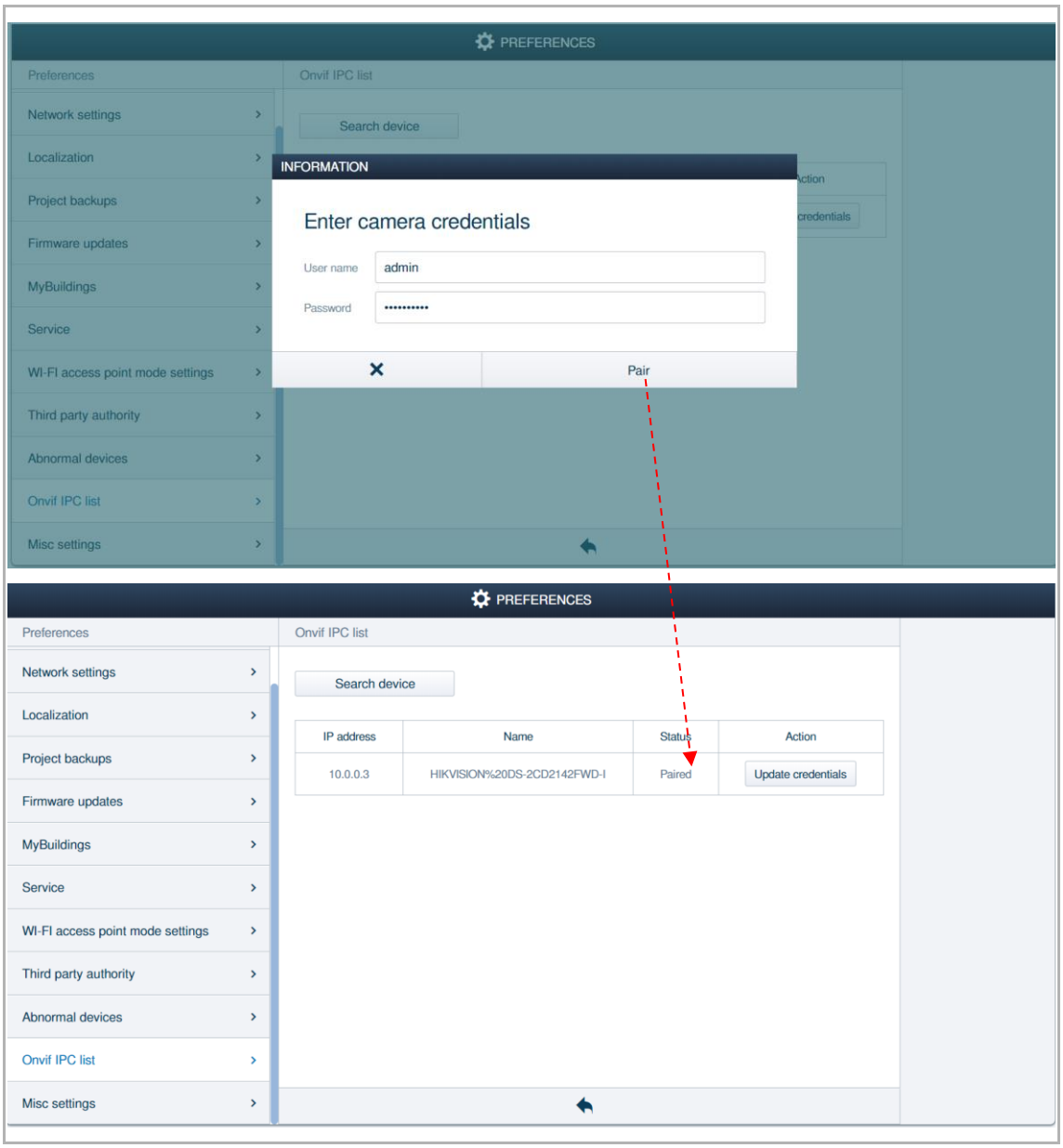
Klik in het scherm "Instellingen", "Onvif-IPC-lijst" van Smart Access Point op "Apparaat zoeken" om de IP-camera te zoeken die voor het openbare netwerk worden gebruikt.



Klik vervolgens op "Inloggegevens inv." nadat de IP-camera is gedetecteerd.

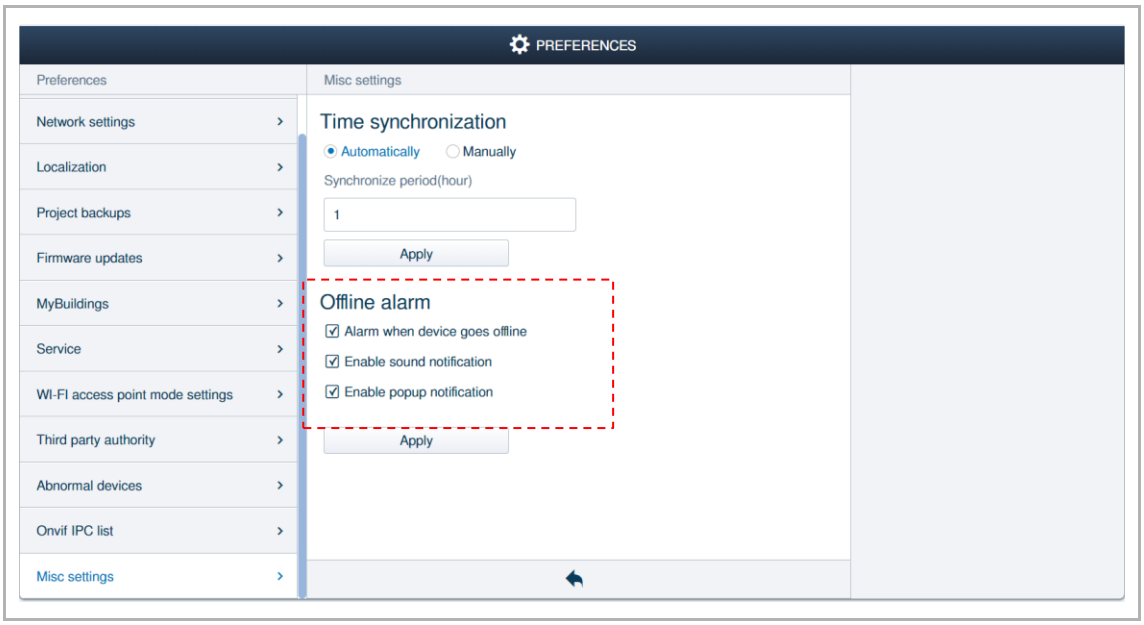


Voer de gebruikersnaam en het wachtwoord van de IP-camera in en klik vervolgens op "Paar".



8.7.12 Alarm-meldingsinstellingen

In het scherm "Instellingen", "Versch. inst.", zijn de geluidsmelding en popupmelding alleen beschikbaar als de functie "Alarm wanneer het apparaat offline gaat" is geactiveerd.



Opmerking

Het alarm wordt gemeld via buitenpost 1 (apparaat-ID=1) of via deurpost 1 (apparaat-ID=1). Als een van deze twee apparaten niet in het systeem kan worden herkend, kan het alarm niet succesvol aan Smart Access Point worden gerapporteerd.

9 Door Entry system-apparaten bedienen

9.1 Topologie buiten-/binnenpost

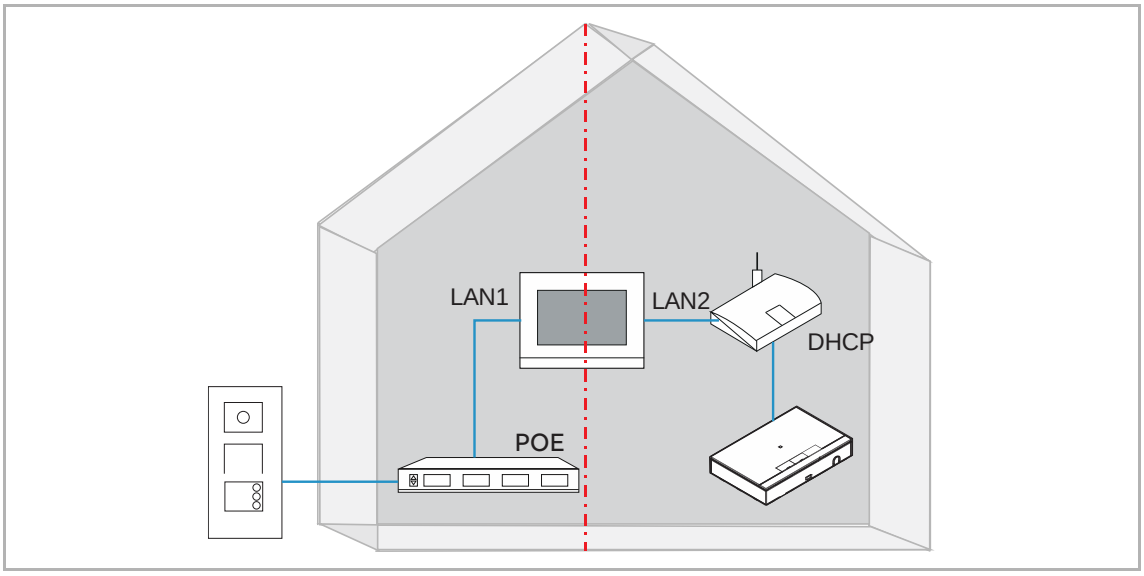
Topologie 1: eengezinswoning

In een ABB-Welcome IP systeem in een particulier gebouw wordt het netwerk van het gebouw losgekoppeld van het unit netwerk.Dit voorkomt ongeoorloofde toegang tot het privé-netwerk via het buitenstation.

Een IP Touch 7/10 is geïnstalleerd.

In dit type installatie voldoet het IP Touch 7/10 bovendien aan de functie van een IP gateway.

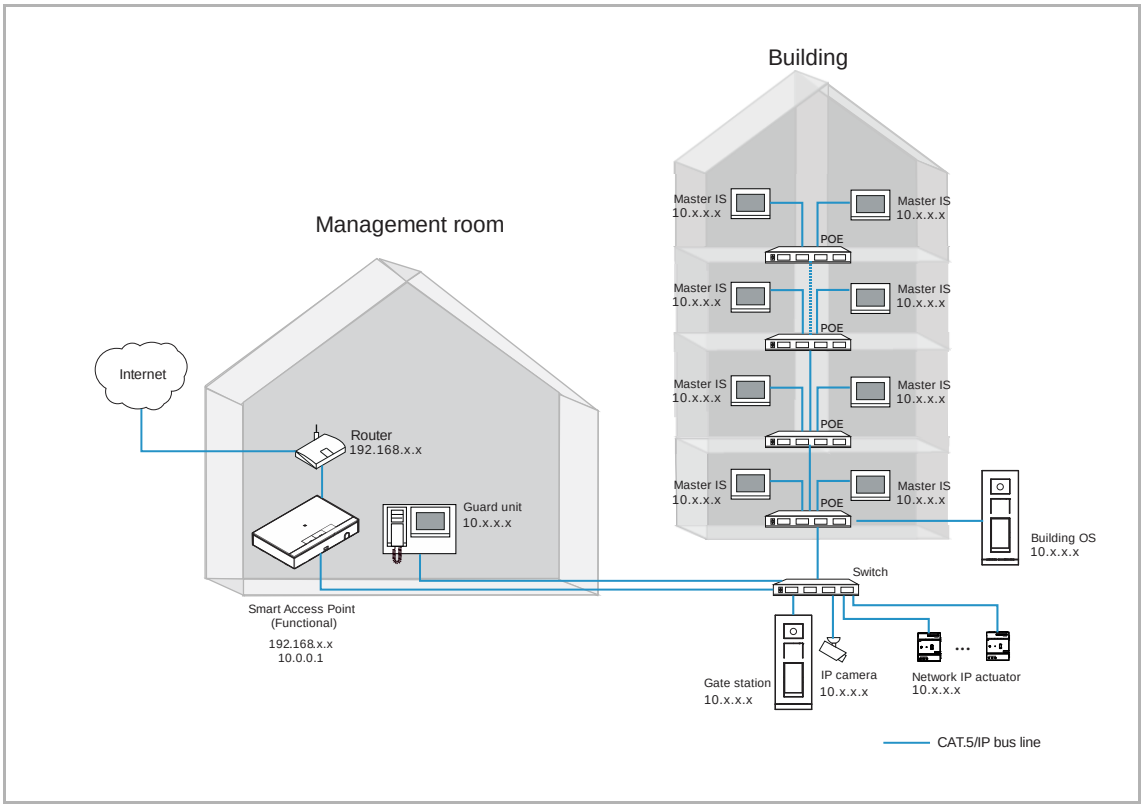
"Smart Access Point" moet worden ingesteld op "Commercial Mode" bij de initiële opstelling.



Topologie 2: appartementencomplex

In dit geval moet "Smart Access Point" tijdens de eerste installatie worden ingesteld op "Functiemodus". zie hoofdstuk 8.3 “Eerste configuratie“ op pagina 19

In dit geval wordt "Smart Access Point" gebruikt om alle apparaten in het gebouw te beheren.

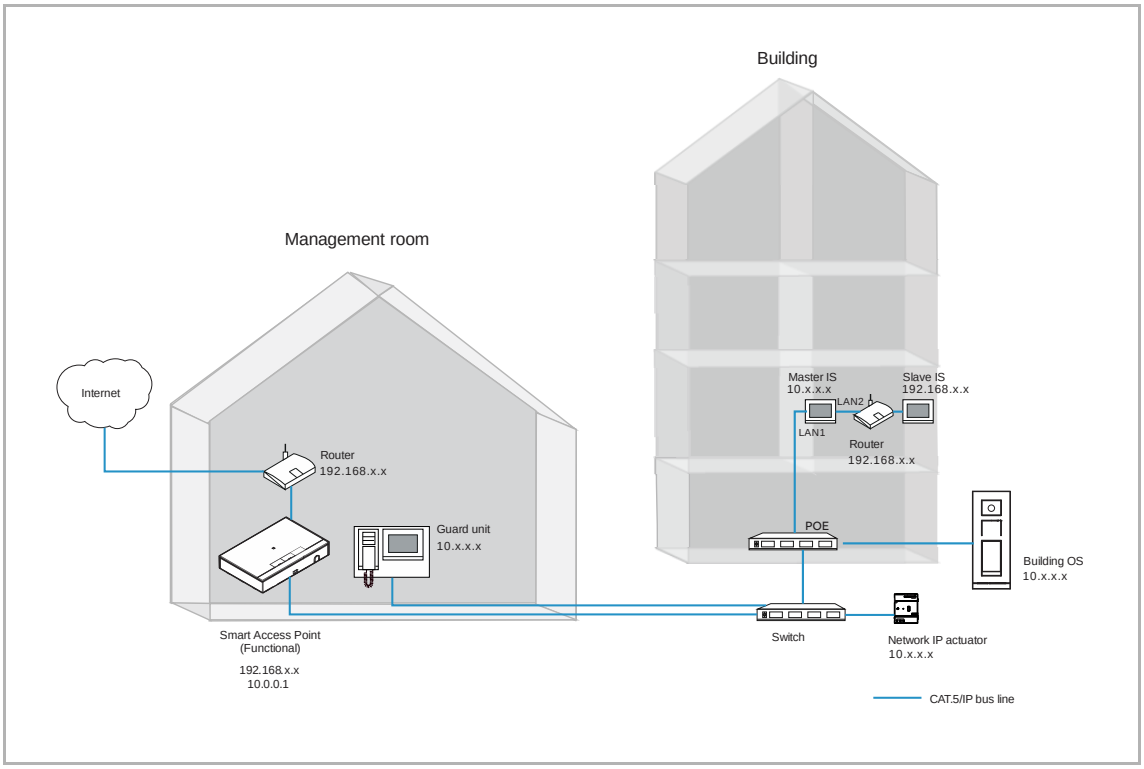


Demonstratie voor het bedienen van de apparaten van de buiten-/binnenpost

De volgende demonstratie verwijst naar de topologie 2.

Deze demonstratie is bedoeld om vertrouwd te raken met de werking van de apparaten van de buiten-/binnenpost.

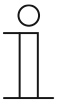
U dient uw handelingen aan te passen wanneer u een echt project uitvoert.



9.2 Apparaatbeheer

Opmerking

Alle apparaten van de buiten-/binnenposten moeten voor gebruik worden voorzien van een handtekening op het "Smart Access Point".



Opmerking

Het "Smart Access Point" wijst automatisch een handtekening toe aan de apparaten wanneer ze worden toegevoegd.

Opmerking

Als het apparaat al door dit Smart Access Point is ondertekend, wordt het niet opnieuw ondertekend.

Opmerking

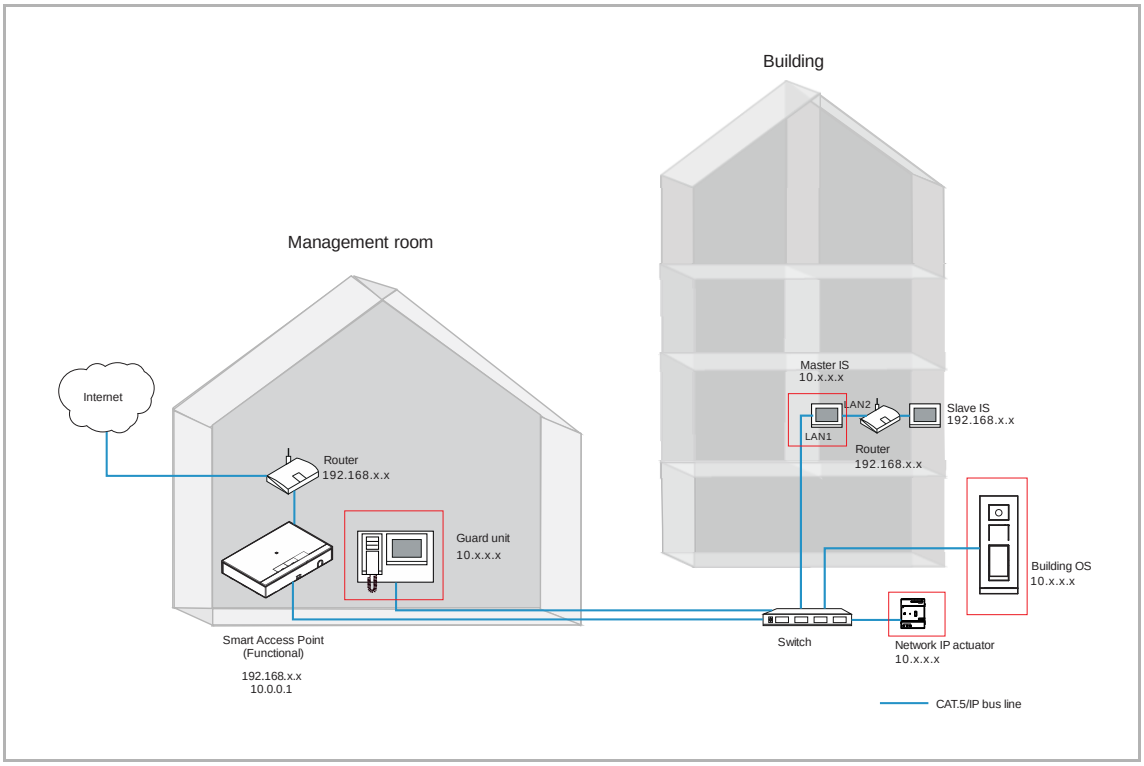
Als het apparaat al door een ander Smart Access Point is ondertekend, wordt het niet ondertekend en wordt "Ondertekenen mislukt" weergegeven op het scherm "Niet geïnt. app.". zie hoofdstuk **Error! Reference source not found.** “**Error! Reference source not found.**“ op pagina **Error! Bookmark not defined.**

9.2.1 Apparaten automatisch toevoegen

Opmerking

Alleen de apparaten op hetzelfde netwerksegment als het "Smart Access Point" kunnen automatisch worden gezocht. Zie de apparaten die omgeven zijn door een rood kader in het onderstaande diagram.

"Slave-binnenpost" kan niet worden toegevoegd via automatisch zoeken.



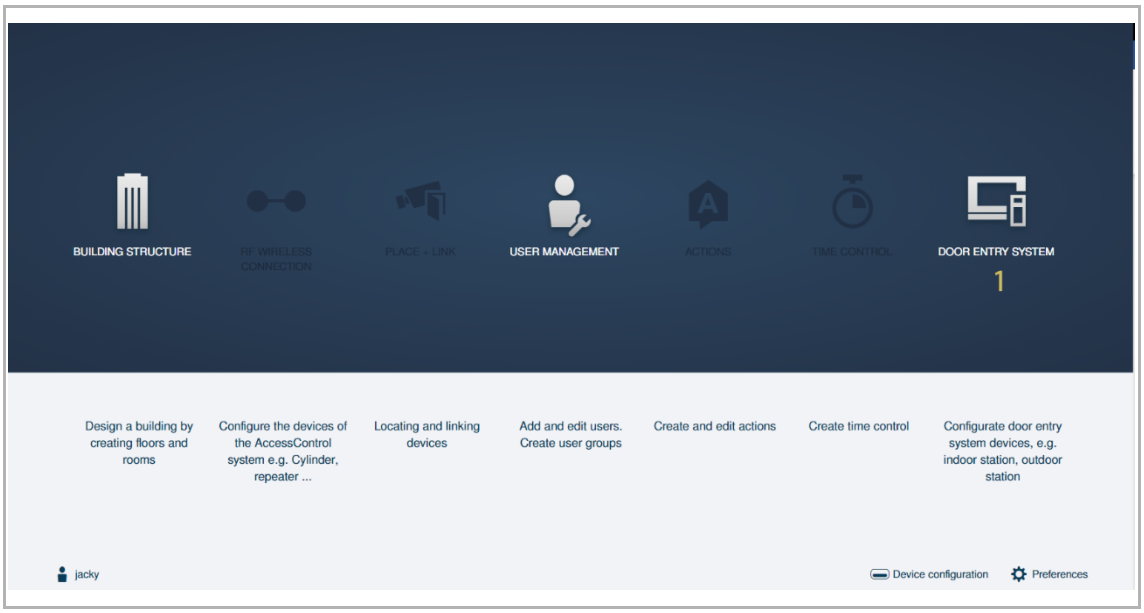
Voorwaarde

- Alle apparaten moeten ingeschakeld zijn.
- Alle apparaten moeten een ander fysiek adres hebben.
- Geen van de apparaten mag worden ondertekend door een ander "Smart Access Point". Als het apparaat door een ander "Smart Access Point" is ondertekend, moet u de handtekening wissen, bijvoorbeeld door het fysieke adres van het apparaat te wijzigen.

Apparaten toevoegen via automatisch zoeken

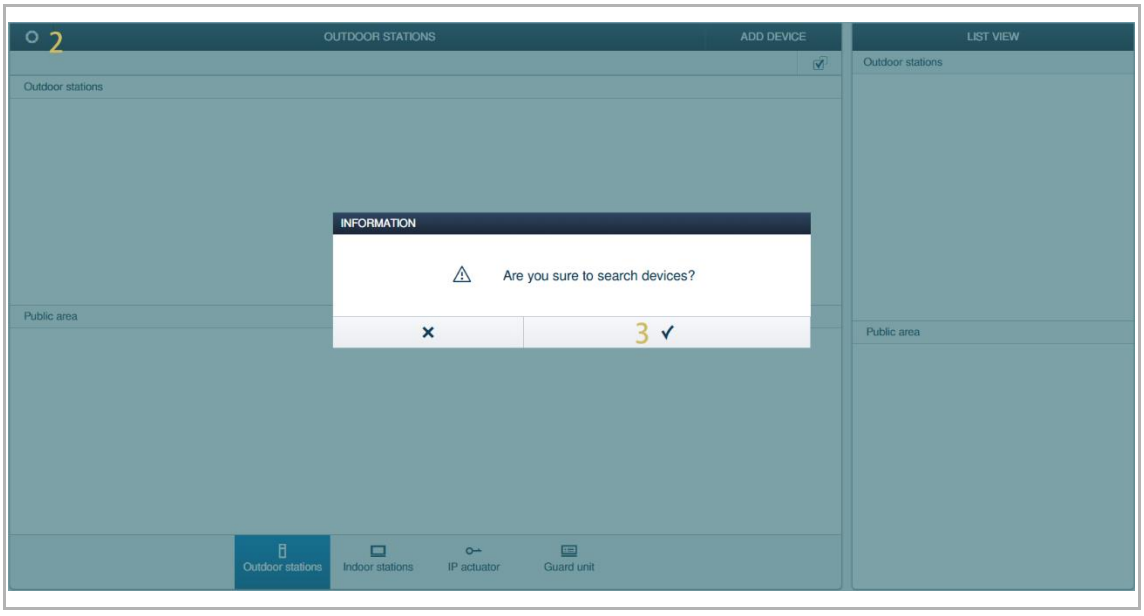
Volg de onderstaande stappen:

[1] Klik op het configuratiescherm op "Buiten-/binnenpost", "om naar het scherm van de buiten-/binnenpost te gaan.



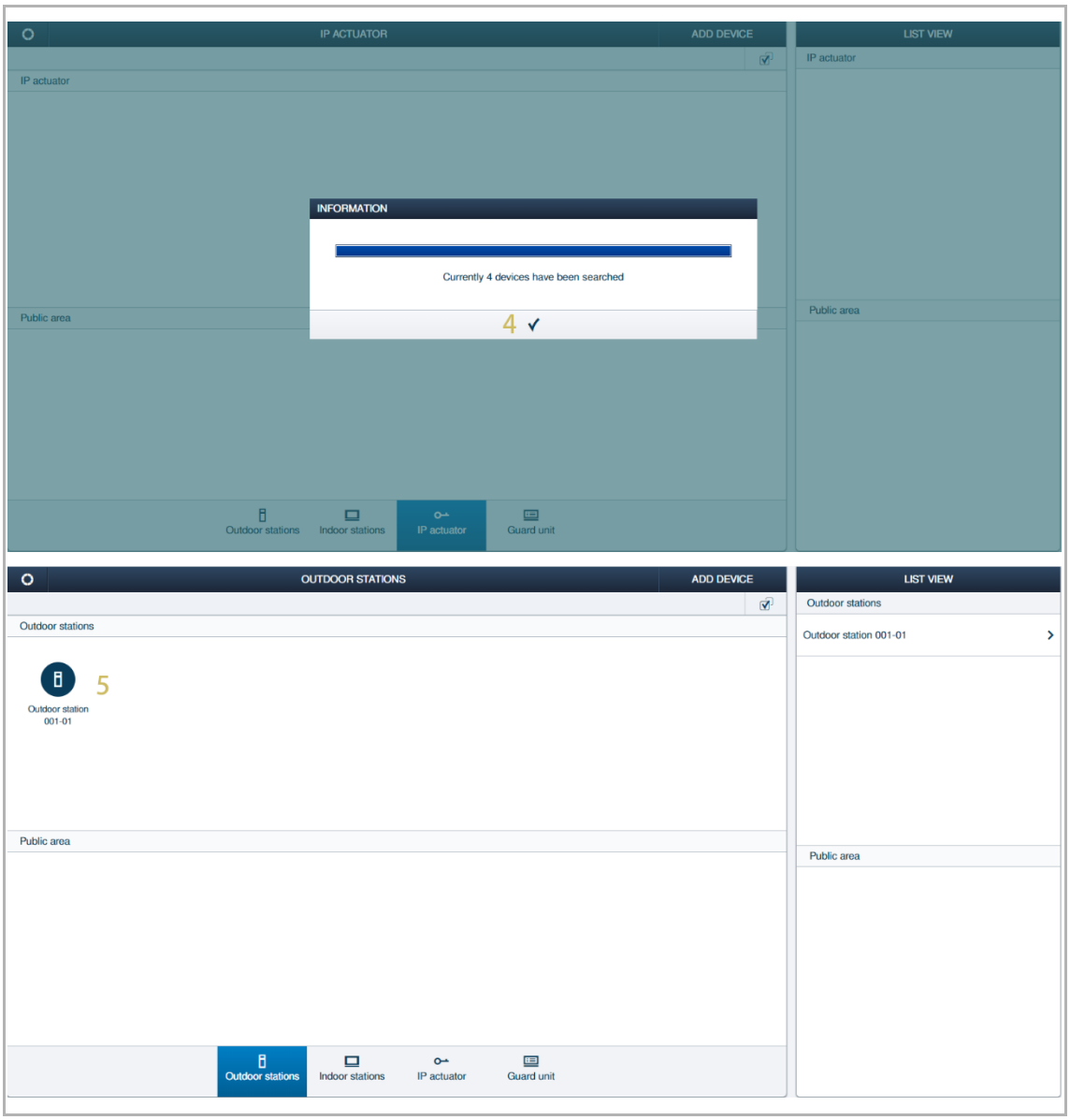
[2] Op het scherm "Buiten-/binnenpost" klikt u op " ".

[3] Klik op "√" om door te gaan.



[4] Het zoekresultaat wordt weergegeven op het scherm, klik op "√" om door te gaan.

[5] Indien succesvol worden de apparaten op het scherm weergegeven.



zie hoofdstuk 9.2.2 “Apparaten handmatig toevoegen“ op pagina 62

9.2.2 Apparaten handmatig toevoegen

Opmerking

Alle apparaten kunnen handmatig worden toegevoegd op het "Smart Access Point".

"Slave-binnenpost" kan niet op deze worden toegevoegd.

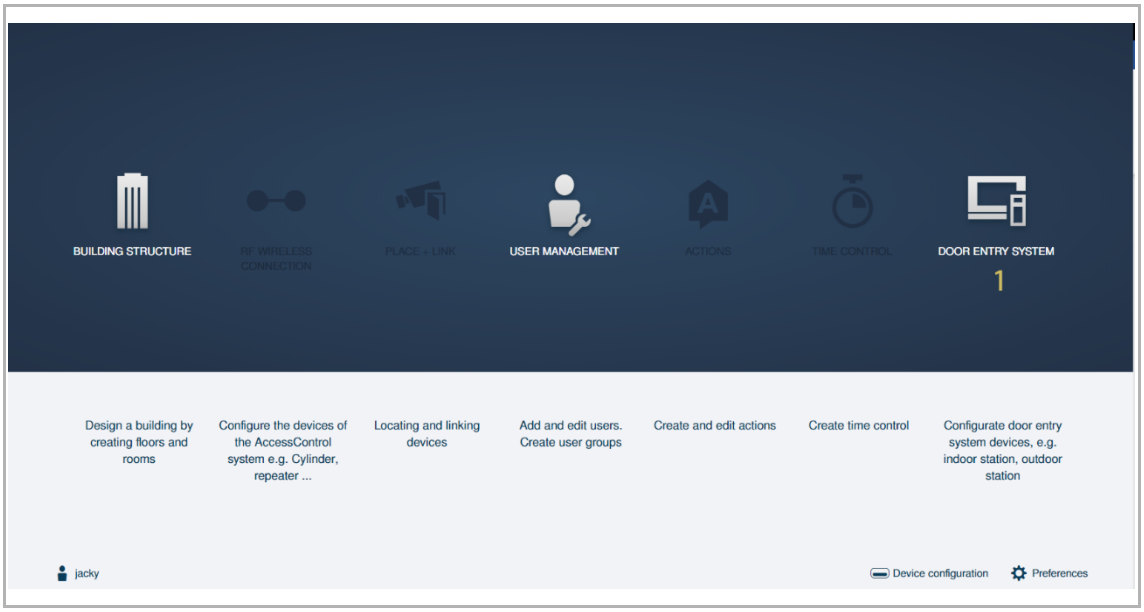
Voorwaarde

- Alle apparaten die handmatig moeten worden toegevoegd, moeten worden ingeschakeld.
- Geen van de handmatig toe te voegen apparaten mag door een ander "Smart Access Point" ondertekend zijn. Als het apparaat door een ander "Smart Access Point" is ondertekend, moet u de handtekening wissen, bijvoorbeeld door het fysieke adres van het apparaat te wijzigen.

Apparaten handmatig toevoegen

Volg de onderstaande stappen:

[1] Klik op het configuratiescherm op "Buiten-/binnenpost", "om naar het scherm van de buiten-/binnenpost te gaan.



[2] Op het scherm "Buiten-/binnenpost" klikt u op "App. toevoegen".

Opmerking
De volgende handelingen laten zien hoe je een slave-binnenpost kunt toevoegen. Pas uw handelingen aan op basis van de eigenlijke apparaten.

[3] Selecteer een apparaattype uit de keuzelijst (bijv. "binnenpost").

[4] Voer het bloknummer in.

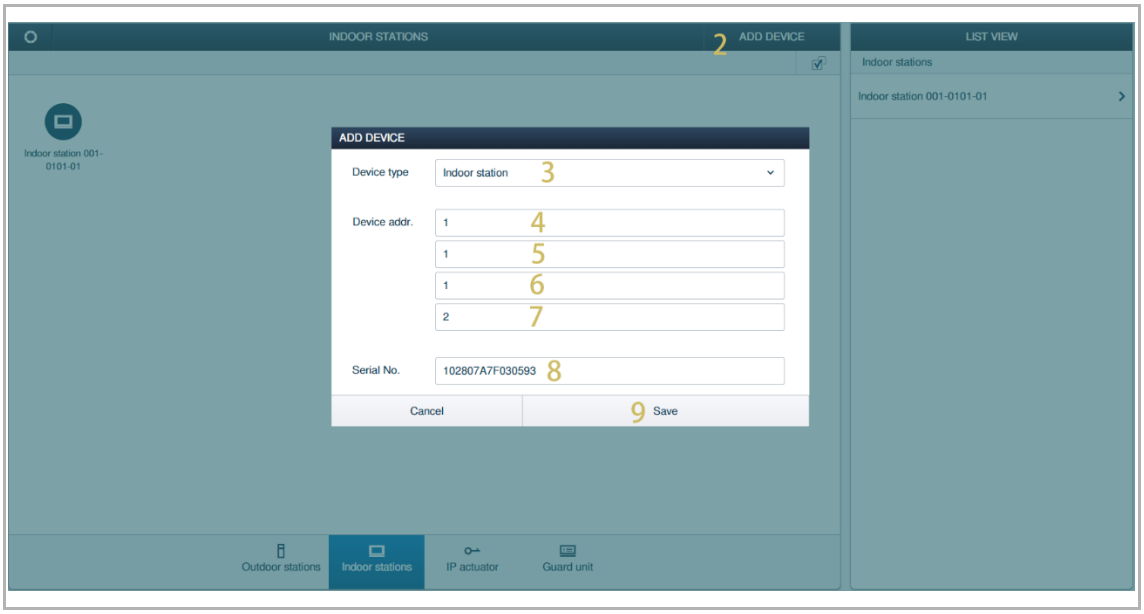
[5] Voer het etagenummer in.

[6] Voer het ruimtenummer in.

[7] Voer het apparaatnummer in.

[8] Voer het serienummer in.

[9] Klik op "Opslaan" om op te slaan.



[10]Indien succesvol wordt het apparaat op het scherm weergegeven.

Opmerking
Als het apparaat al door een ander Smart Access Point is ondertekend, wordt het niet ondertekend en wordt "Ondertekenen mislukt" weergegeven op het scherm "Niet geïnt. app". zie hoofdstuk **Error! Reference source not found.** “**Error! Reference source not found.**“ op pagina **Error! Bookmark not defined.**

9.3 Vertrouwde apparaten beheren

9.3.1 Vertrouwde apparaten voor de buitenpost beheren

Als u het slot van de buitenpost wilt ontgrendelen, moet u het volgende controleren:

- Als de binnenpost en de buitenpost op het "Smart Access Point" zijn gesigneerd.
- Als de binnenpost toegevoegd is aan de lijst met vertrouwde apparaten op de buitenpost.

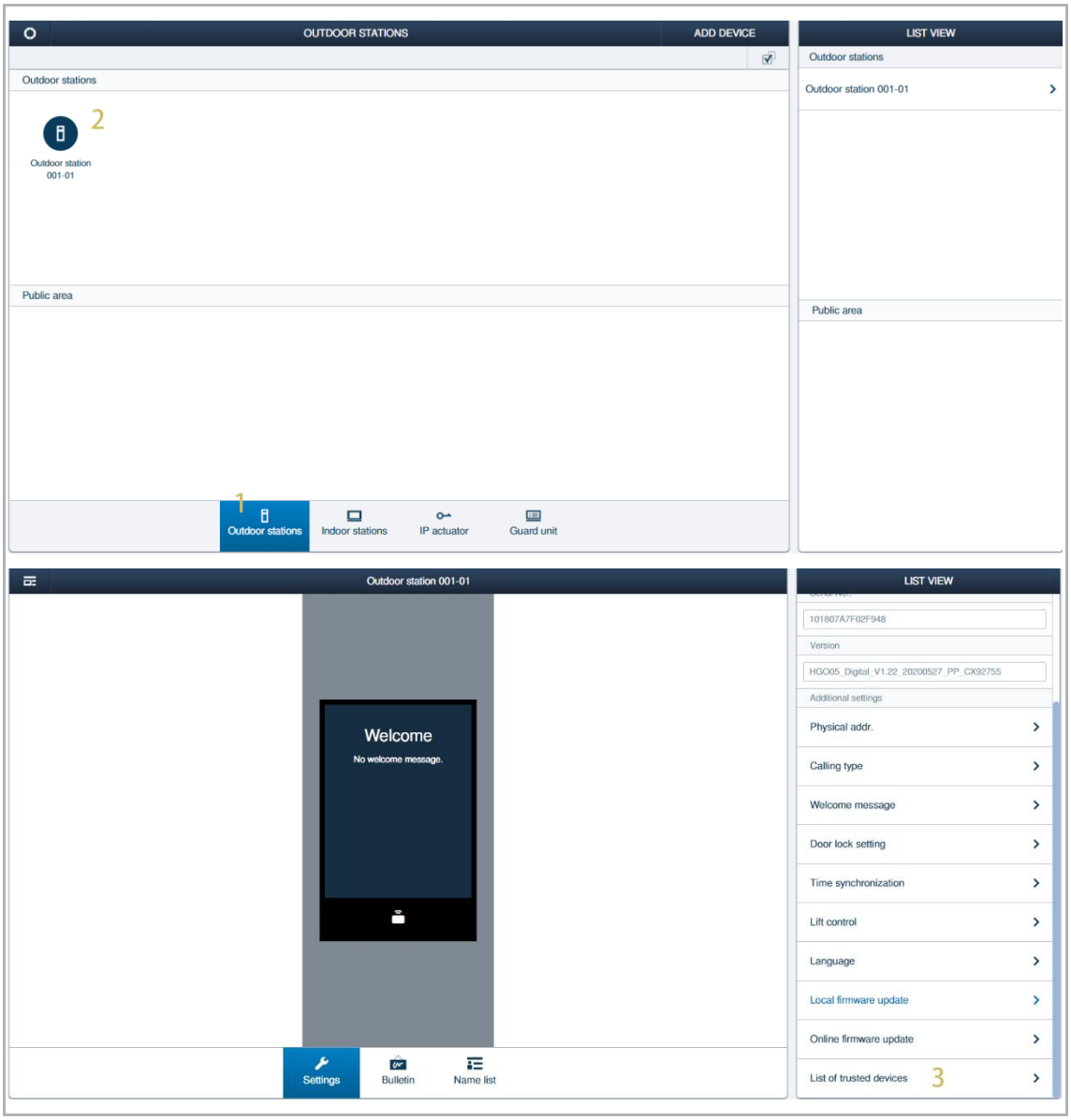
1. Vertrouwde apparaten toevoegen

Volg de onderstaande stappen:

[1] Klik in het scherm "Buiten-/binnenpost" op "Buitenposten".

[2] Klik op de gewenste buitenpost.

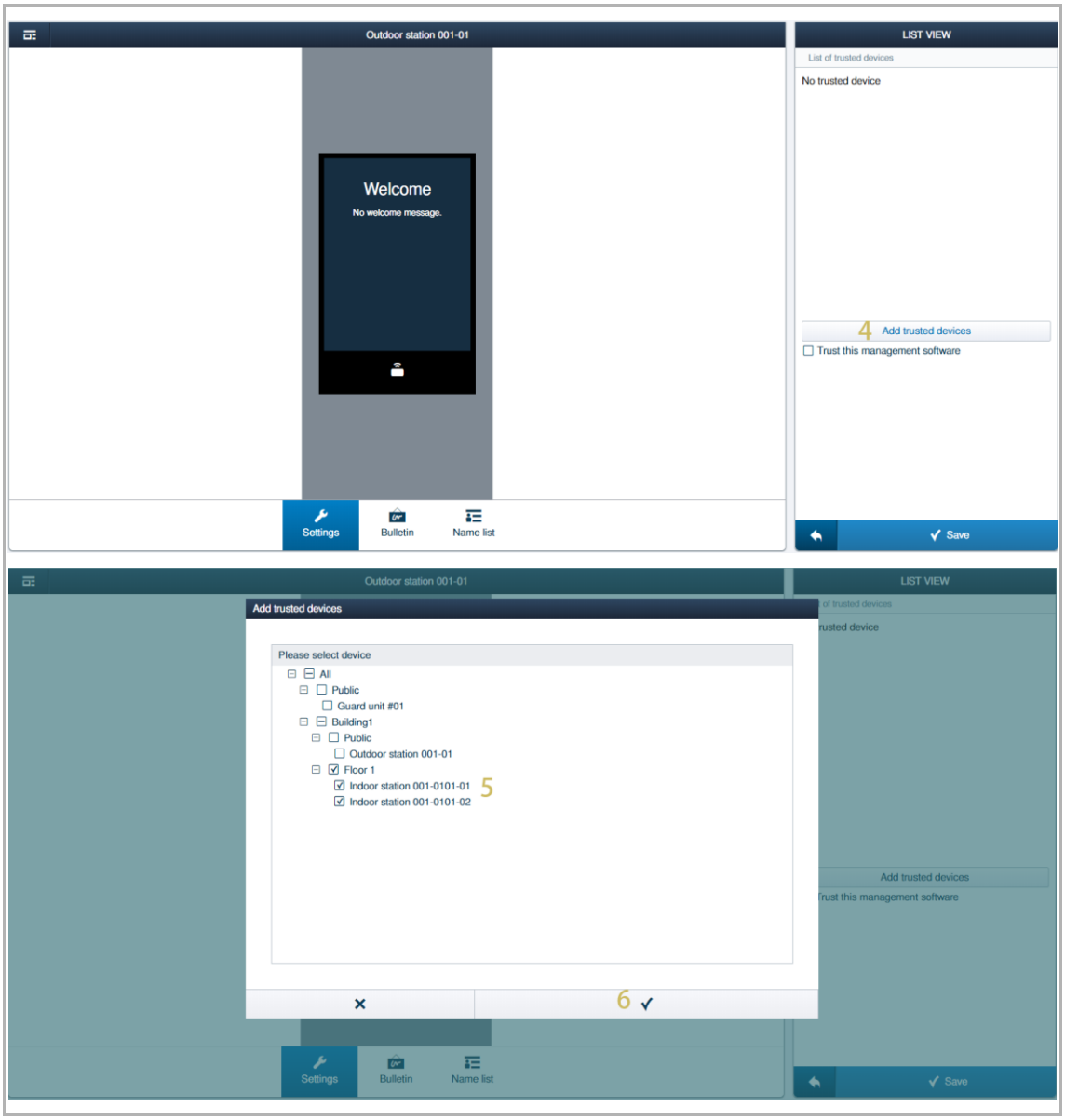
[3] Scrol naar beneden in de lijst en klik op "Lijst met vertrouwde apparaten".



[4] Klik op "Vertr. app.toevoegen".

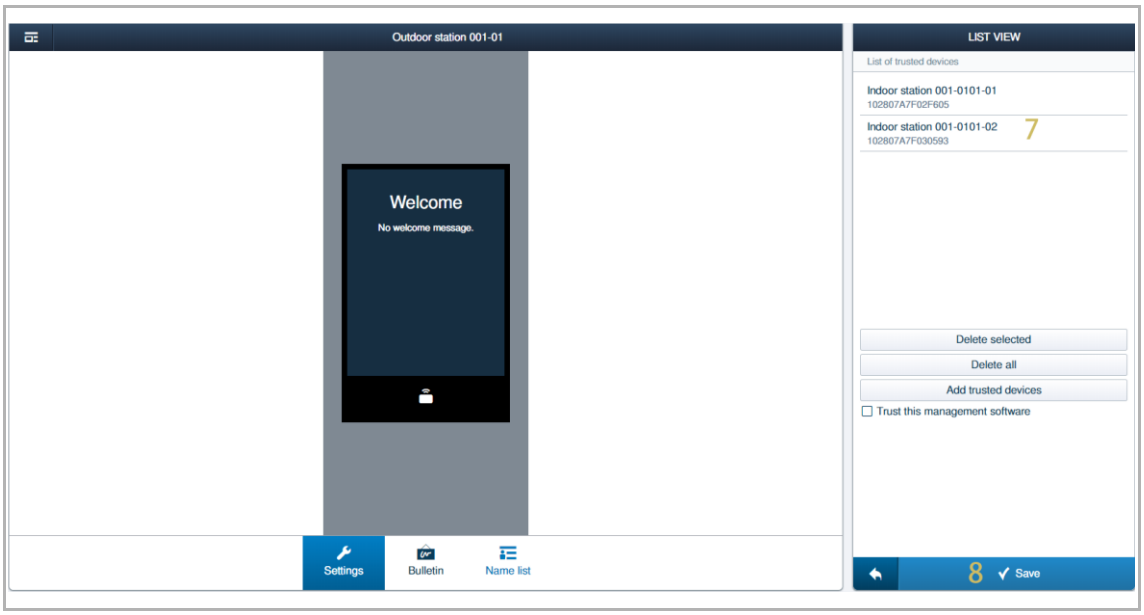
[5] Vink de keuzevakjes aan om de vertrouwde apparaten te selecteren.

[6] Klik op "√" om te bevestigen.



[7] Het resultaat wordt weergegeven op het scherm.

[8] Klik op "Opslaan" om op te slaan.



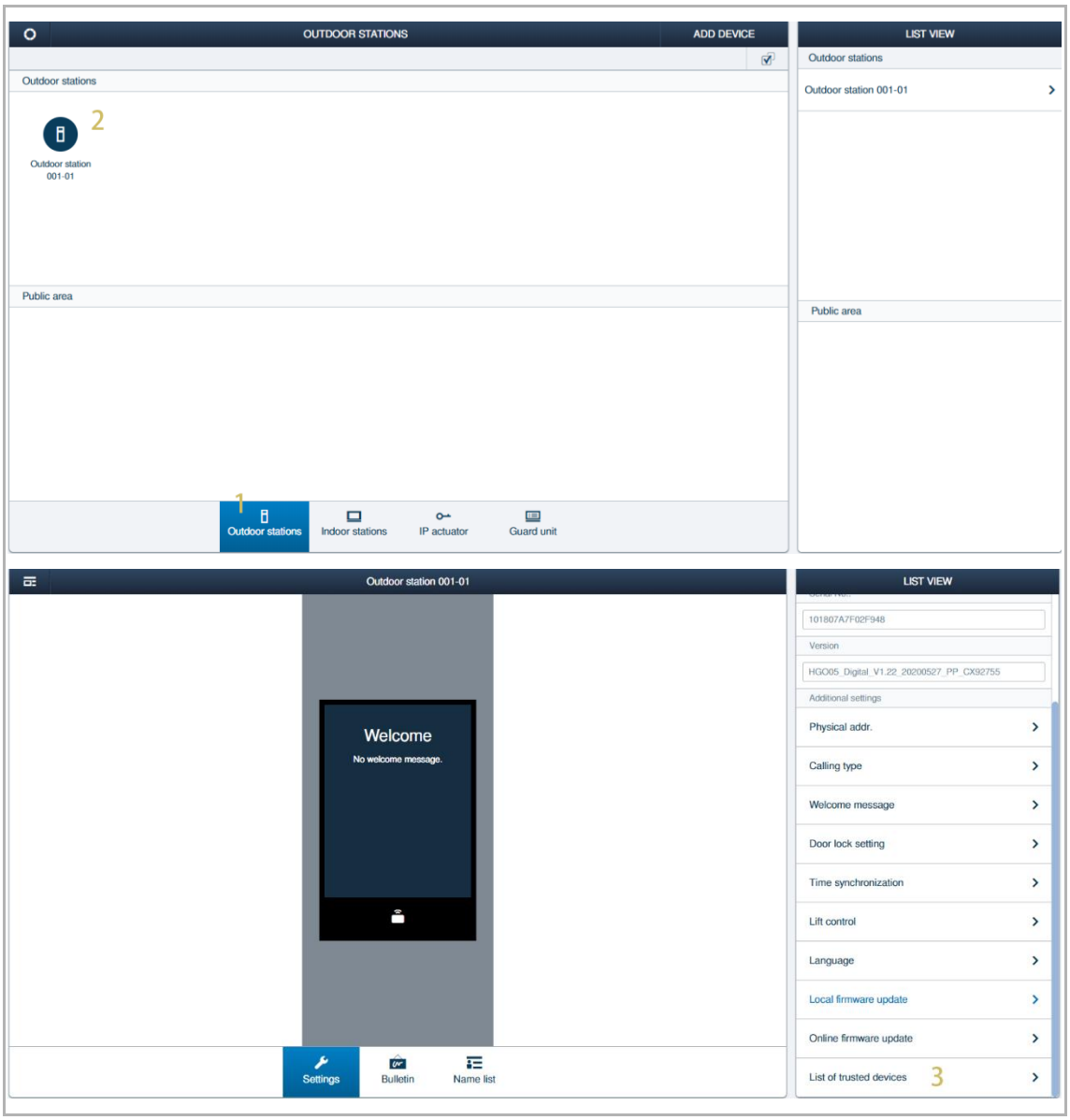
2. Vertrouwde apparaten verwijderen

Volg de onderstaande stappen:

[1] Klik in het scherm "Buiten-/binnenpost" op "Buitenposten".

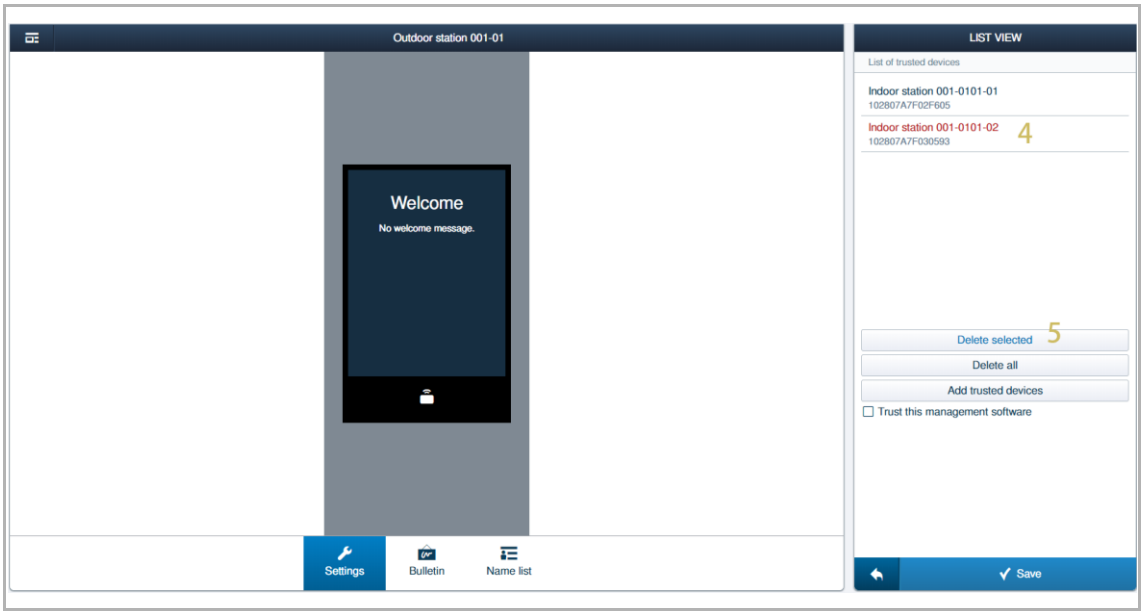
[2] Klik op de gewenste buitenpost.

[3] Scrol naar beneden in de lijst en klik op "Lijst met vertrouwde apparaten".



[4] Klik op de apparaten om deze een voor een te selecteren (de geselecteerde apparaten worden in het rood gemarkeerd).

[5] Klik op "Selectie wissen".



9.3.2 Vertrouwde apparaten voor de IP-aktor beheren

Als u het slot van de IP-aktor wilt ontgrendelen, moet u het volgende controleren:

- Als de binnenpost en de IP-aktor op het "Smart Access Point" zijn gesigneerd.
- Als de binnenpost toegevoegd is aan de lijst met vertrouwde apparaten op de IP-aktor.

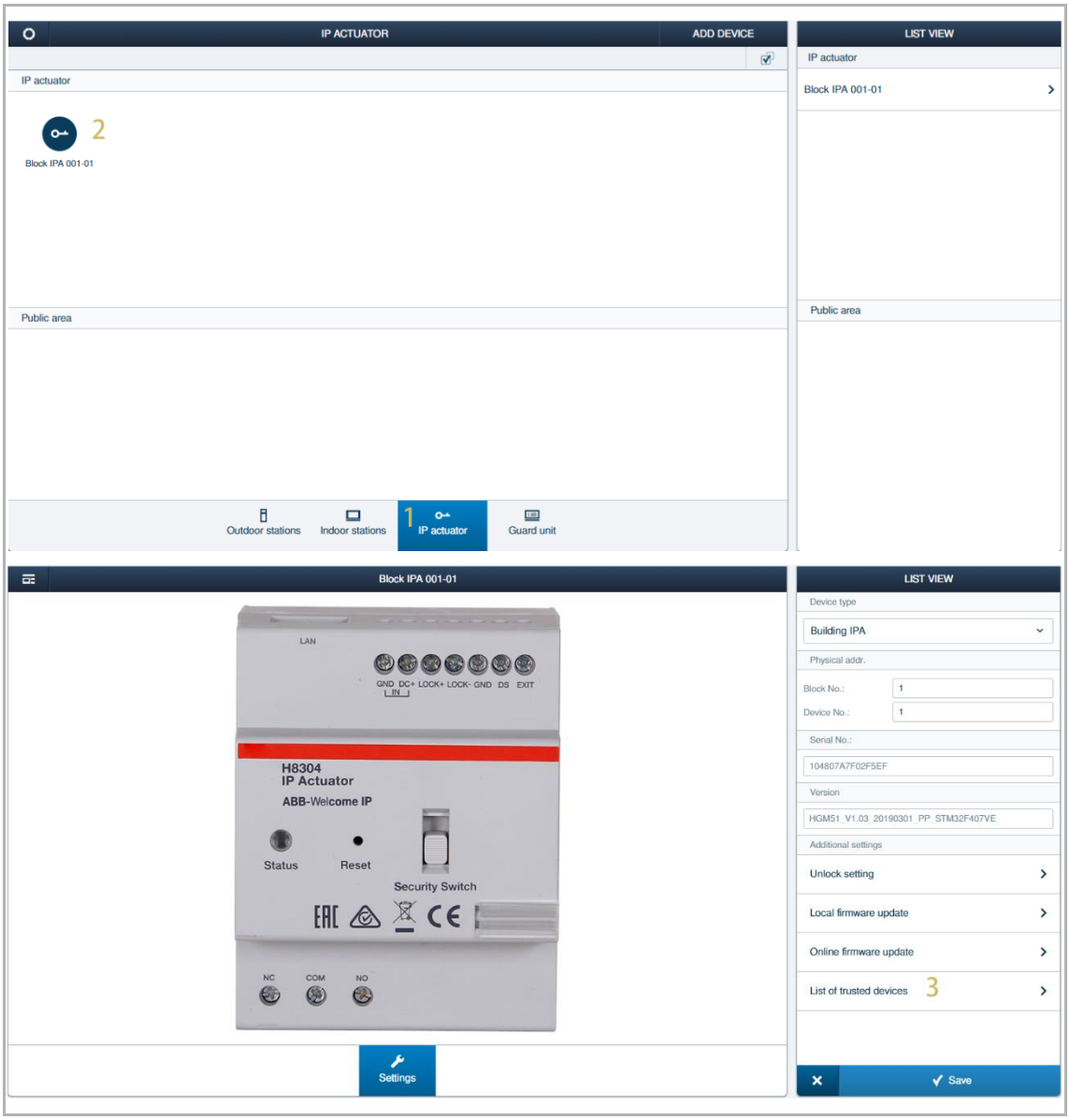
1. Vertrouwde apparaten toevoegen

Volg de onderstaande stappen:

[1] Klik in het scherm "Buiten-/binnenpost" op "IP-aktor".

[2] Klik op de betreffende IP-aktor.

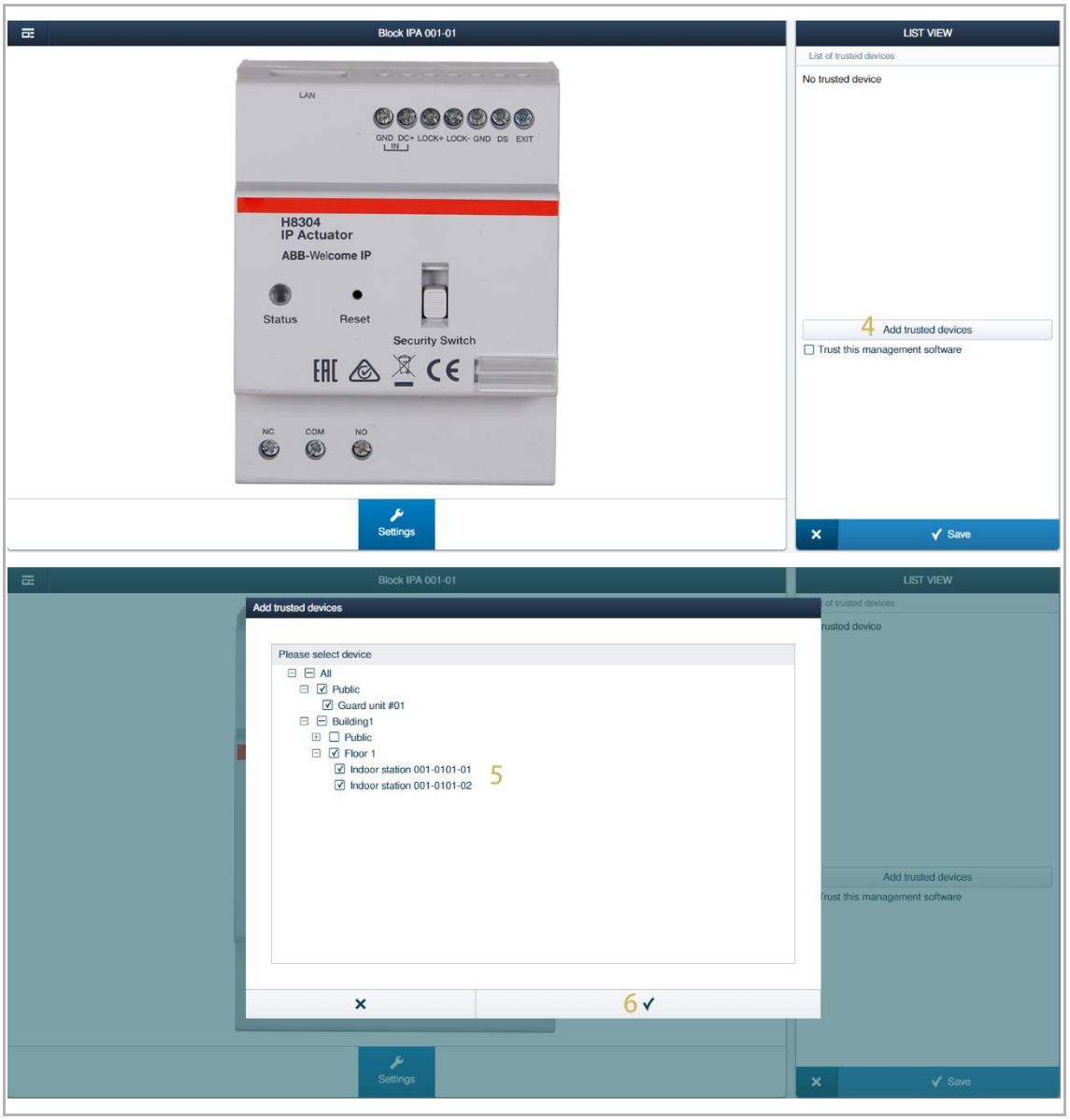
[3] Klik op de "Lijst met vertrouwde apparaten".



[4] Klik op "Vertr. app.toevoegen".

[5] Vink de keuzevakjes aan om de vertrouwde apparaten te selecteren.

[6] Klik op "√" om te bevestigen.



[7] Het resultaat wordt weergegeven op het scherm.

[8] Klik op "Opslaan" om op te slaan.

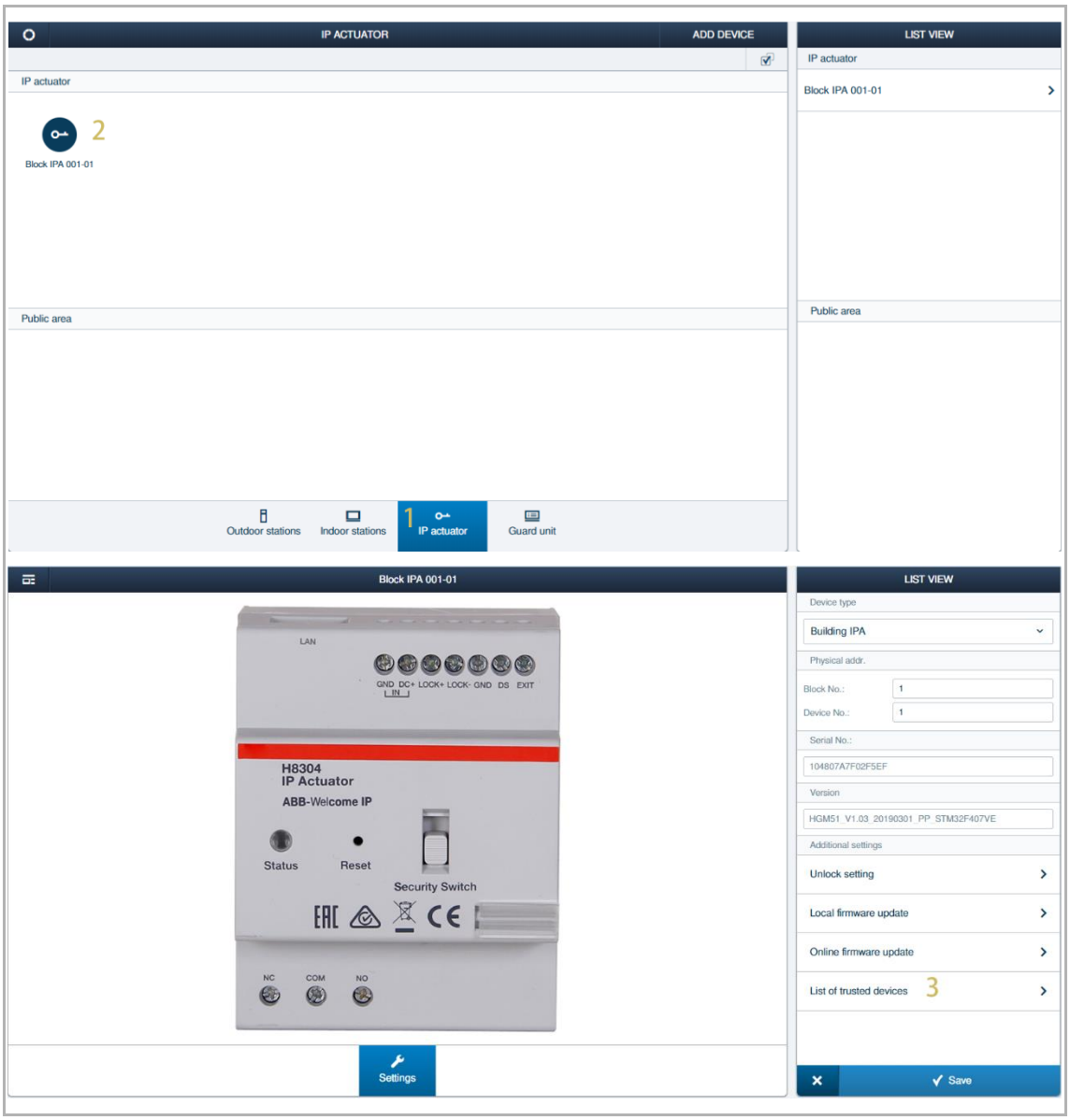
2. Vertrouwde apparaten verwijderen

Volg de onderstaande stappen:

[1] Klik in het scherm "Buiten-/binnenpost" op "IP-aktor".

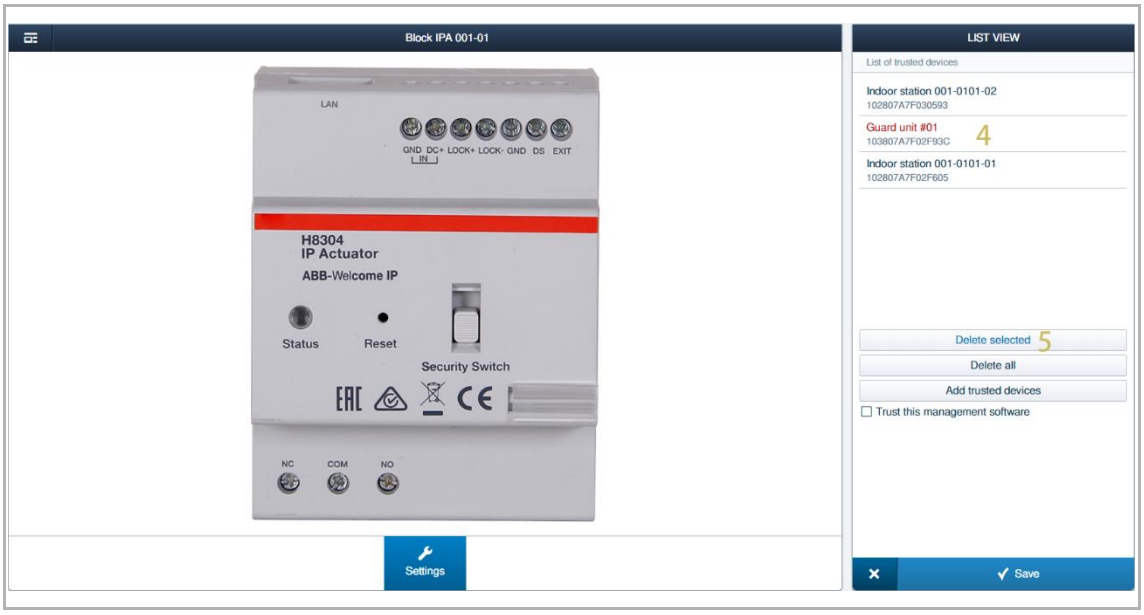
[2] Klik op de betreffende IP-aktor.

[3] Klik op de "Lijst met vertrouwde apparaten".



[4] Klik op de apparaten om deze een voor een te selecteren (de geselecteerde apparaten worden in het rood gemarkeerd).

[5] Klik op "Selectie wissen".



9.3.3 Vertrouwde apparaten voor "Smart Access Point" beheren

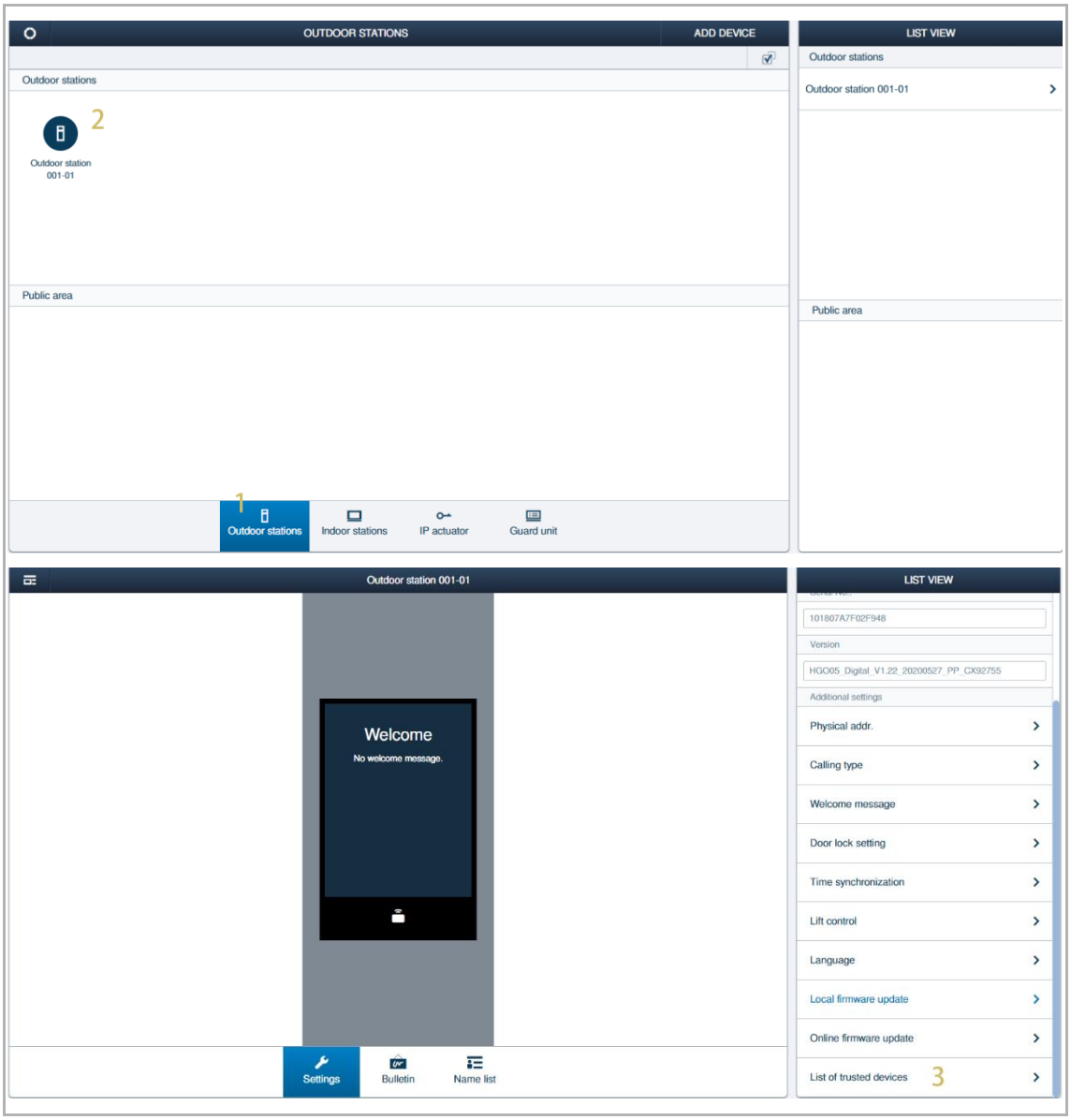
1. Buitenposten toevoegen aan vertrouwde apparaten

Volg de onderstaande stappen:

[1] Klik in het scherm "Buiten-/binnenpost" op "Buitenposten".

[2] Klik op de gewenste buitenpost.

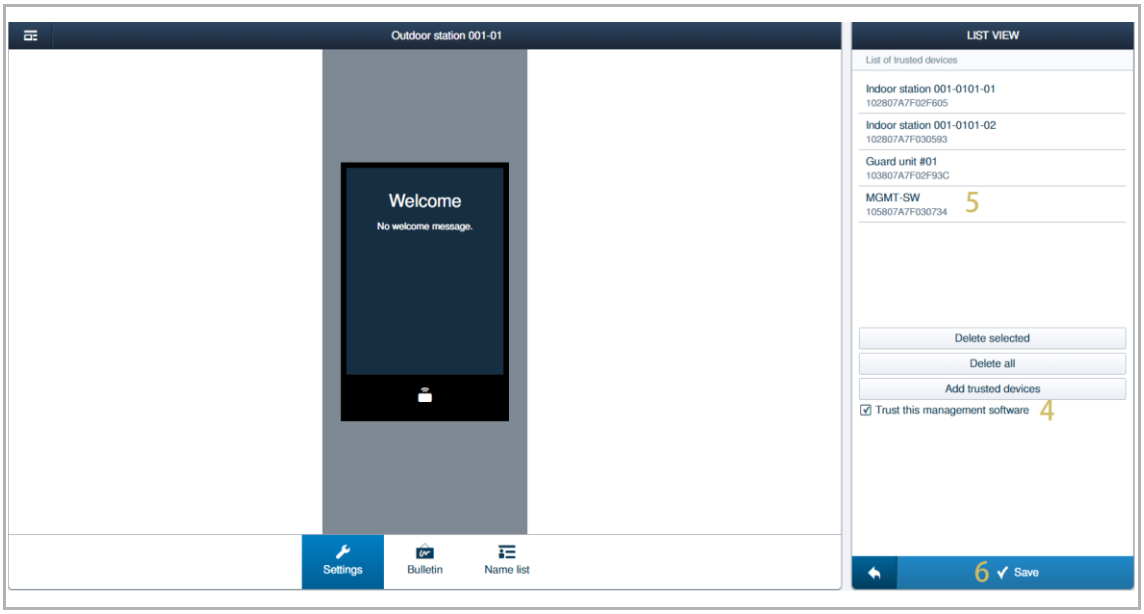
[3] Scrol naar beneden in de lijst en klik op "Lijst met vertrouwde apparaten".



[4] Klik op "Vertrouw deze managementsoftware".

[5] Het resultaat wordt weergegeven in de lijst.

[6] Klik op "√" om op te slaan.



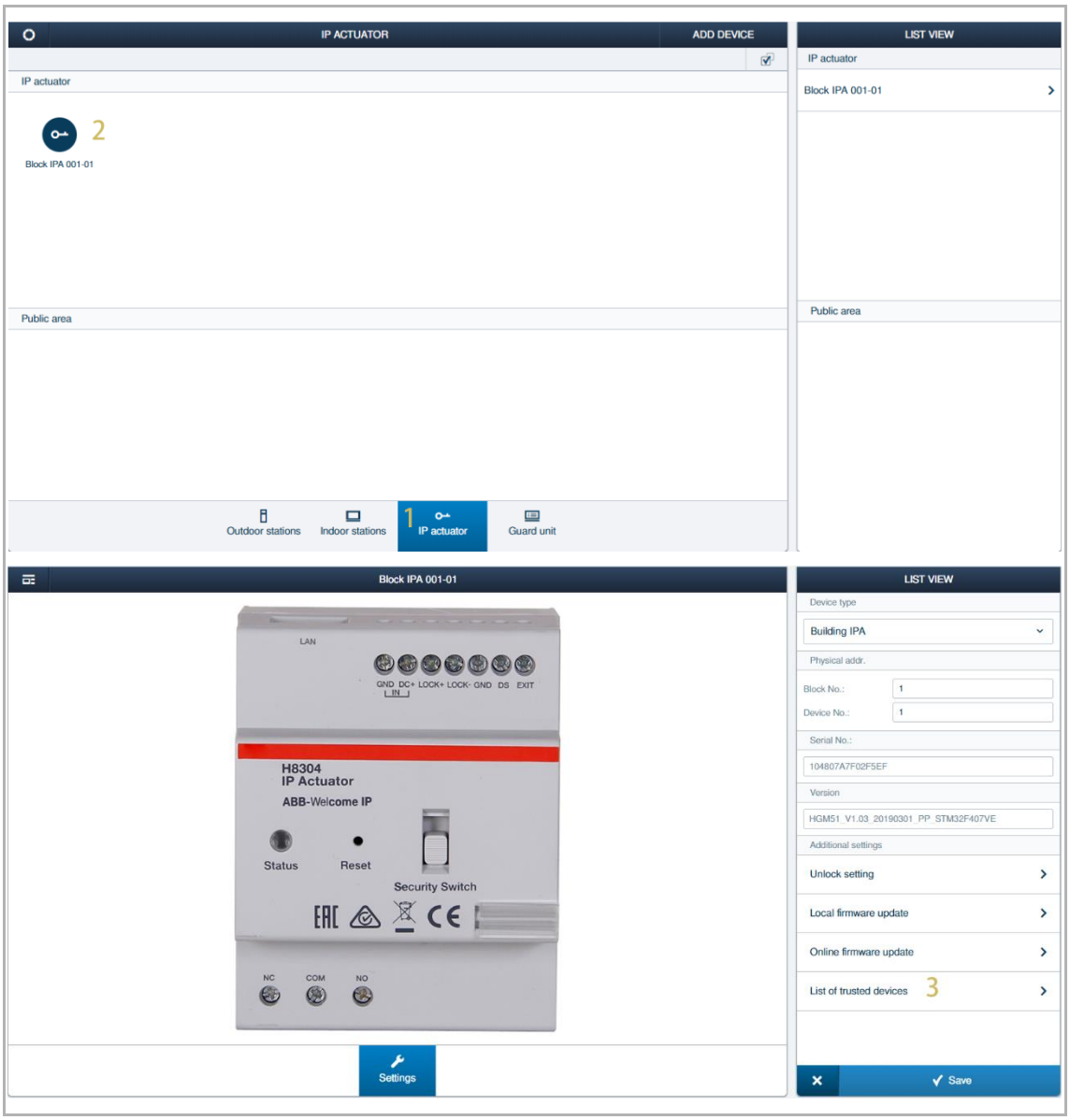
2. IP-aktoren toevoegen aan vertrouwde apparaten

Volg de onderstaande stappen:

[1] Klik in het scherm "Buiten-/binnenpost" op "IP-aktor".

[2] Klik op de betreffende IP-aktor.

[3] Klik op de "Lijst met vertrouwde apparaten".



[4] Klik op "Vertrouw deze managementsoftware".

[5] Het resultaat wordt weergegeven in de lijst.

[6] Klik op "√" om op te slaan.

9.3.4 Nooddeblokkering

In sommige noodsituaties kan het nodig zijn om alle publieke deuren te ontgrendelen. Om dit te bereiken, moet u alle buitenposten en alle openbare IP-aktoren toevoegen aan "Smart Access Point".

zie hoofdstuk 9.3.3 “Vertrouwde apparaten voor "Smart Access Point" beheren“ op pagina 74.

Alle openbare deuren ontgrendelen

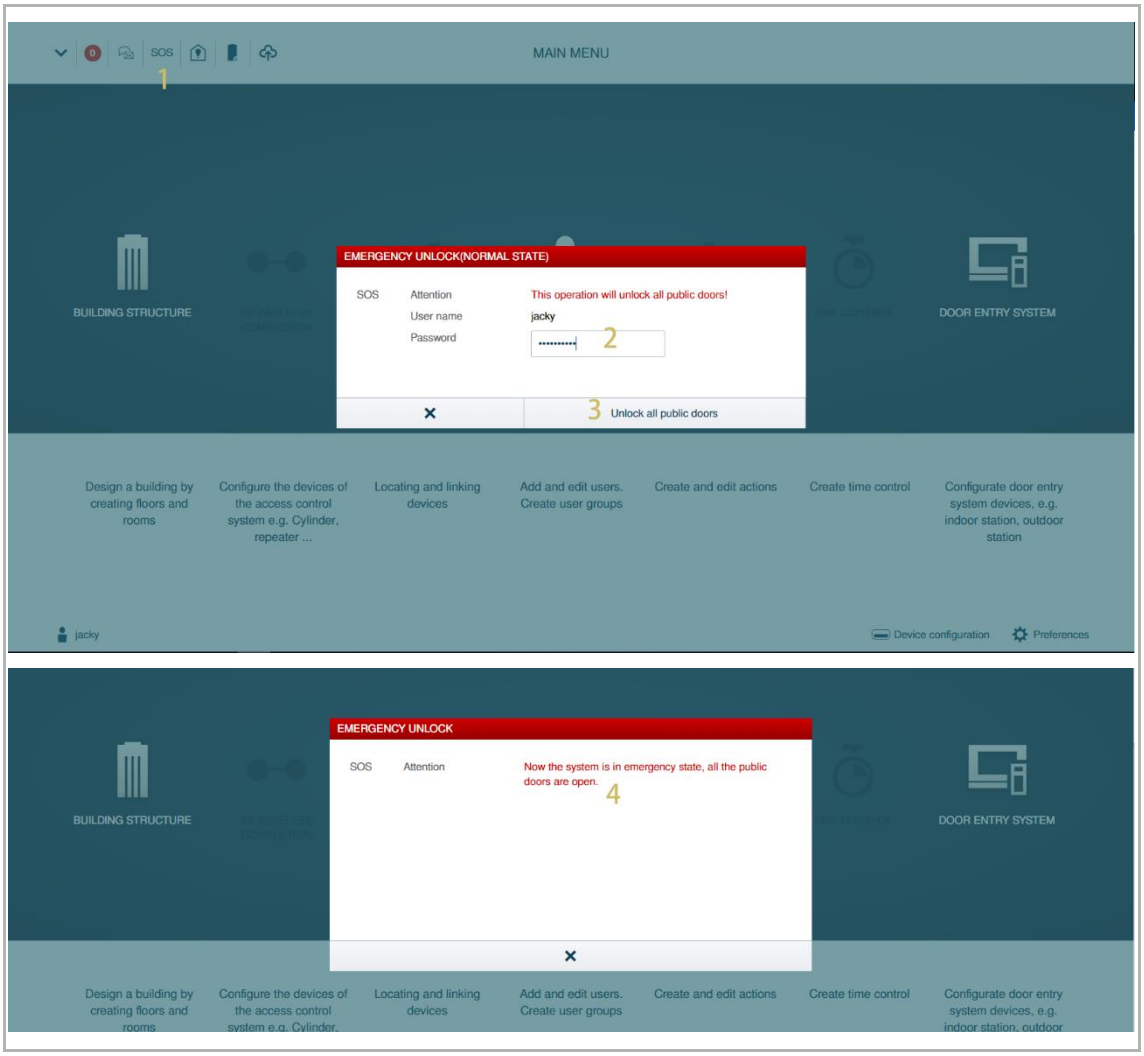
Volg de onderstaande stappen:

[1] Klik in het configuratiescherm op "SOS".

[2] Voor het wachtwoord in van de huidige admin-gebruiker.

[3] Klik op "Alle openbare deuren deblokkeren".

[4] De resultaatstatus wordt weergegeven op het scherm.



Alle openbare deuren sluiten

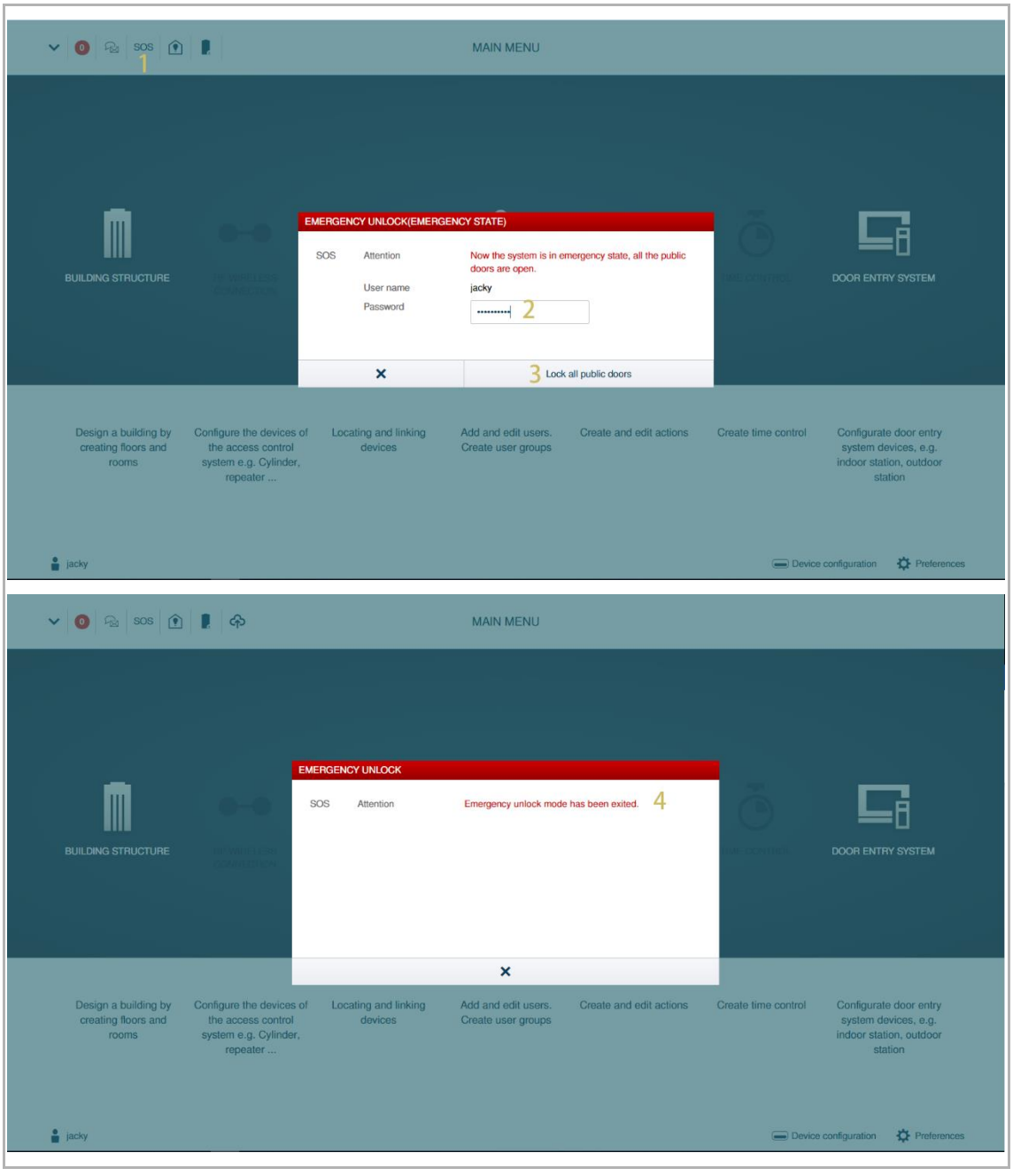
Volg de onderstaande stappen:

[1] Klik in het configuratiescherm op "SOS".

[2] Voor het wachtwoord in van de huidige admin-gebruiker.

[3] Klik op "Alle openbare deuren blokkeren".

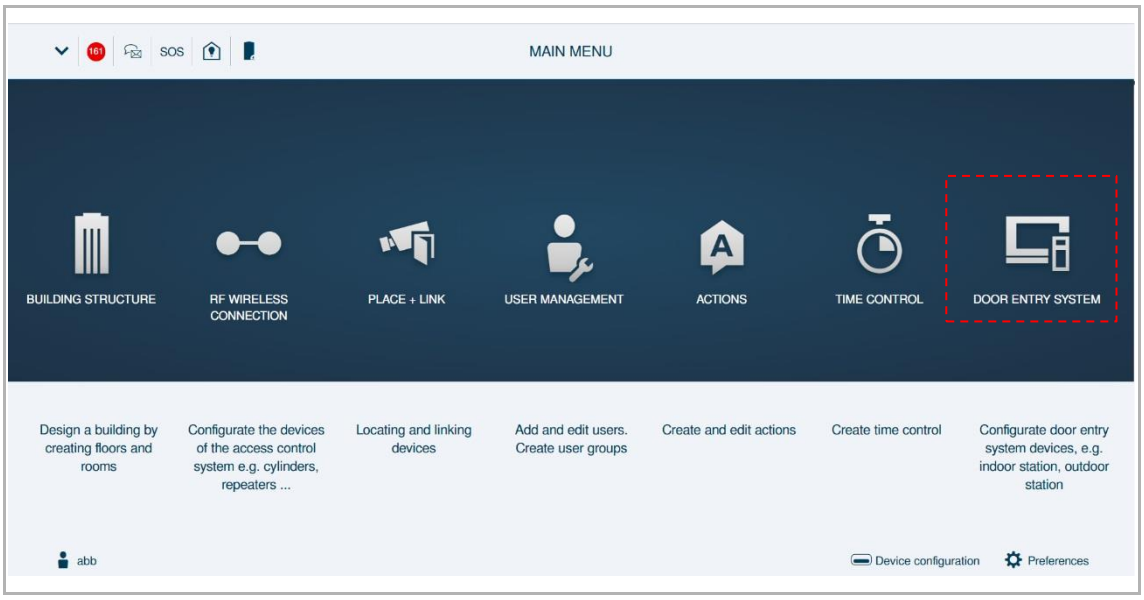
[4] De resultaatstatus wordt weergegeven op het scherm.



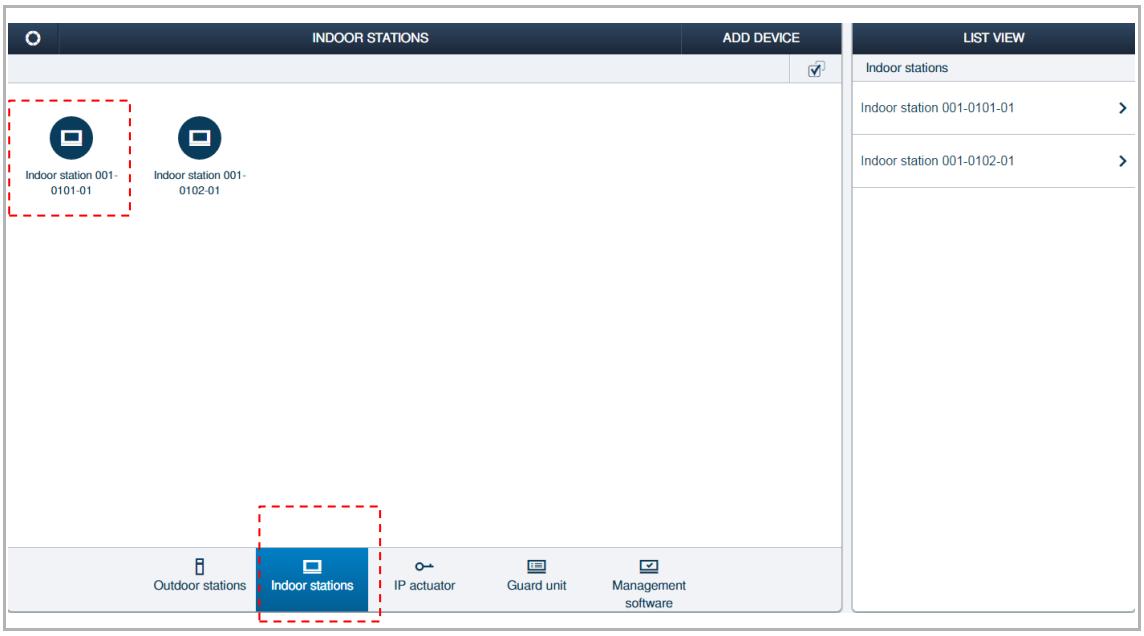
9.4 Binnenpost configureren

Scherm van binnenpost oproepen

Klik op het configuratiescherm op "Binnenpost", vervolgens op "Binnenposten" om het scherm "Binnenposten" te openen.



Klik op het scherm "Binnenposten" op de betreffende binnenpost om het scherm van de binnenpost te openen.



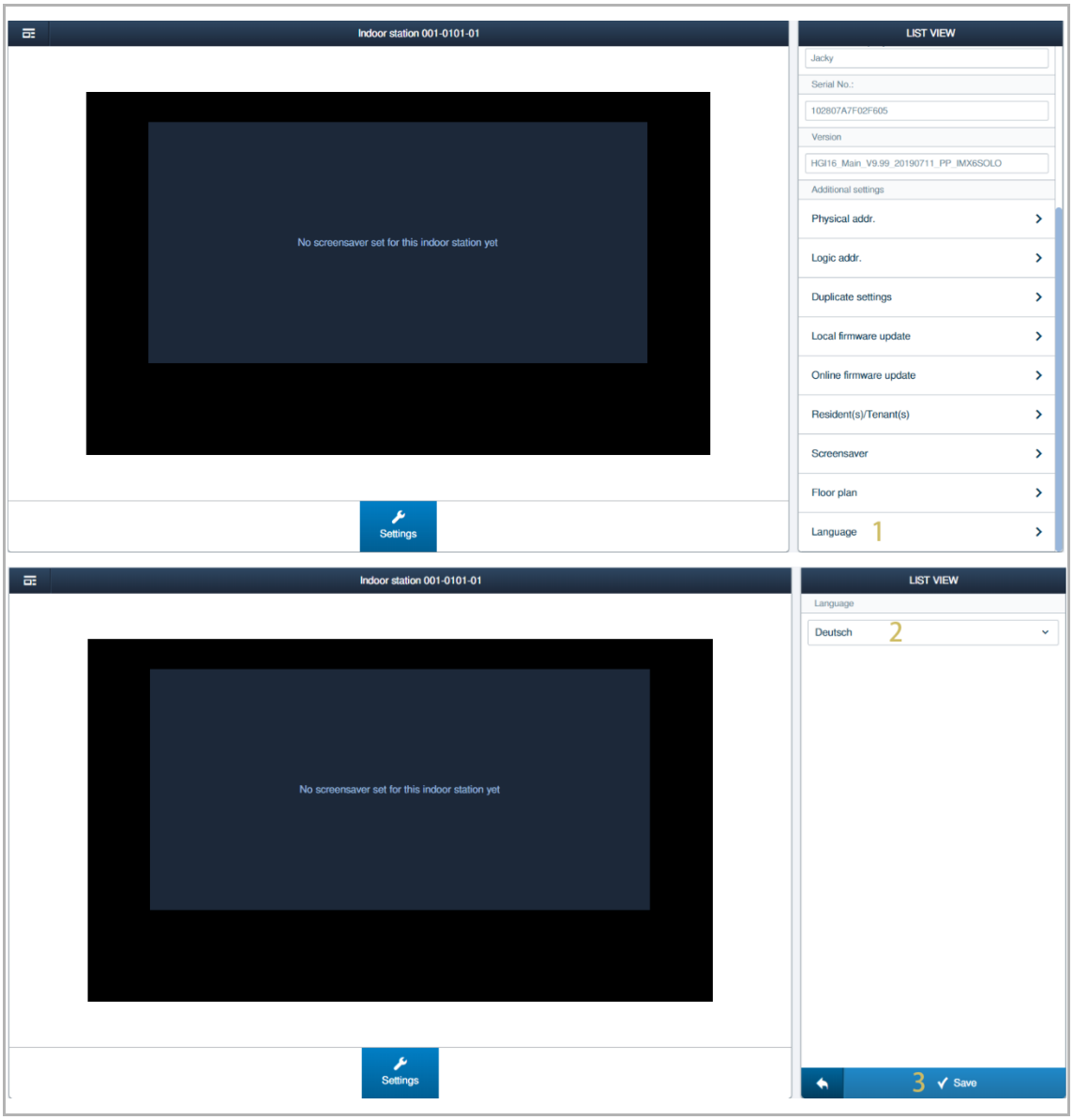
9.4.1 Taal wijzigen

Volg de onderstaande stappen:

[1] Op het scherm van de binnenpost klikt u op "Taal".

[2] Selecteer de taal uit de keuzelijst.

[3] Klik op "√" om op te slaan.



9.4.2 Apparaat een andere naam geven

Volg de onderstaande stappen:

[1] Op het scherm van de binnenpost klikt u op "Bewoner(s)/huurder(s)".

[2] Voer de voornaam in.

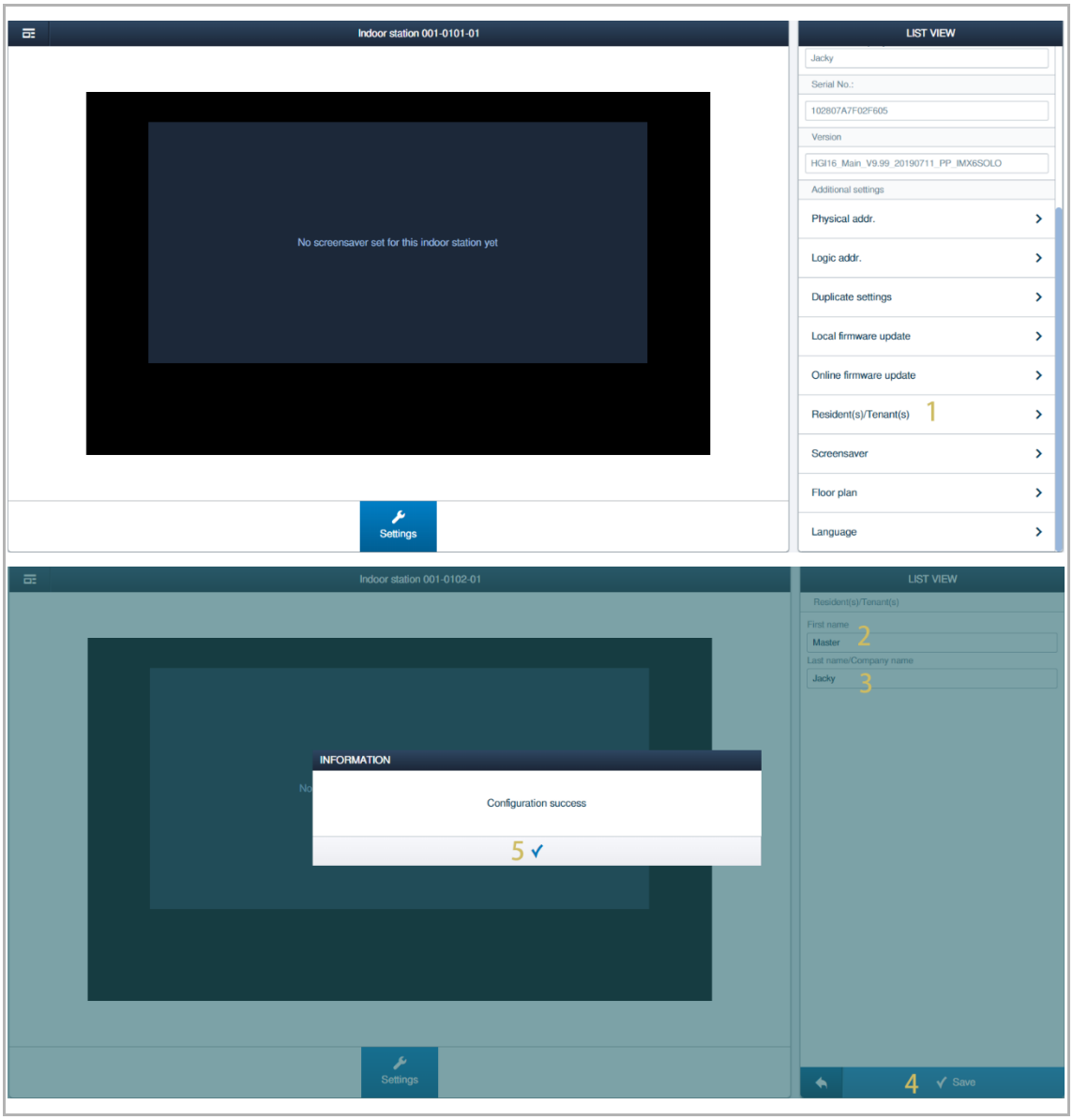
[3] Voer de achternaam of de bedrijfsnaam in.

Opmerking

Als de bewoner meerdere binnenposten in het appartement heeft, wordt aanbevolen om de overeenkomstige naam te gebruiken om het verband duidelijk te maken (bijv. "Master", "Slave 1" enz.).

[4] Klik op "√" om op te slaan.

[5] Klik op "√" om door te gaan.

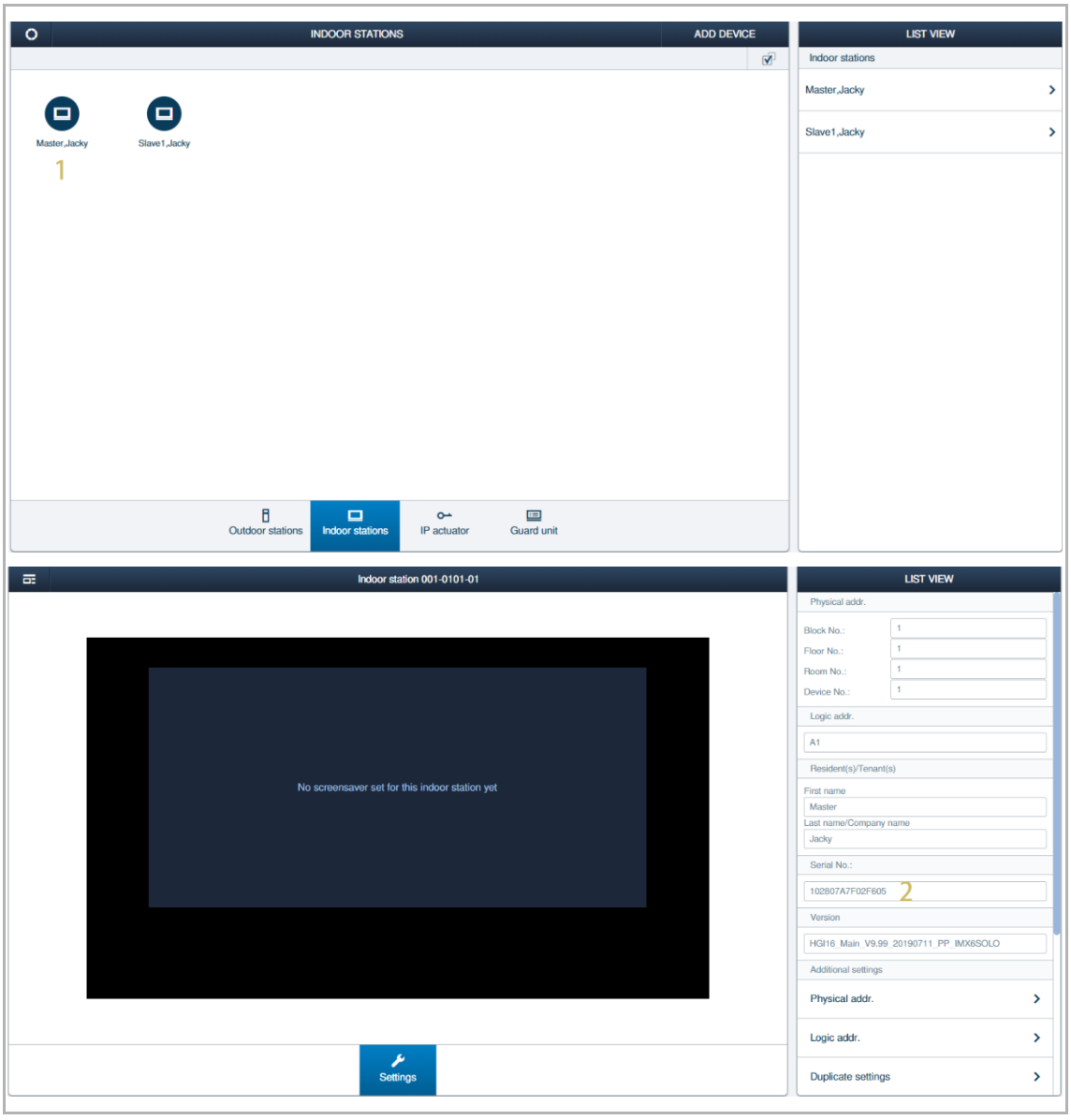


9.4.3 Serienummer bekijken

Volg de onderstaande stappen:

[1] Klik op het scherm "Binnenposten" op de betreffende binnenpost.

[2] Het serienummer wordt weergegeven op het scherm. Het wordt aanbevolen om het serienummer te noteren voor verder gebruik.



9.4.4 Fysiek adres beheren

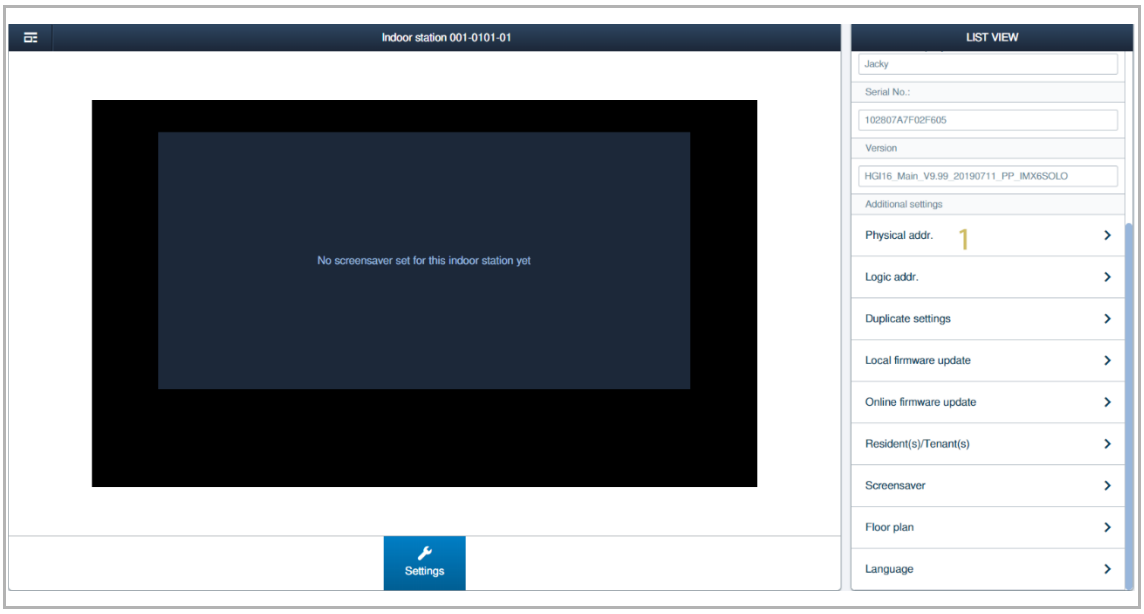
Opmerking

Als de master-binnenpost het fysieke adres wijzigt, moeten de slave-binnenposten opnieuw de handtekening van het "Smart Access Point" krijgen.

Noteer het serienummer van de slave-binnenposten voordat u het fysieke adres wijzigt. zie hoofdstuk 9.4.3 “Serienummer bekijken“ op pagina 83.

Volg de onderstaande stappen:

[1] Klik op het scherm van de master-binnenpost op "Fysiek adres".



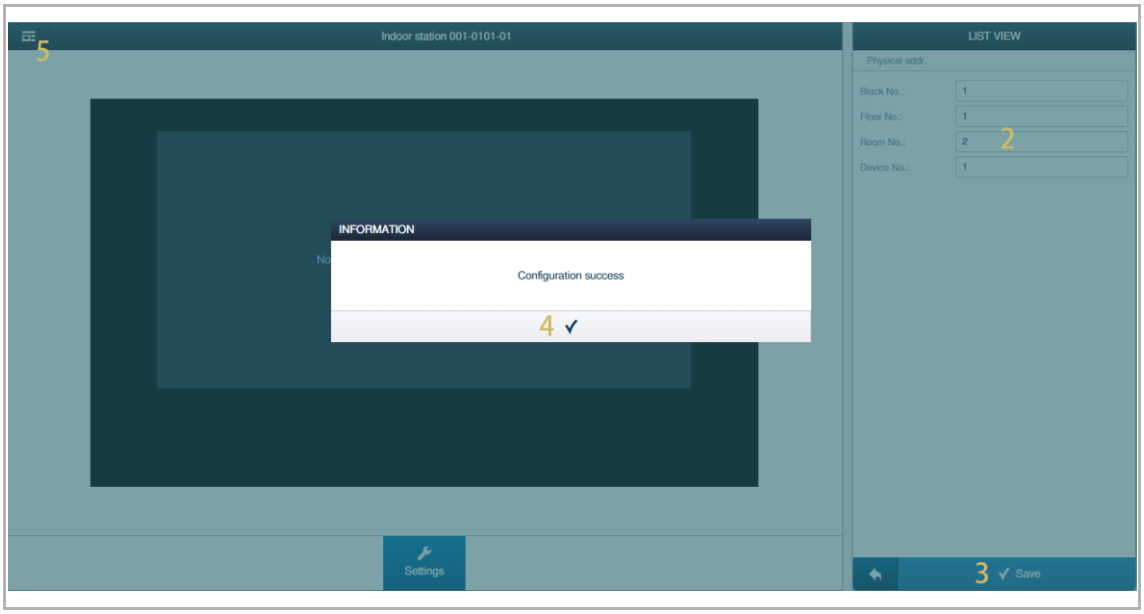
[2] Wijzig het fysieke adres.

[3] Klik op "√" om op te slaan.

[4] Klik op "√" om te bevestigen.

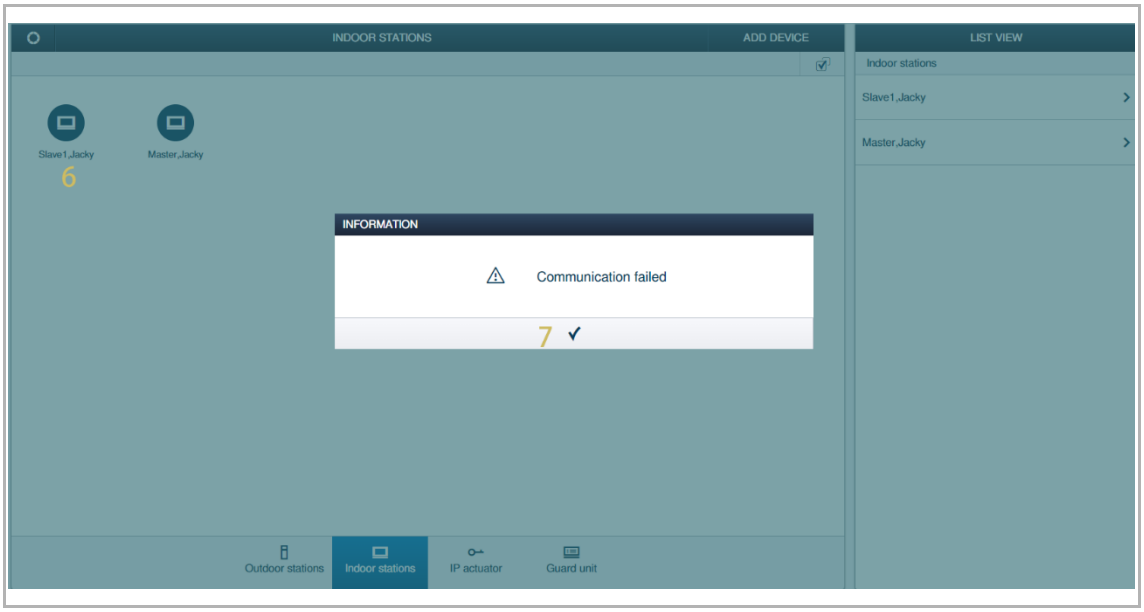
Als er geen slave-binnenposten zijn, is het veranderingsproces bij stap 4 voltooid. Anders kunt u doorgaan met de volgende stappen.

[5] Klik op " " om terug te gaan naar het scherm "Binnenposten".

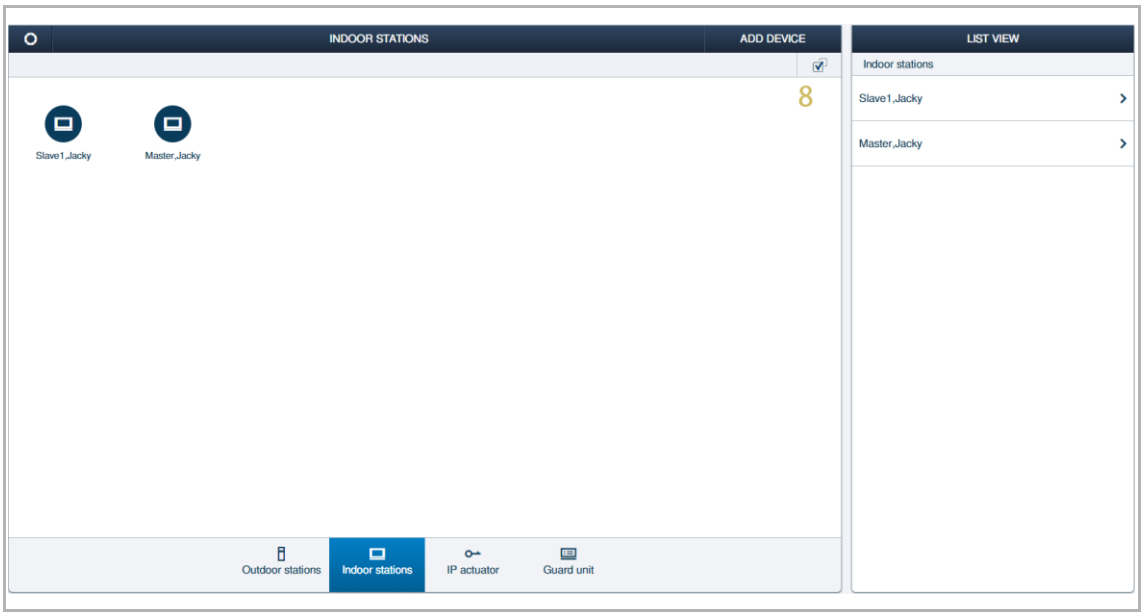


[6] Klik op de slave-binnenpost.

[7] Het slave-binnenpost kreeg geen toegang tot het scherm omdat de handtekening automatisch werd verwijderd. Klik op "√" om door te gaan.



[8] Klik op " " op het scherm "Binnenposten".



[9] Klik op de slave-binnenpost.

[10]Klik op "Wissen".

[11]Klik op "Bevestigen" en vervolgens op "√".

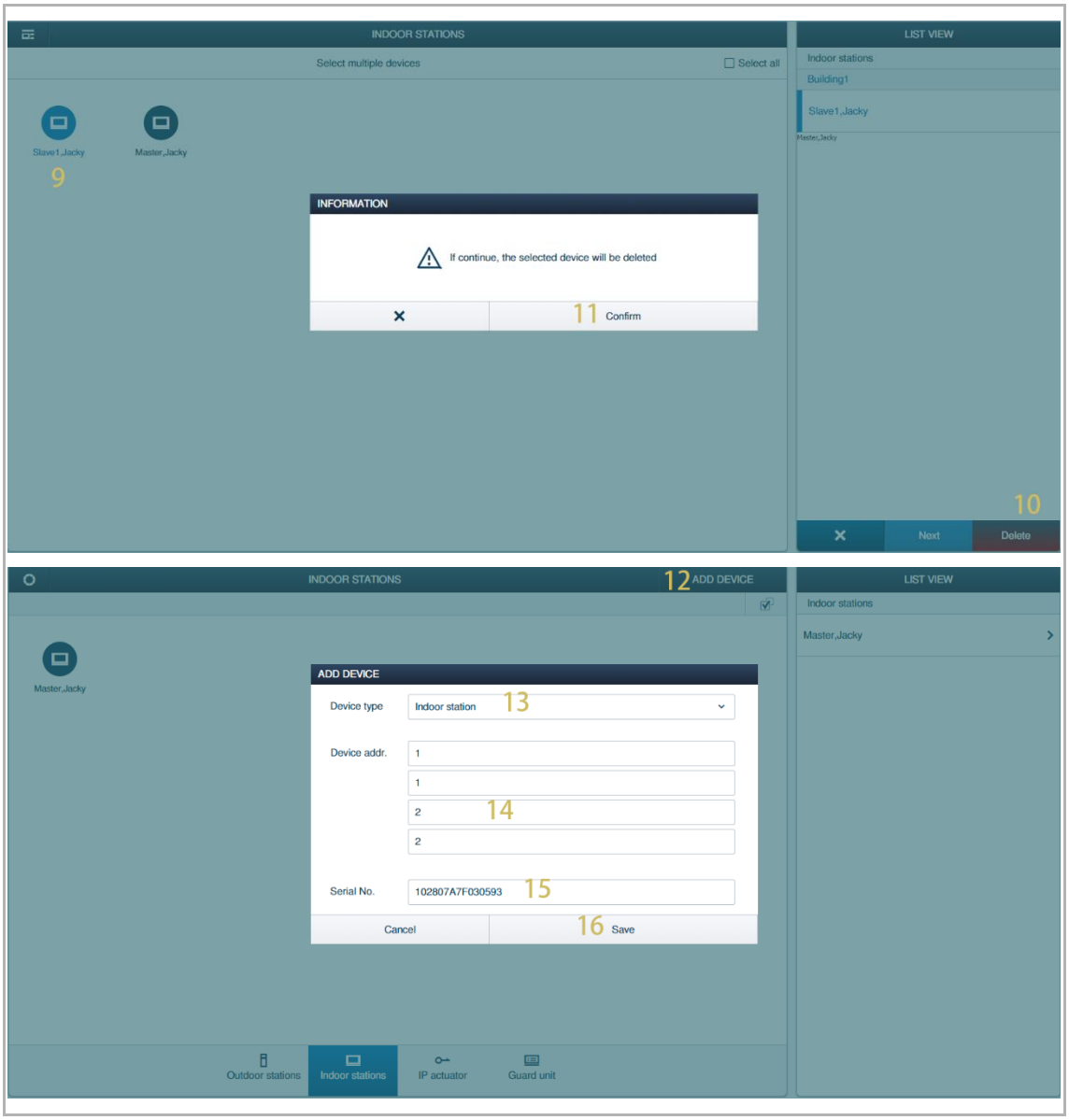
[12]Klik op "App. toevoegen" op het scherm "Binnenposten".

[13]Stel het "Apparaattype" in op "Binnenpost".

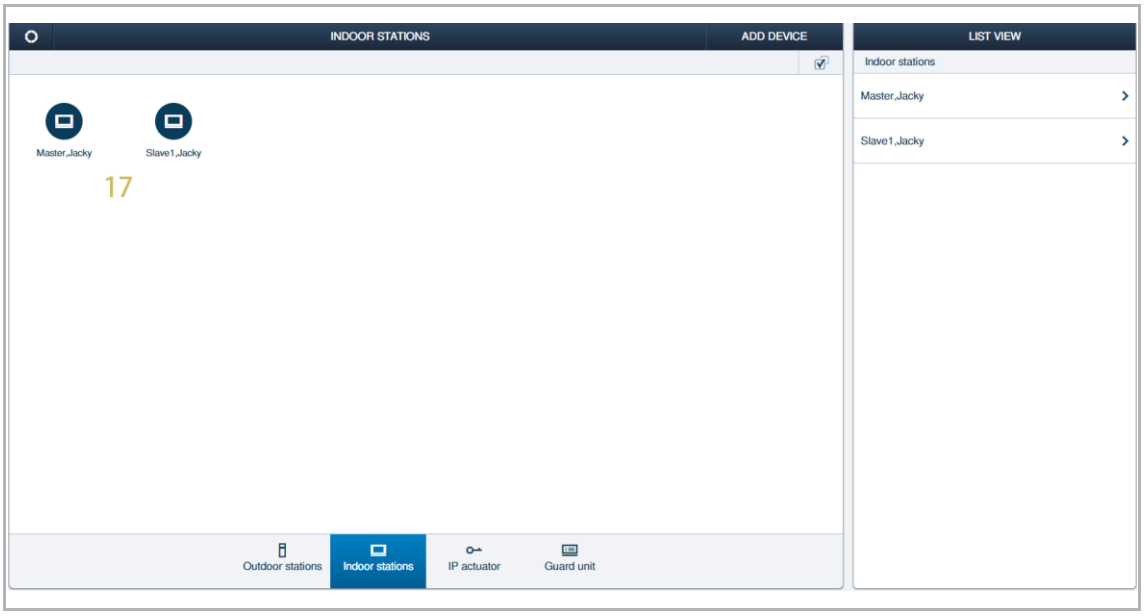
[14]Voor het nieuwe fysieke adres in van de slave-binnenpost.

[15]Voer het serienummer in van de slave-binnenpost.

[16]Klik op "Opslaan" en vervolgens op "√".



[17]Geef de slave-binnenpost een andere naam. zie hoofdstuk 9.4.2 “Apparaat een andere naam geven“ op pagina 82.



9.4.5 Logisch adres beheren

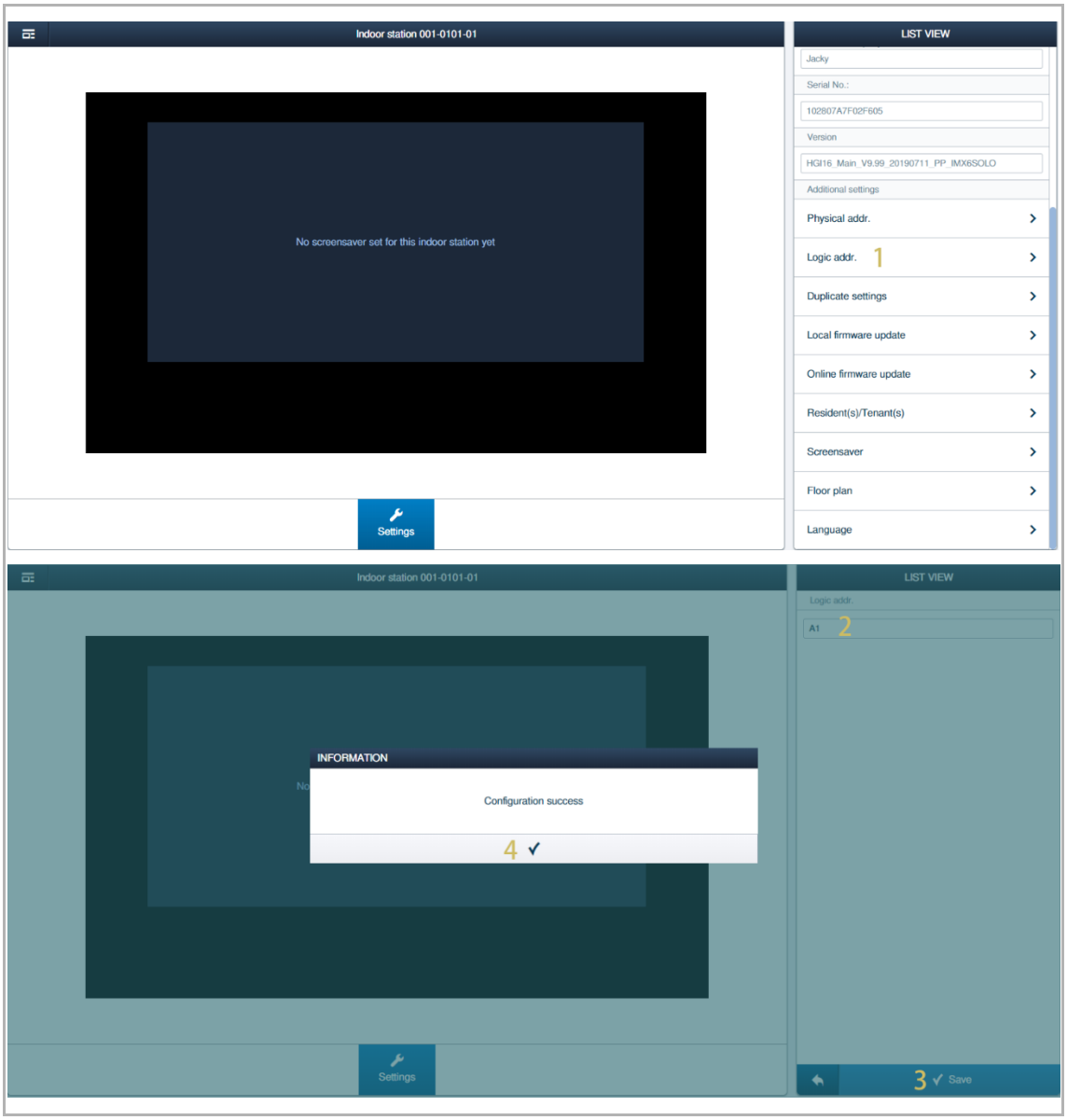
Volg de onderstaande stappen:

[1] Klik op het scherm van de master-binnenpost op "Logisch adr.".

[2] Voer het logische adres in. Het adres kan niet hetzelfde zijn als het bestaande adres op het "Smart Access Point".

[3] Klik op "√" om op te slaan.

[4] Klik op "√" om te bevestigen.



Opmerking

Het op de binnenpost ingestelde logische adres kan op de buitenpost worden gebruikt. zie hoofdstuk 9.4.5 “Logisch adres beheren“ op pagina 89.

9.4.6 Screensaver beheren

Volg de onderstaande stappen:

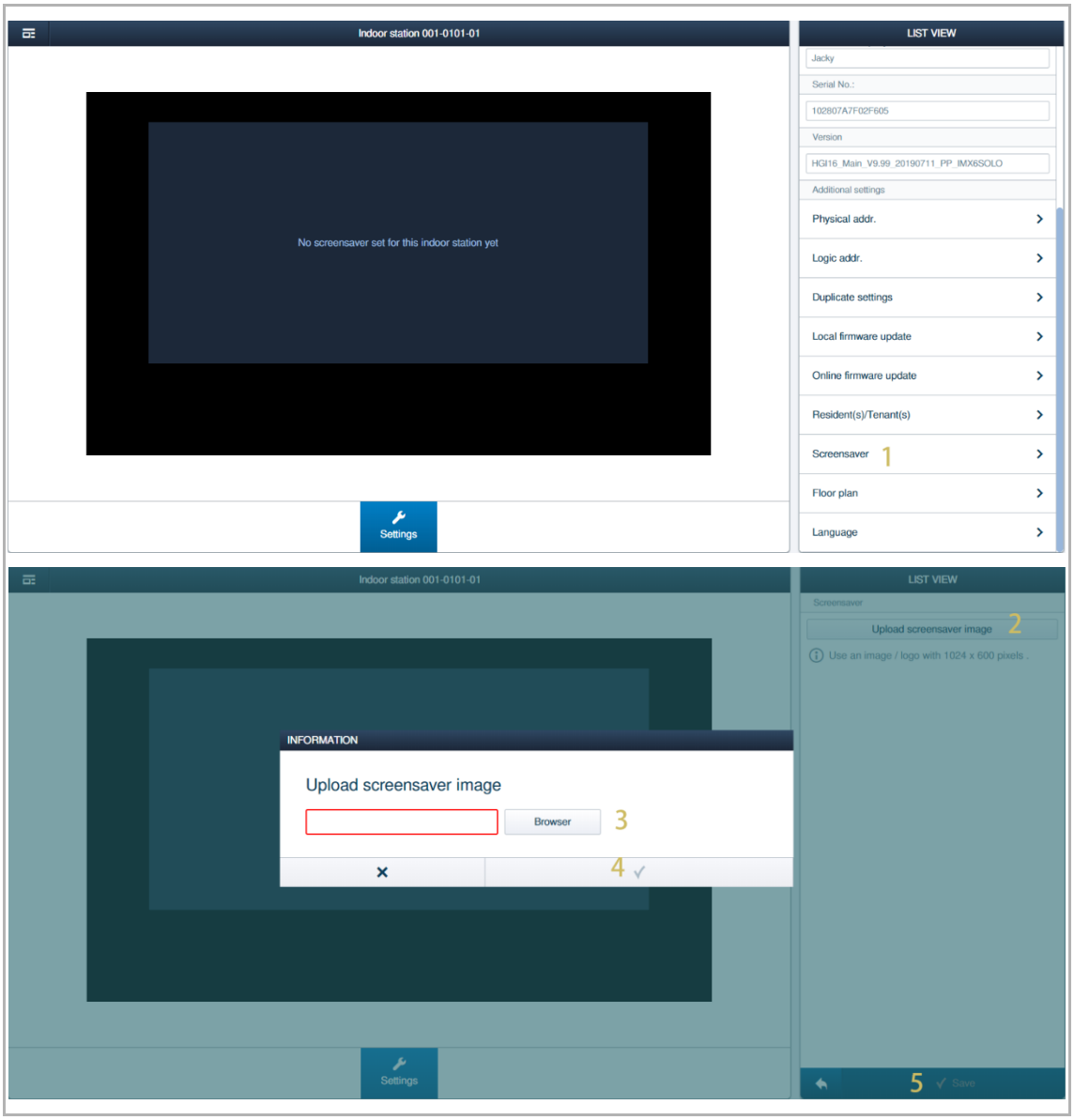
[1] Klik op het scherm van de master-binnenpost op "Screensaver".

[2] Klik op "Afbeelding screensaver uploaden".

[3] Klik op "Bladeren" om de afbeelding te selecteren (alleen .jpg wordt ondersteund, maximale resolutie van de afbeelding is 1024 x 600 pixels).

[4] Klik op "√" om te bevestigen.

[5] Klik op "√" om te uploaden.



9.4.7 Etageplattegrond beheren

Volg de onderstaande stappen:

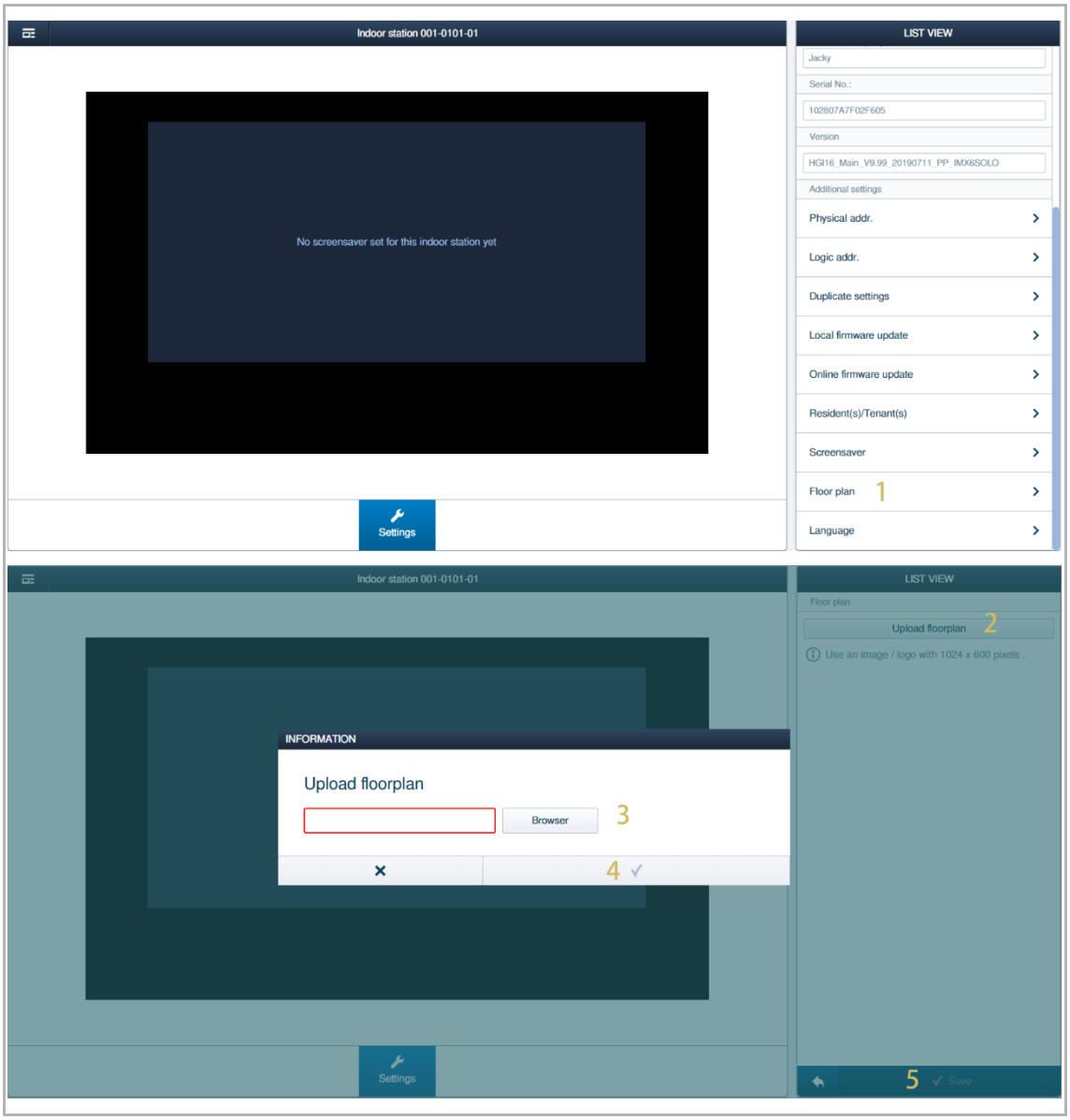
[1] Klik op het scherm van de master-binnenpost op "Plattegrond".

[2] Klik op "Etageschema uploaden".

[3] Klik op "Bladeren" om de afbeelding te selecteren (alleen .jpg wordt ondersteund, maximale resolutie van de afbeelding is 1024 x 600 pixels).

[4] Klik op "√" om te bevestigen.

[5] Klik op "√" om te uploaden.



9.4.8 Instellingen kopiëren

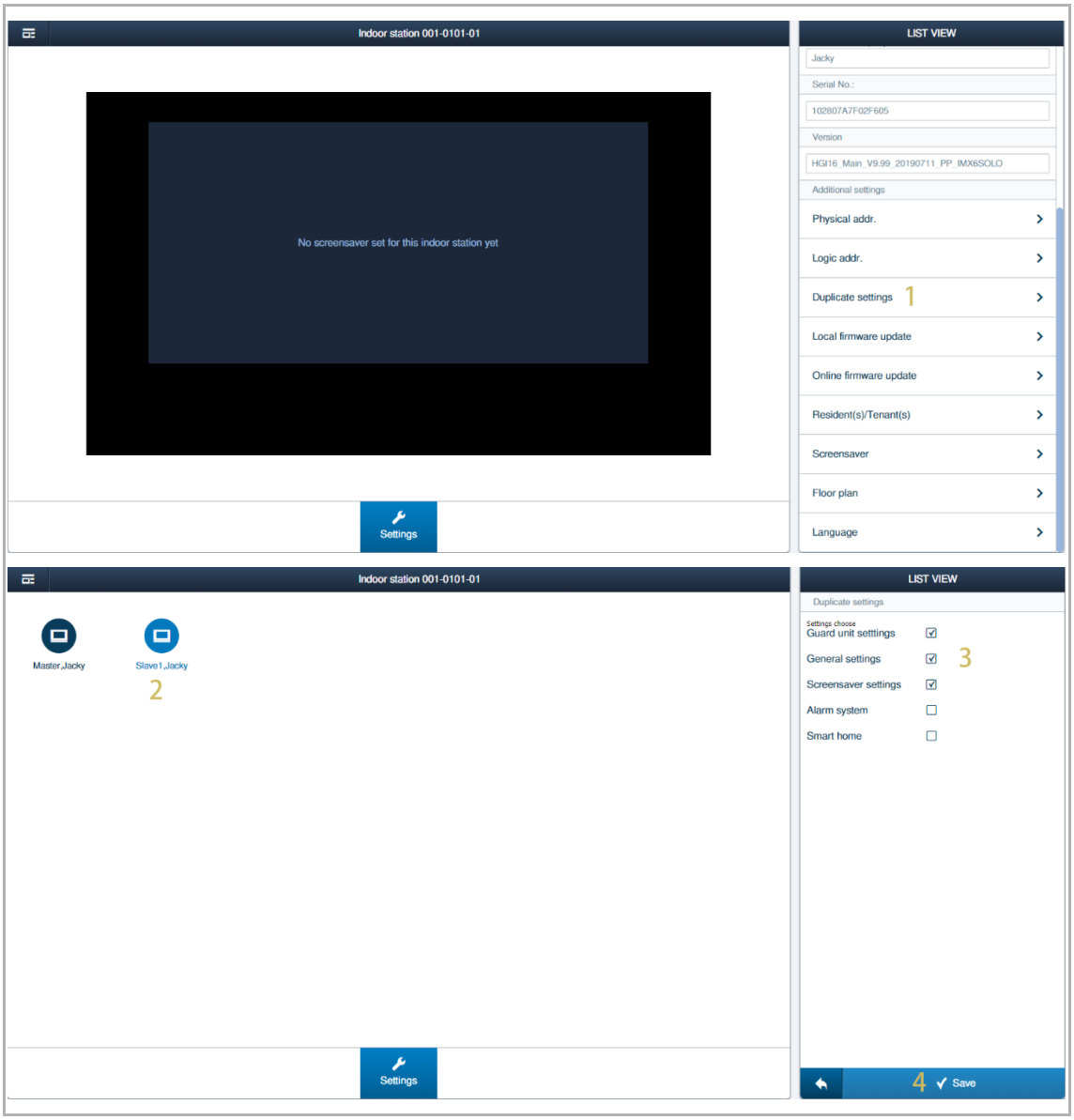
Volg de onderstaande stappen:

[1] Klik op het scherm van de master-binnenpost op "Instellingen kopiëren".

[2] Klik om de gewenste binnenpost te selecteren die moeten worden gekopieerd.

[3] Vink de keuzevakjes aan om de te kopiëren instellingen te selecteren.

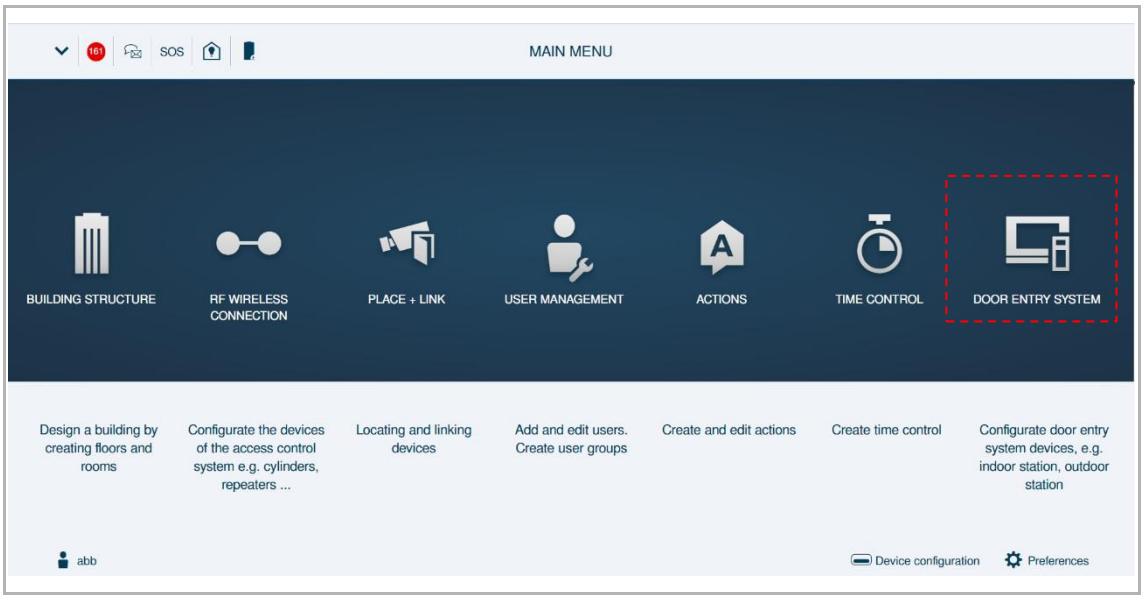
[4] Klik op "√" om te bevestigen.



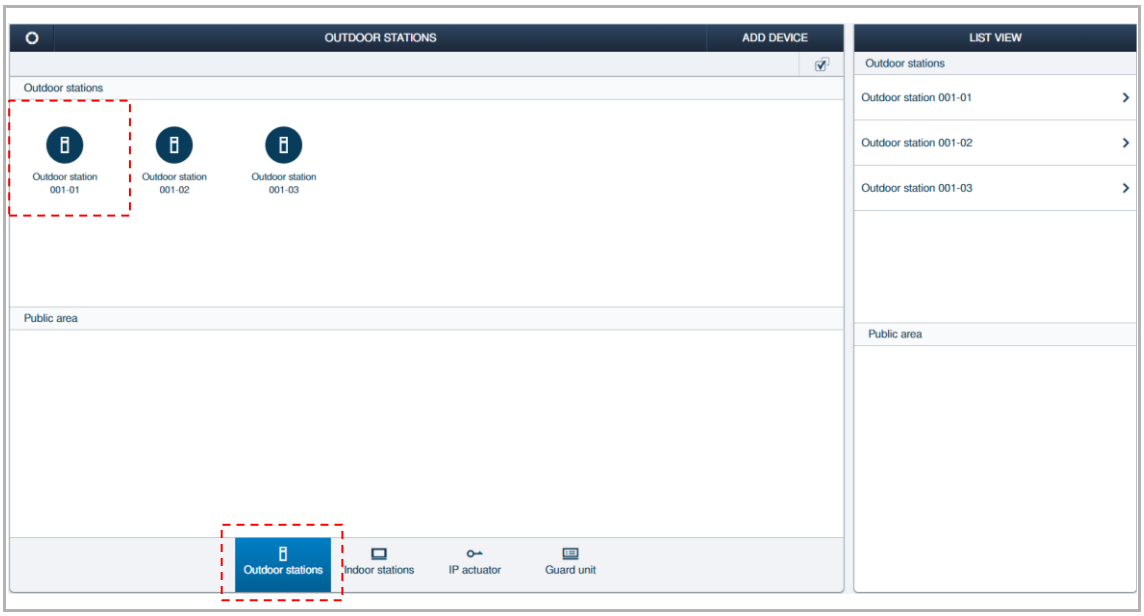
9.5 Buitenpost configureren

Scherm van buitenpost oproepen

Klik op het configuratiescherm op "Buiten-/binnenpost", vervolgens op "Buitenposten" om het scherm "Buitenposten" te openen.



Klik in het scherm "Buitenposten" en op de betreffende buitenpost om het bijbehorende scherm te openen.



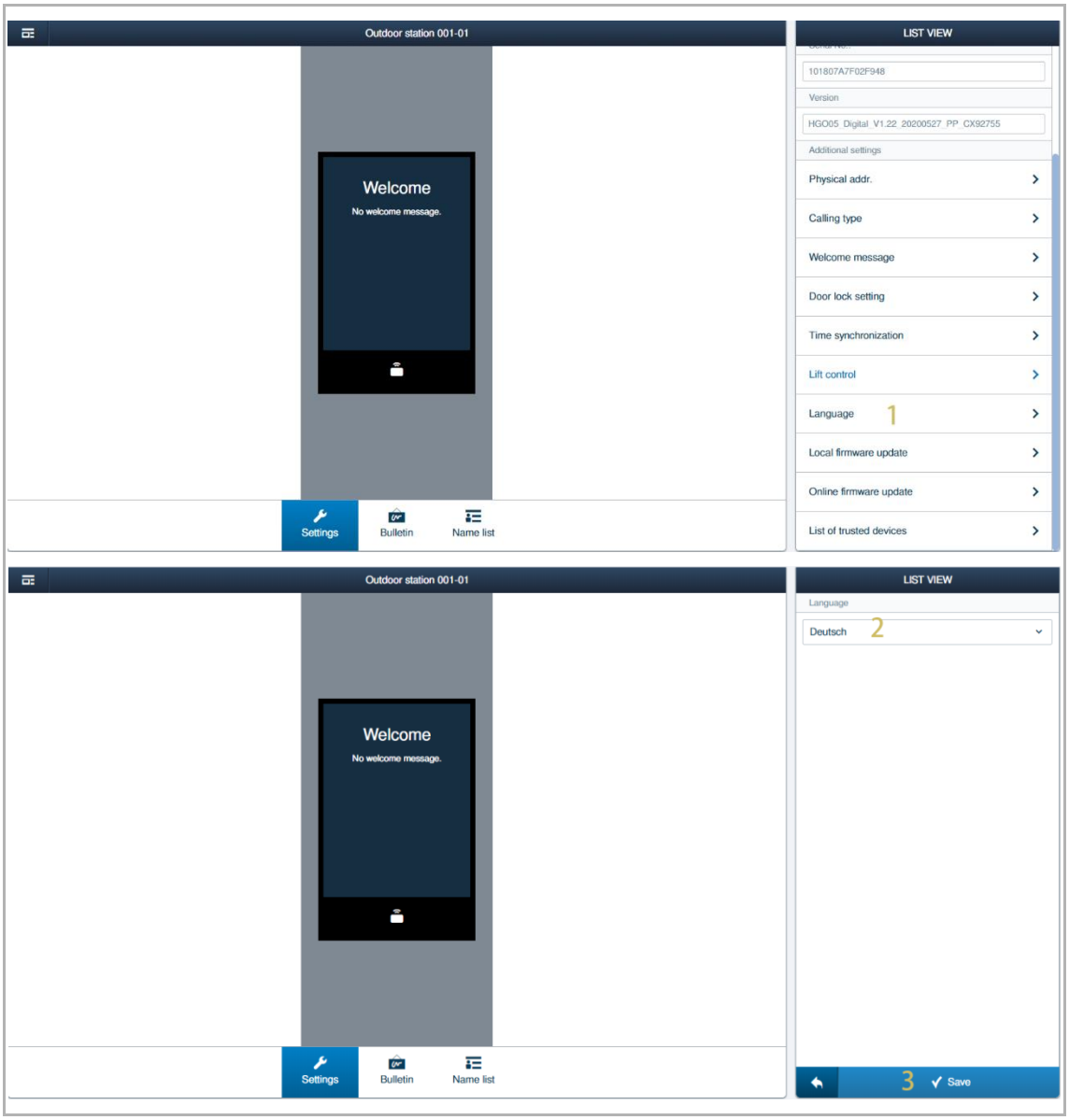
9.5.1 Taal wijzigen

Volg de onderstaande stappen:

[1] Op het scherm van de buitenpost klikt u op "Taal".

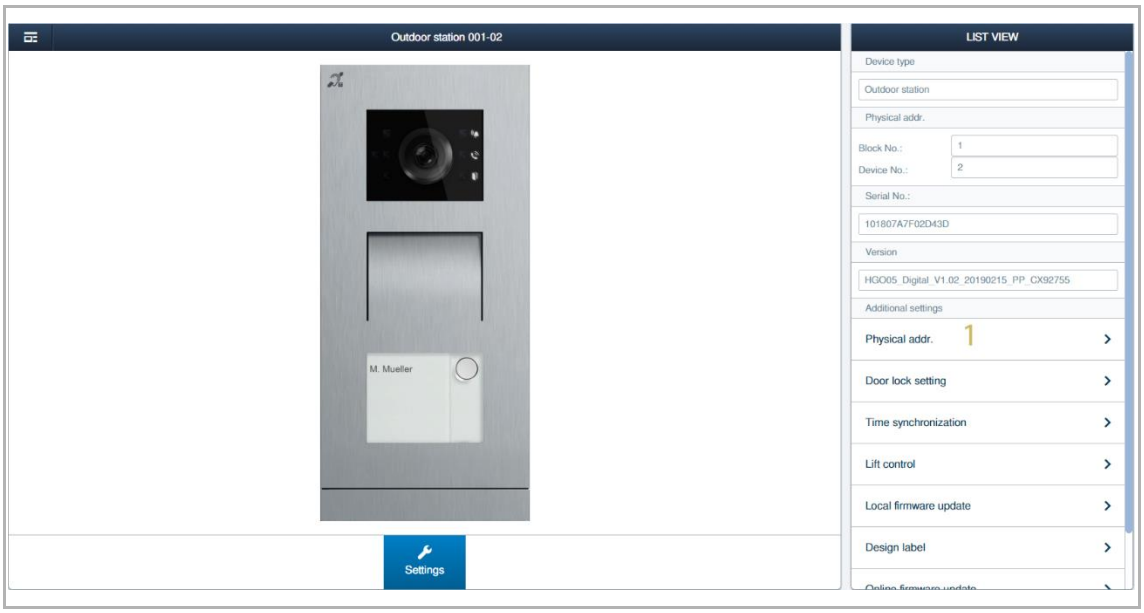
[2] Selecteer de taal uit de keuzelijst.

[3] Klik op "√" om op te slaan.



9.5.2 Fysiek adres beheren

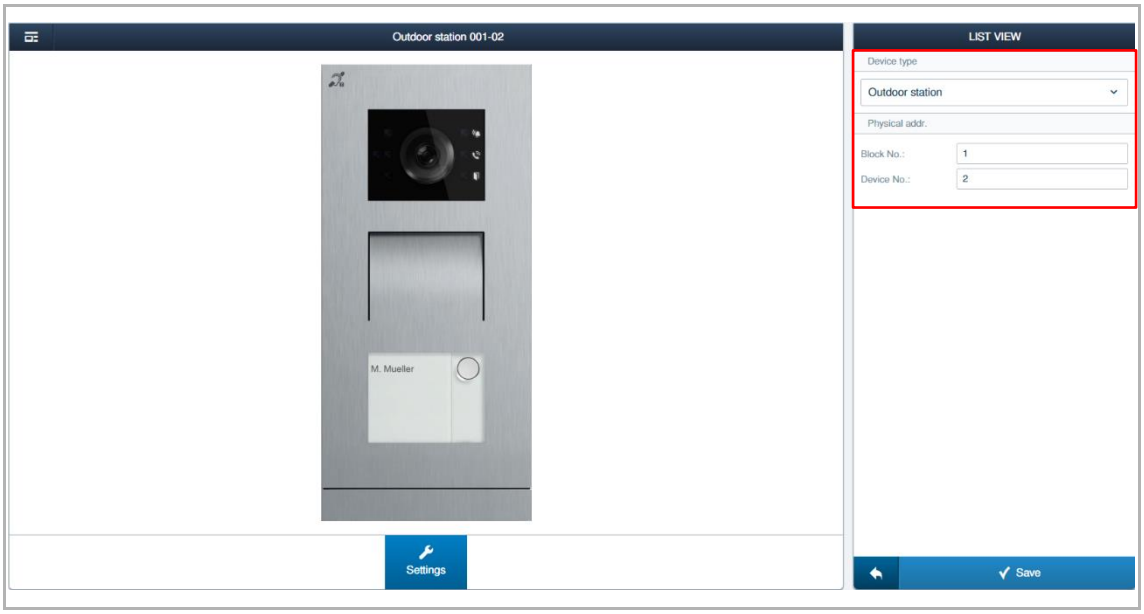
Op het scherm van de buitenpost klikt u op "Fysiek adres".



Er kan worden gekozen uit 3 typen apparaten.

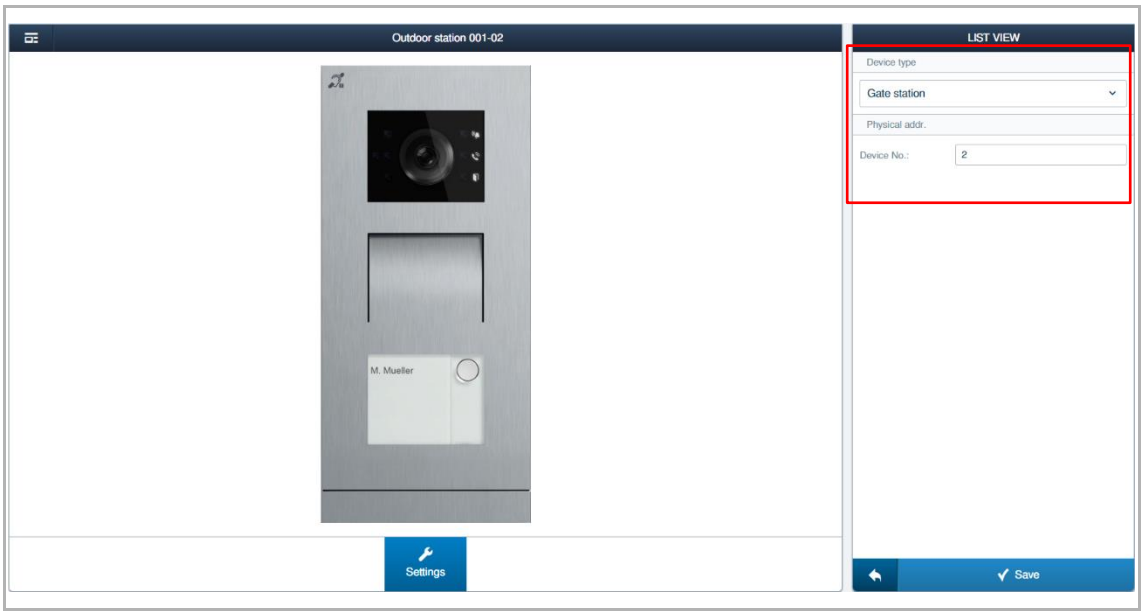
1. Buitenpost

Als het "Apparaattype" is ingesteld op " Buitenpost", moet u het bloknummer en het apparaatnummer instellen.



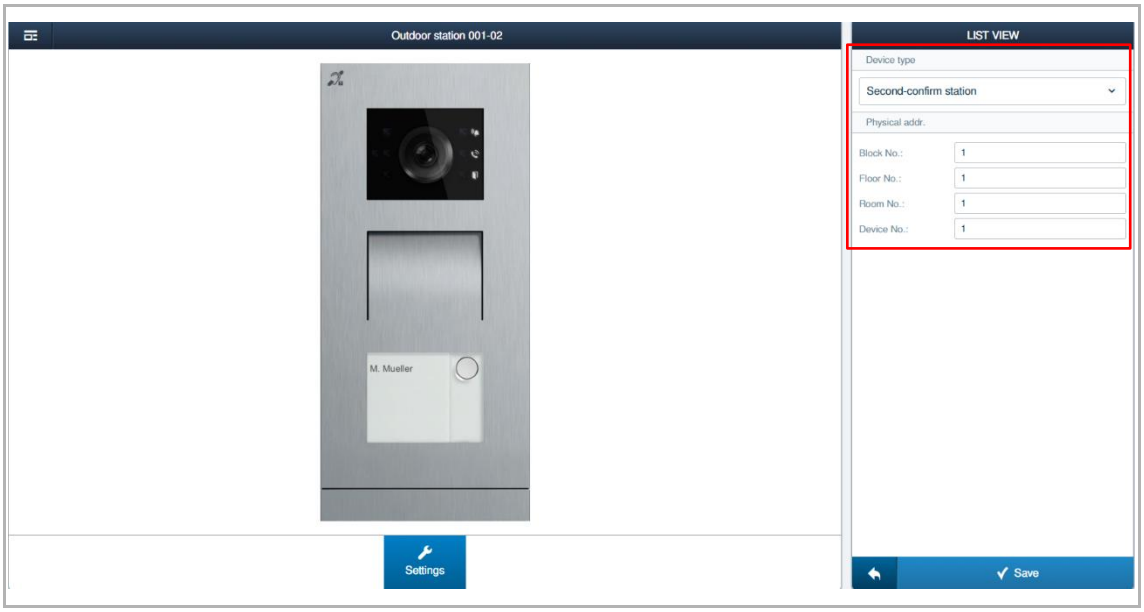
2. Deurpost

Als het "Apparaattype" is ingesteld op "Deurpost", moet u het bloknummer en het apparaatnummer instellen.



3. Bevestiging tweede post

Als het "Apparaattype" is ingesteld op "Tweede bevestigde post", moet u het bloknummer, het etagenummer, het ruimtenummer en het apparaatnummer instellen.



Opmerking

Alleen de IP-drukknop van de buitenpost kan worden ingesteld op "Bevestiging tweede post".

9.5.3 Ontgrendelinstelling

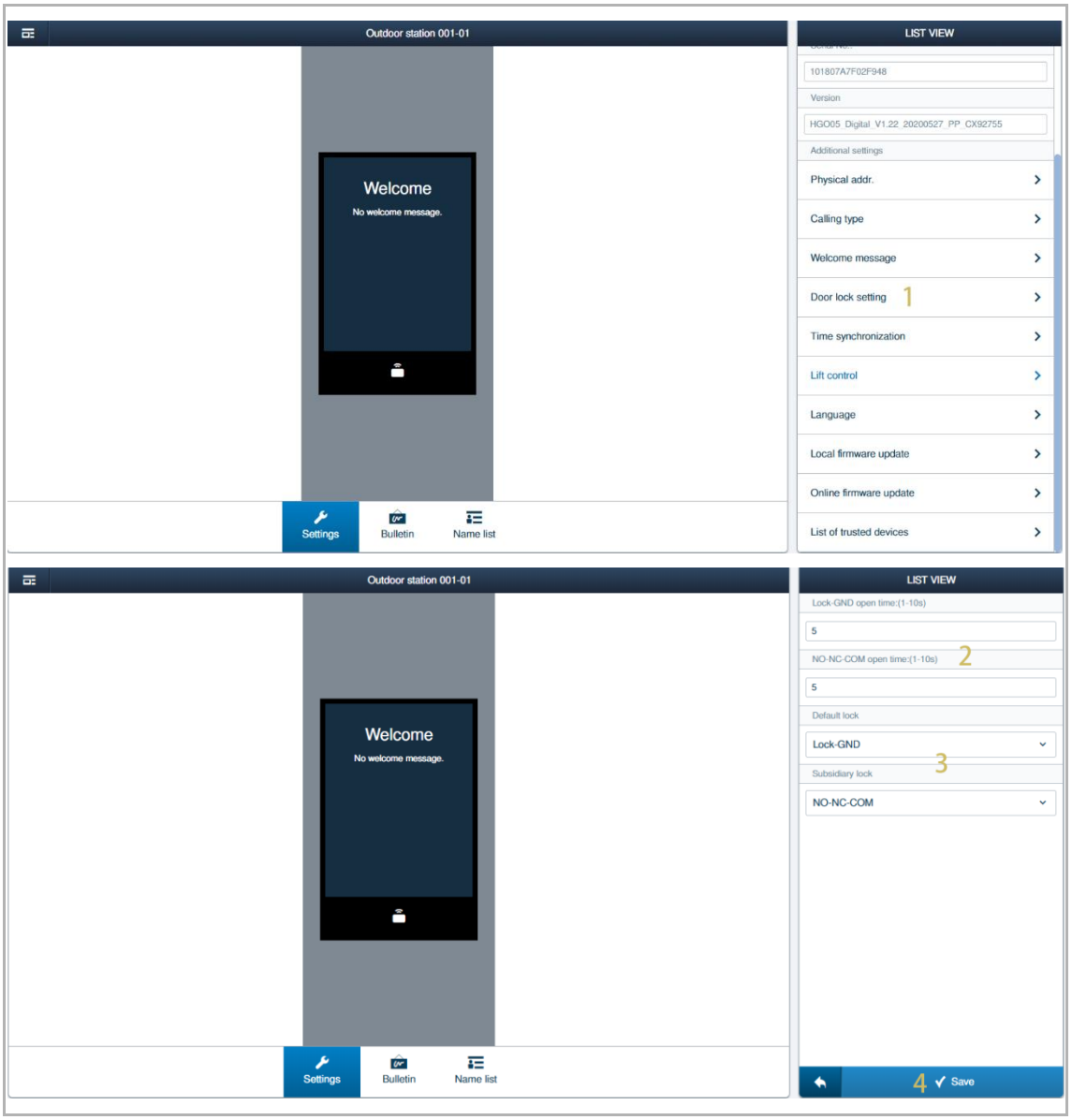
Volg de onderstaande stappen:

[1] Op het scherm van de buitenpost klikt u op "Inst. deurvergrendeling".

[2] Stel de deblokkeringstijd voor de blokkeringen in.

[3] Stel het blokkeringstype voor de blokkeringen in.

[4] Klik op "√" om op te slaan.



9.5.4 Tijdsynchronisatie

Volg de onderstaande stappen:

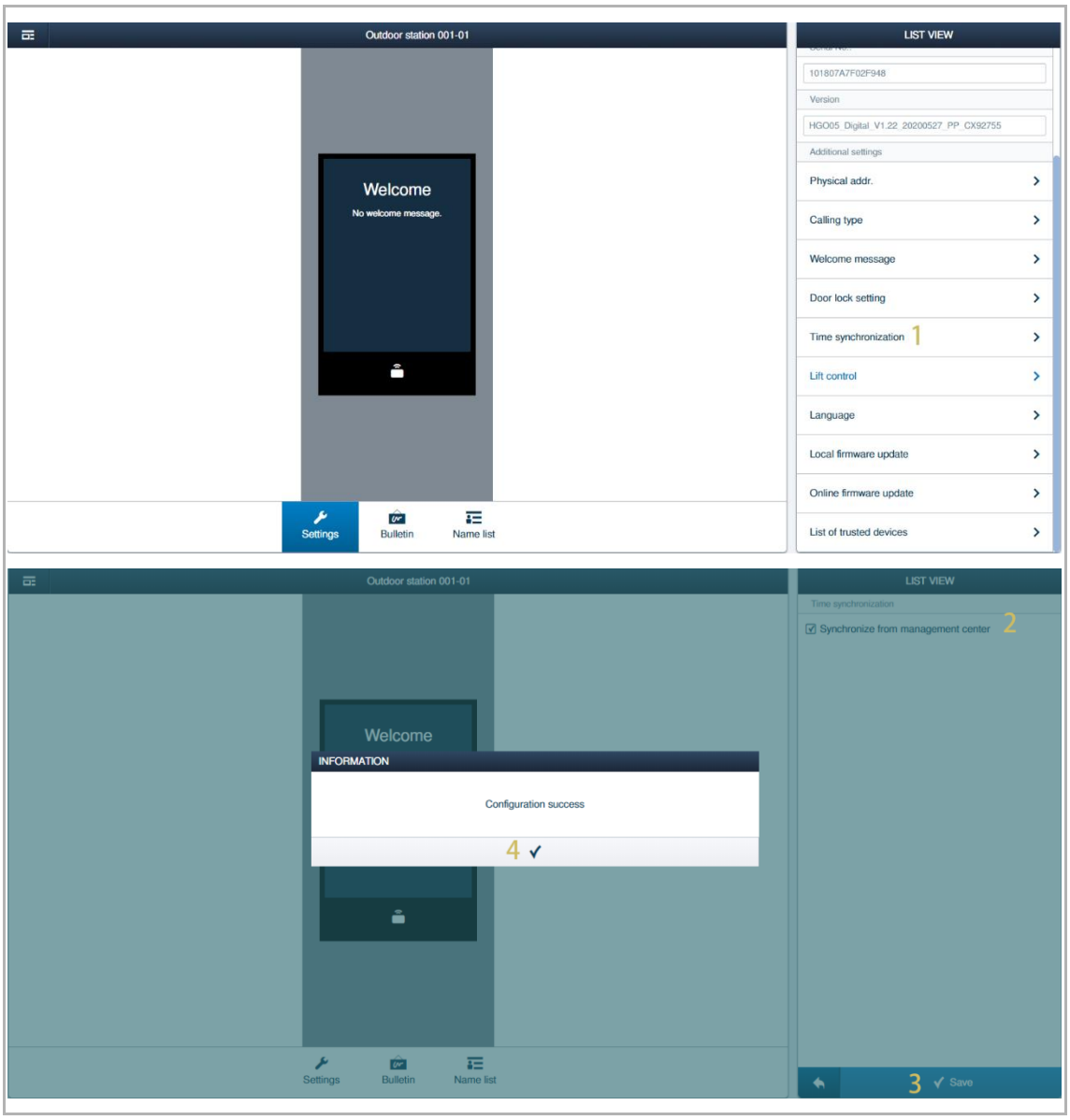
[1] Op het scherm van de buitenpost klikt u op "Tijdsynchronisatie".

[2] Vink het keuzevakje aan om de functie te activeren.

[3] Klik op "√" om op te slaan.

[4] Klik op "√" om te bevestigen.

Na de instelling kan de buitenpost de tijd synchroniseren met het "Smart Access Point".



9.5.5 Liftbesturing beheren

Volg de onderstaande stappen:

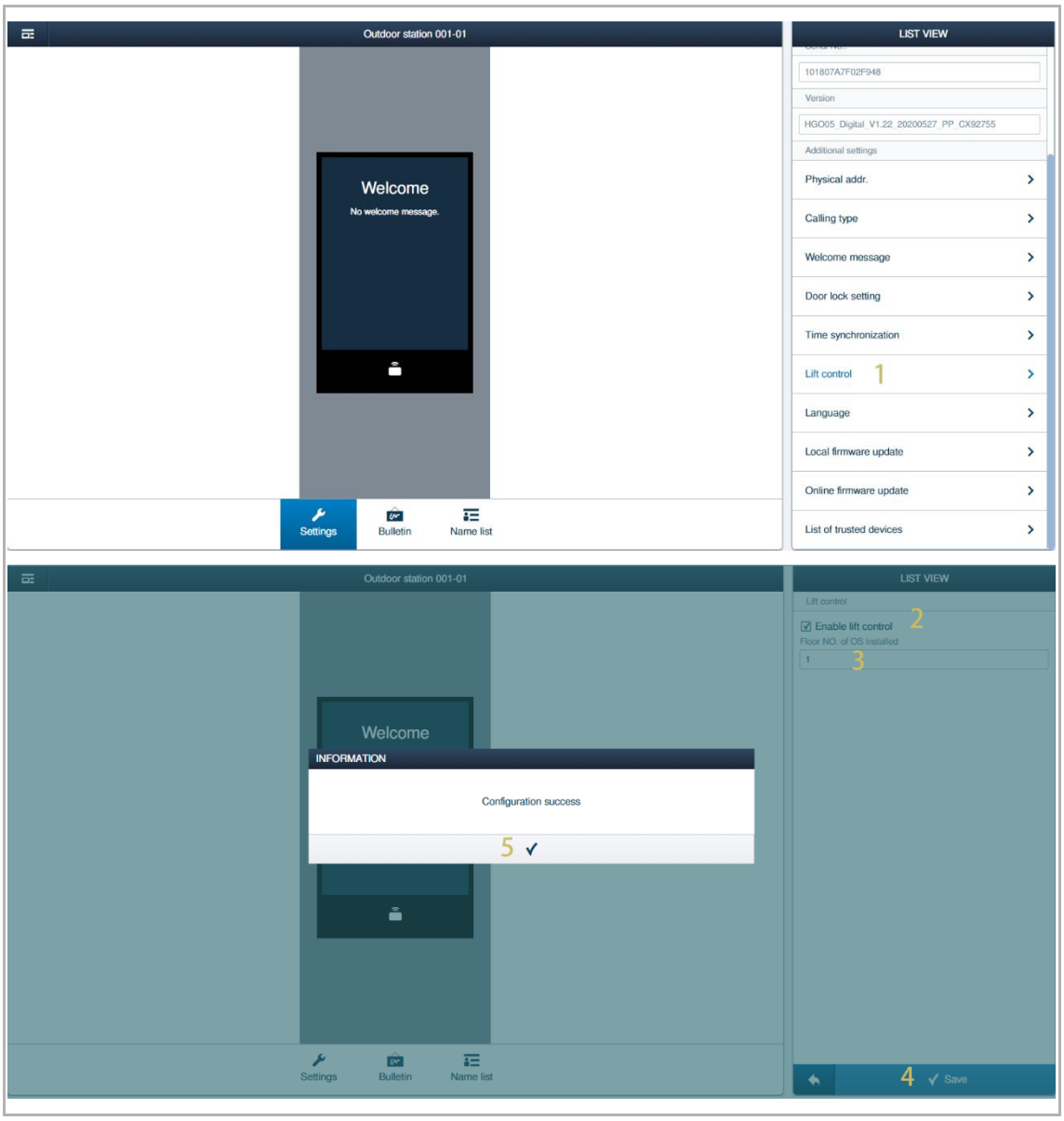
[1] Op het scherm van de buitenpost klikt u op "Liftbesturing".

[2] Vink het keuzevakje aan om de functie te activeren.

[3] Voer de etage in waar de buitenpost zich bevindt.

[4] Klik op "√" om op te slaan.

[5] Klik op "√" om te bevestigen.



9.5.6 Oproep initiëren via fysiek adres

Dit hoofdstuk is van toepassing op de IP touch 5-buitenpost en IP-buitenpost met toetsenbord.

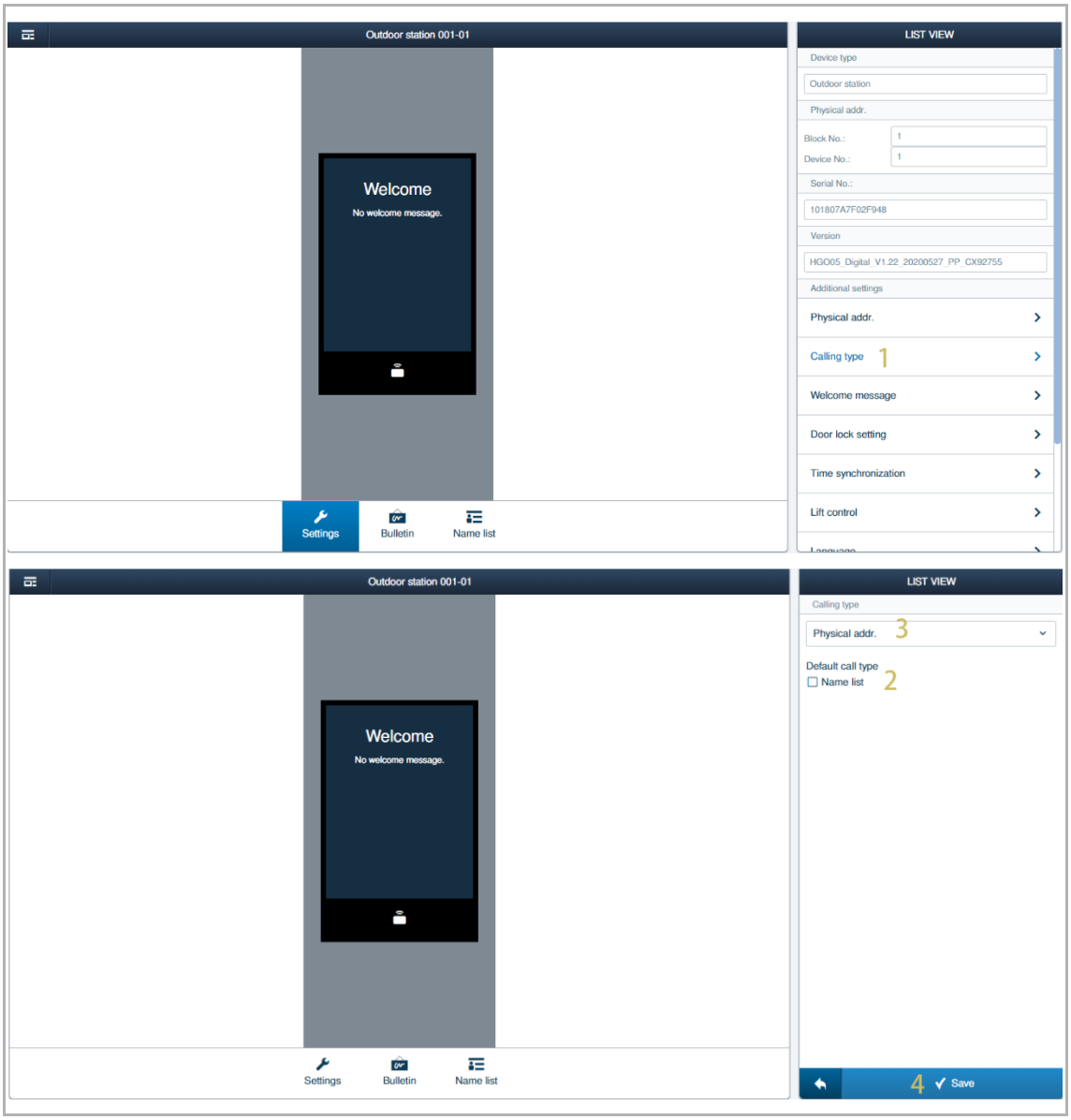
Volg de onderstaande stappen:

[1] Op het scherm van de buitenpost klikt u op "Oproeptype".

[2] Deactiveer de "namenlijst" (geldt alleen voor IP touch 5-buitenposten).

[3] Stel "Oproeptype" in op "Fysiek adres"

[4] Klik op "√" om op te slaan.



9.5.7 Oproep initiëren via logisch adres

Dit hoofdstuk is van toepassing op de IP touch 5-buitenpost en IP-buitenpost met toetsenbord.

1. Logisch adres toevoegen

Volg de onderstaande stappen:

[1] Op het scherm van de buitenpost klikt u op "Oproeptype".

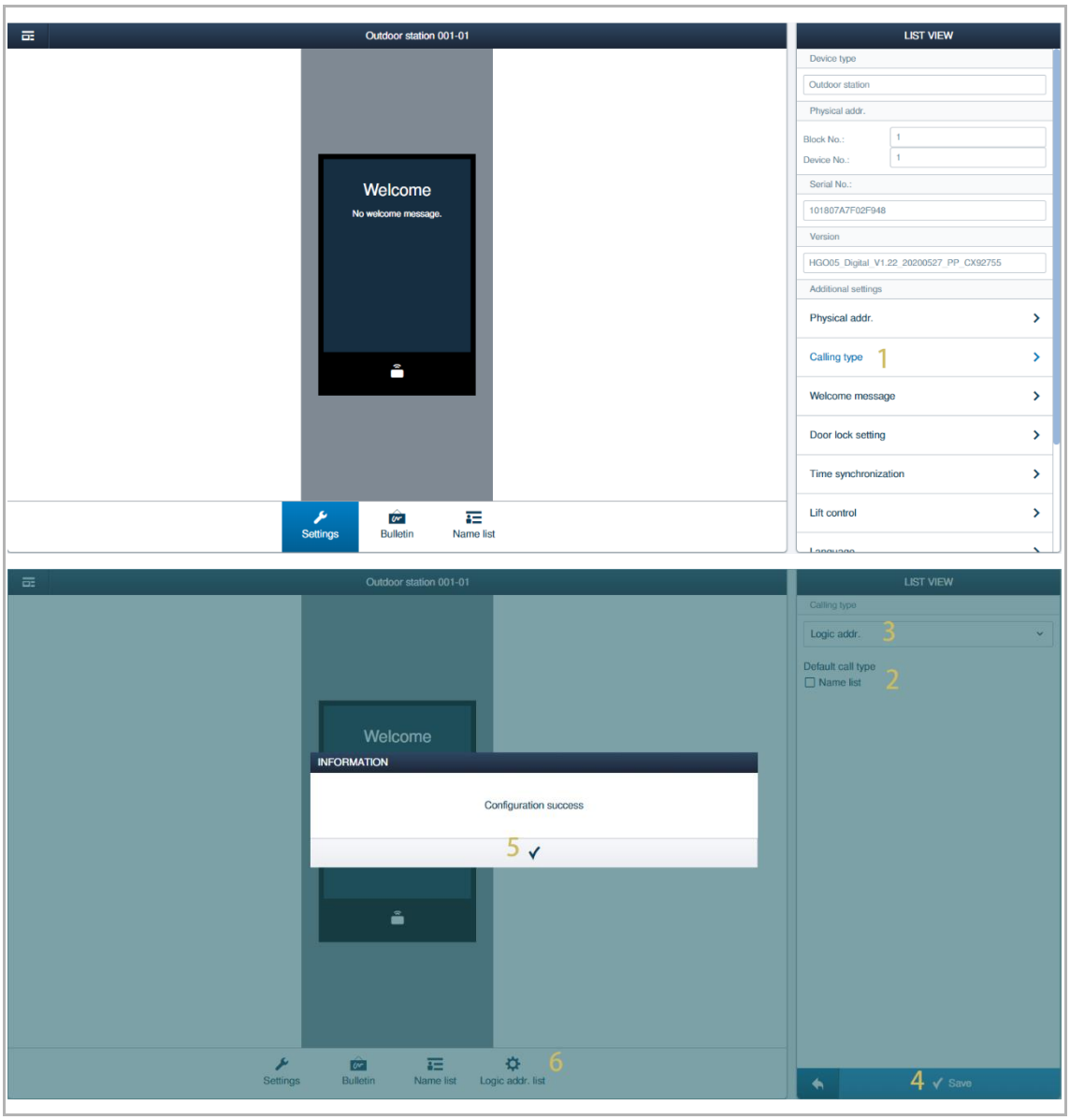
[2] Deactiveer de "namenlijst" (geldt alleen voor IP touch 5-buitenposten).

[3] Stel "Oproeptype" in op "Logisch adr."

[4] Klik op "√" om op te slaan.

[5] Klik op "√" om te bevestigen.

[6] "Lijst logische adr." wordt weergegeven op het scherm. Klik om door te gaan.

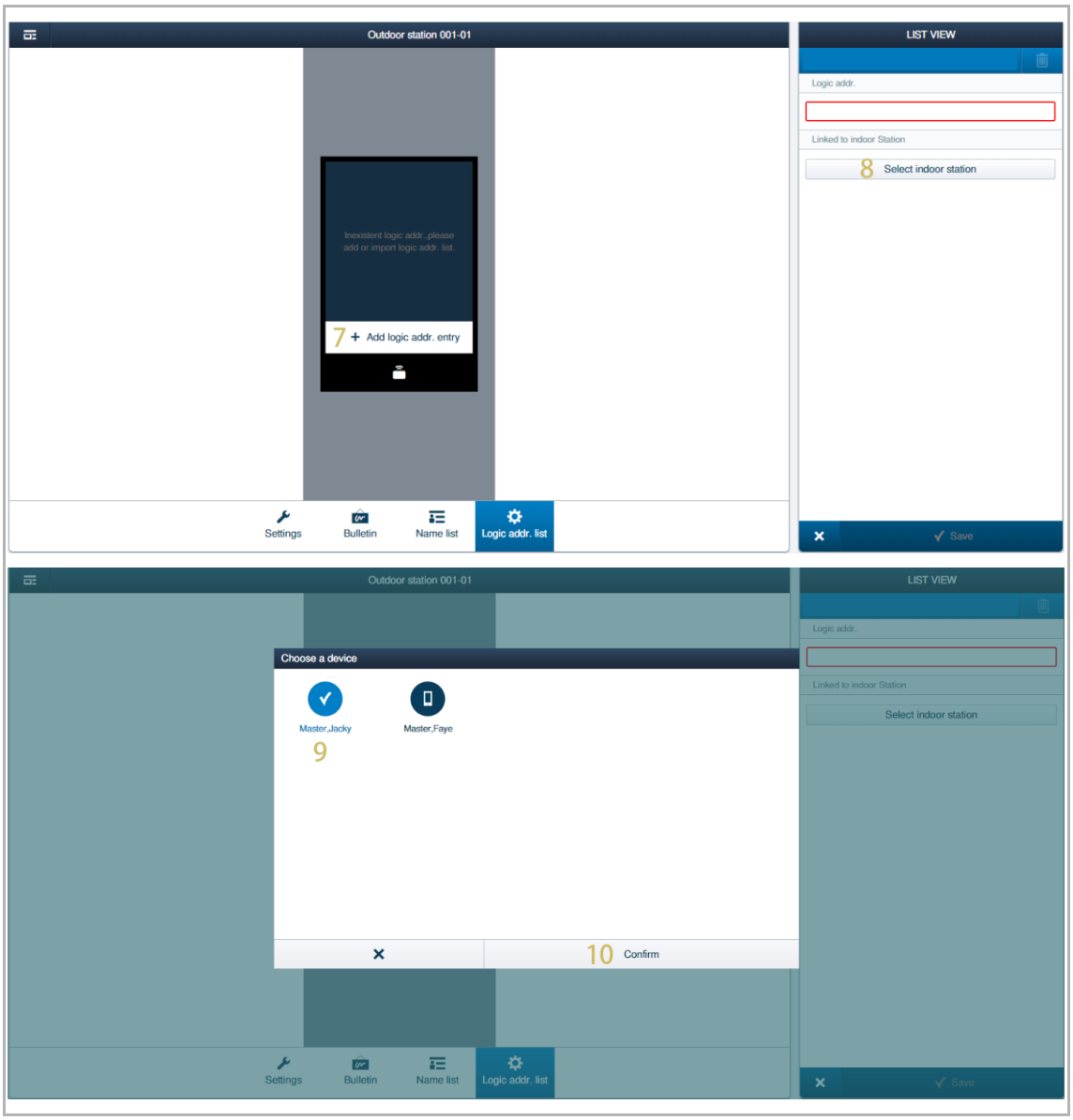


[7] Op het scherm "Lijst logische adr." klikt u op "+".

[8] Klik op de "Binnenpost selecteren".

[9] Klik om de gewenste binnenpost te selecteren.

[10] Klik op "Bevestigen".

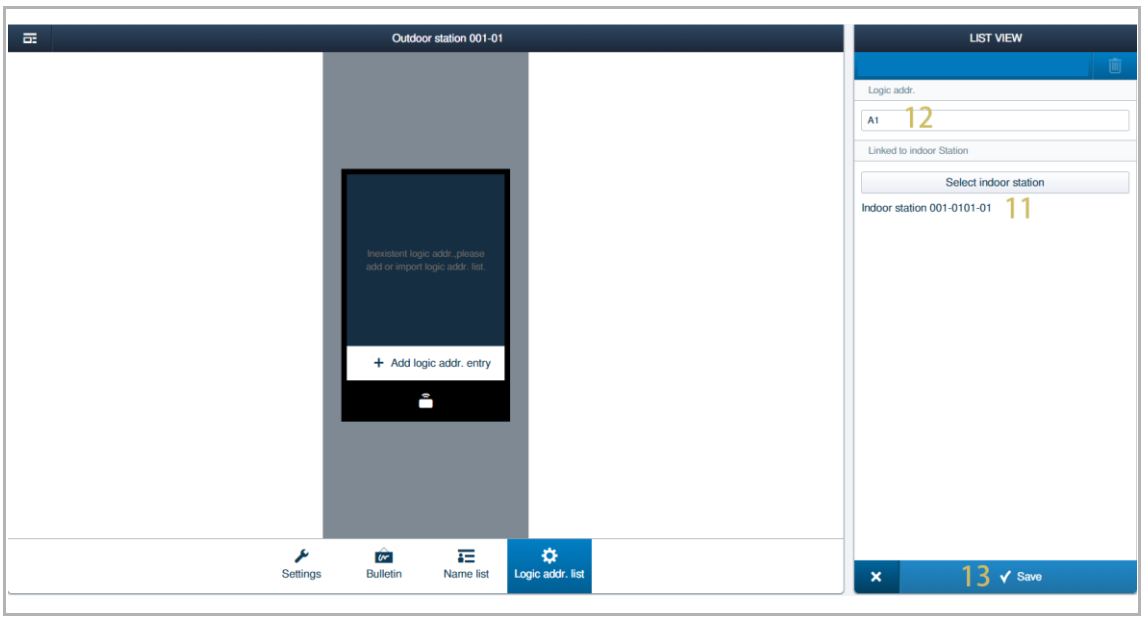


[11]De binnenpost is toegevoegd aan de lijst.

[12]Het logische adres is geïmporteerd in de lijst.

[13]Klik op "√" om op te slaan en vervolgens op "√" om te bevestigen.

Herhaal de stappen 7-13 om de logische adressen één voor één toe te voegen.



2. Logisch adres importeren

Volg de onderstaande stappen:

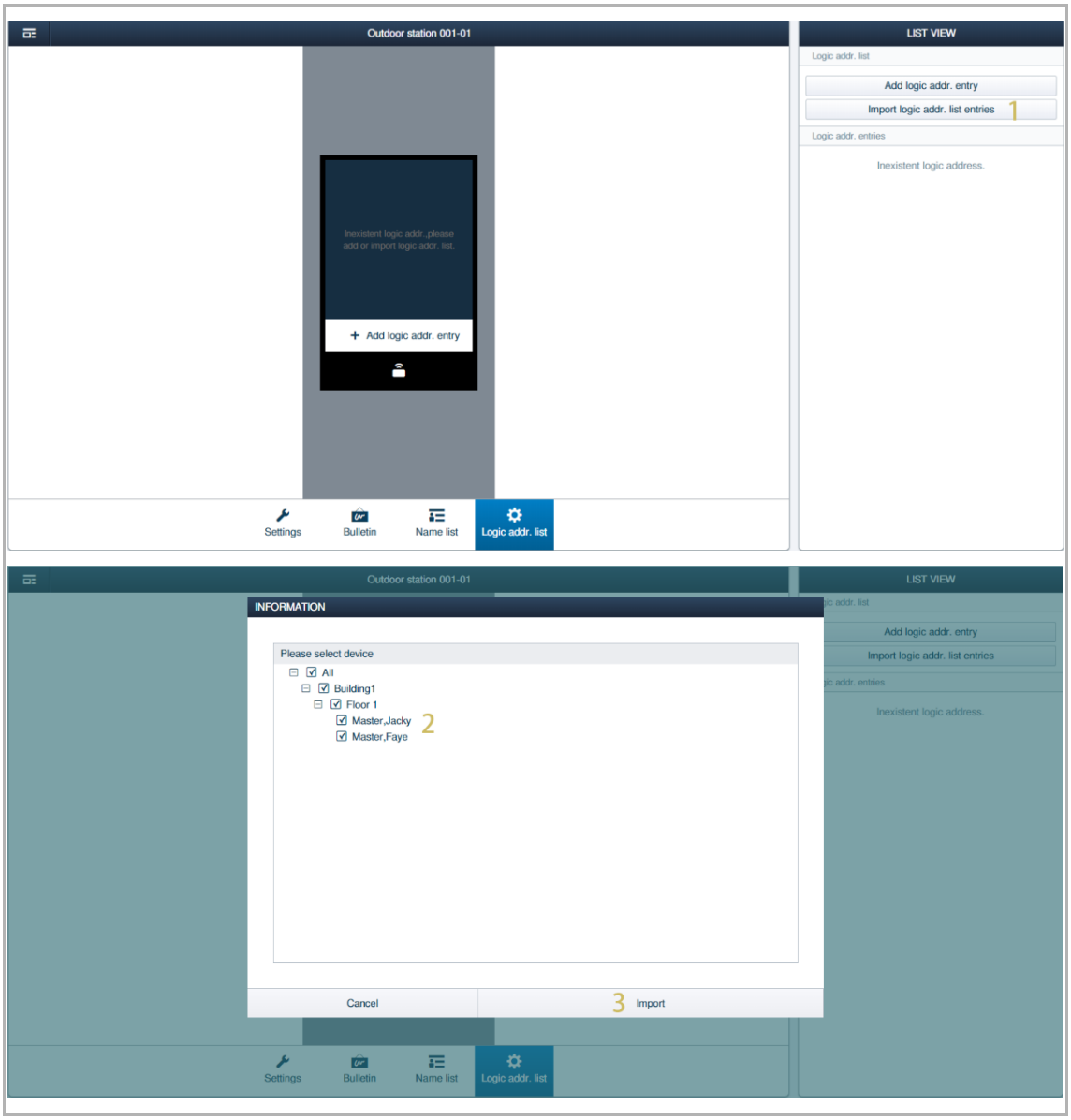
[1] Op het scherm "Lijst logische adr." klikt u op "Importeren lijst logische adr.".

Opmerking

Aanbevolen wordt om het logische adres van de binnenpost in te stellen voordat deze wordt geïmporteerd.

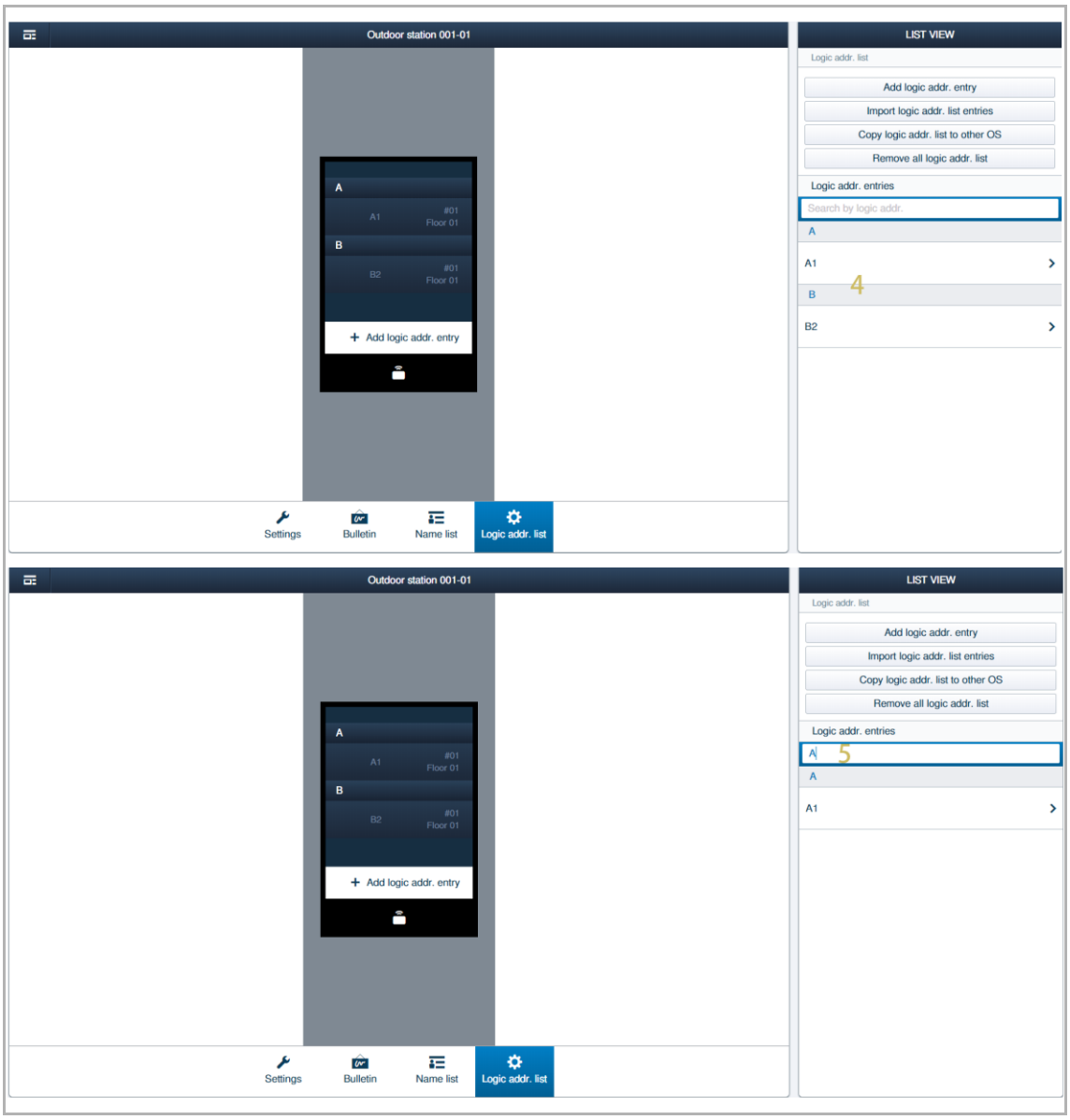
[2] Klik om de gewenste binnenposten te selecteren.

[3] Klik op "Importer." en vervolgens op "√".



[4] De logische adressen zijn geïmporteerd in de lijst.

[5] Voer een sleutelwoord in om de zoekresultaten te filteren.



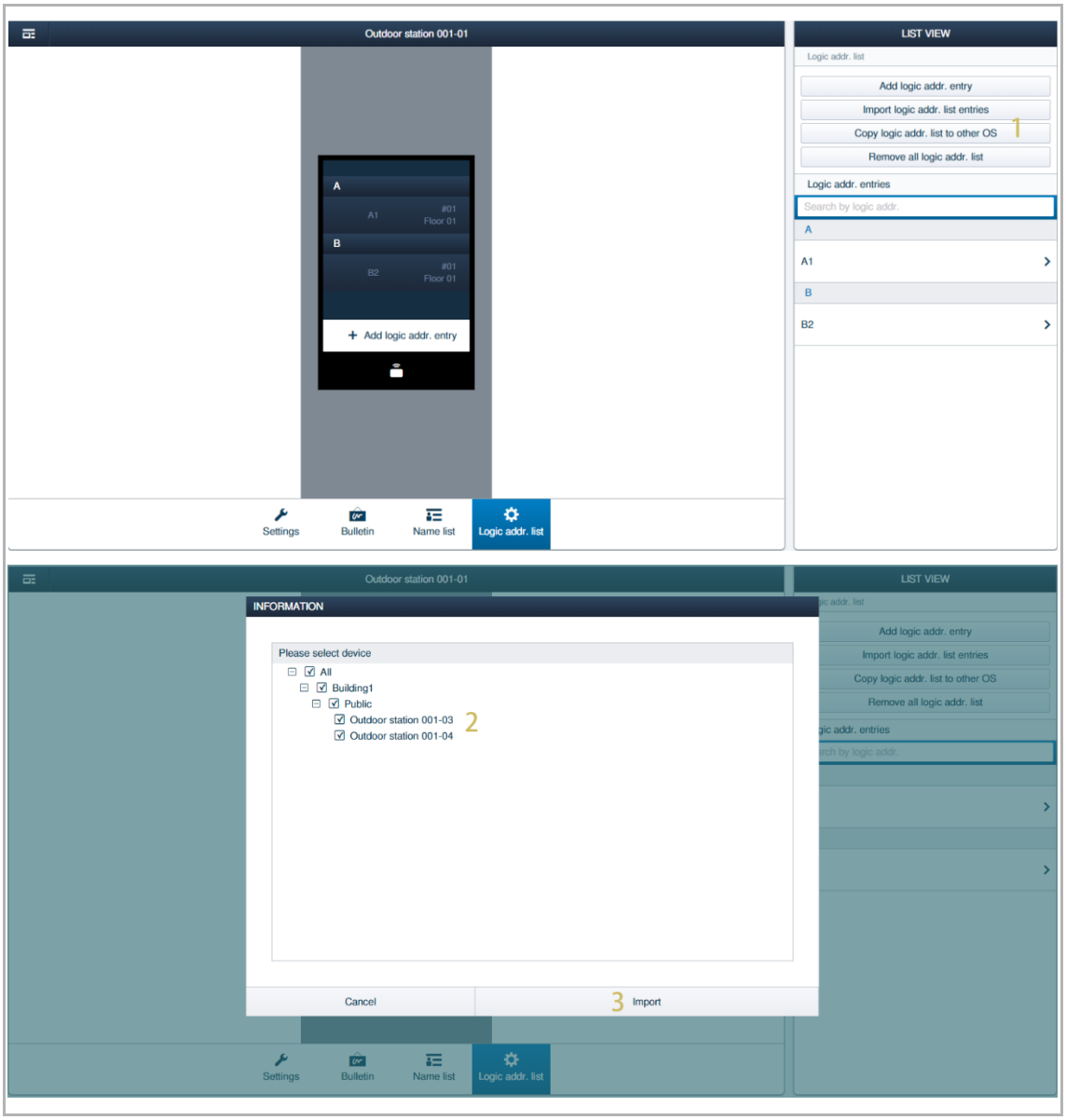
3. Lijst met logische adressen kopiëren naar een andere buitenpost

Volg de onderstaande stappen:

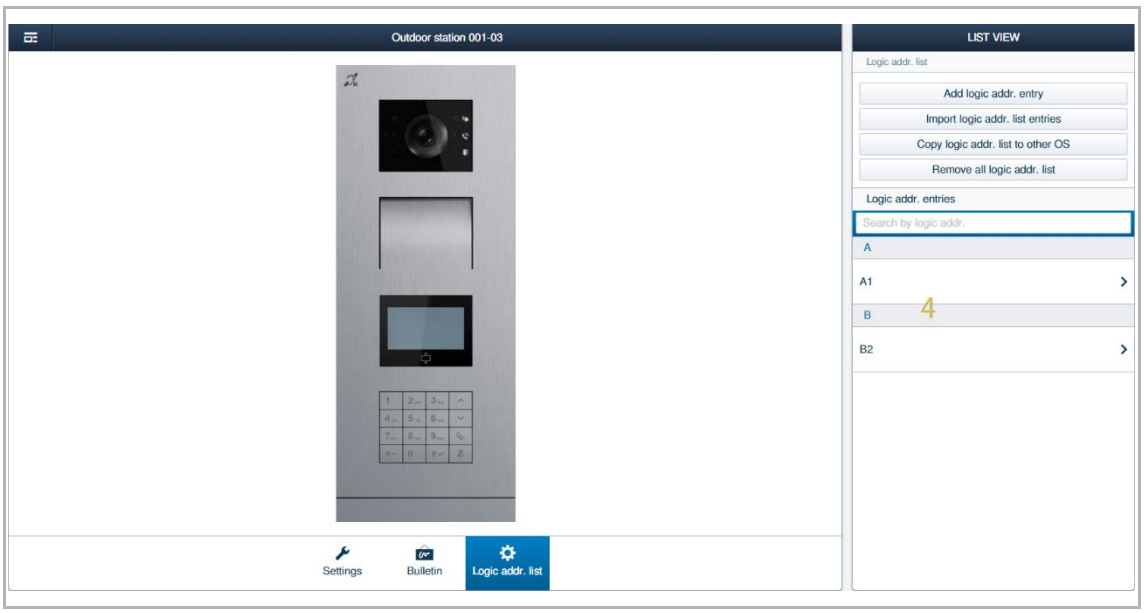
[1] Op het scherm "Lijst logische adr." klikt u op "Kopiëren lijst logische adr. naar andere buitenpost".

[2] Klik om de gewenste buitenposten te selecteren.

[3] Klik op "Importer." en vervolgens op "√".



[4] De lijst met logische adressen is gekopieerd naar de andere buitenpost.

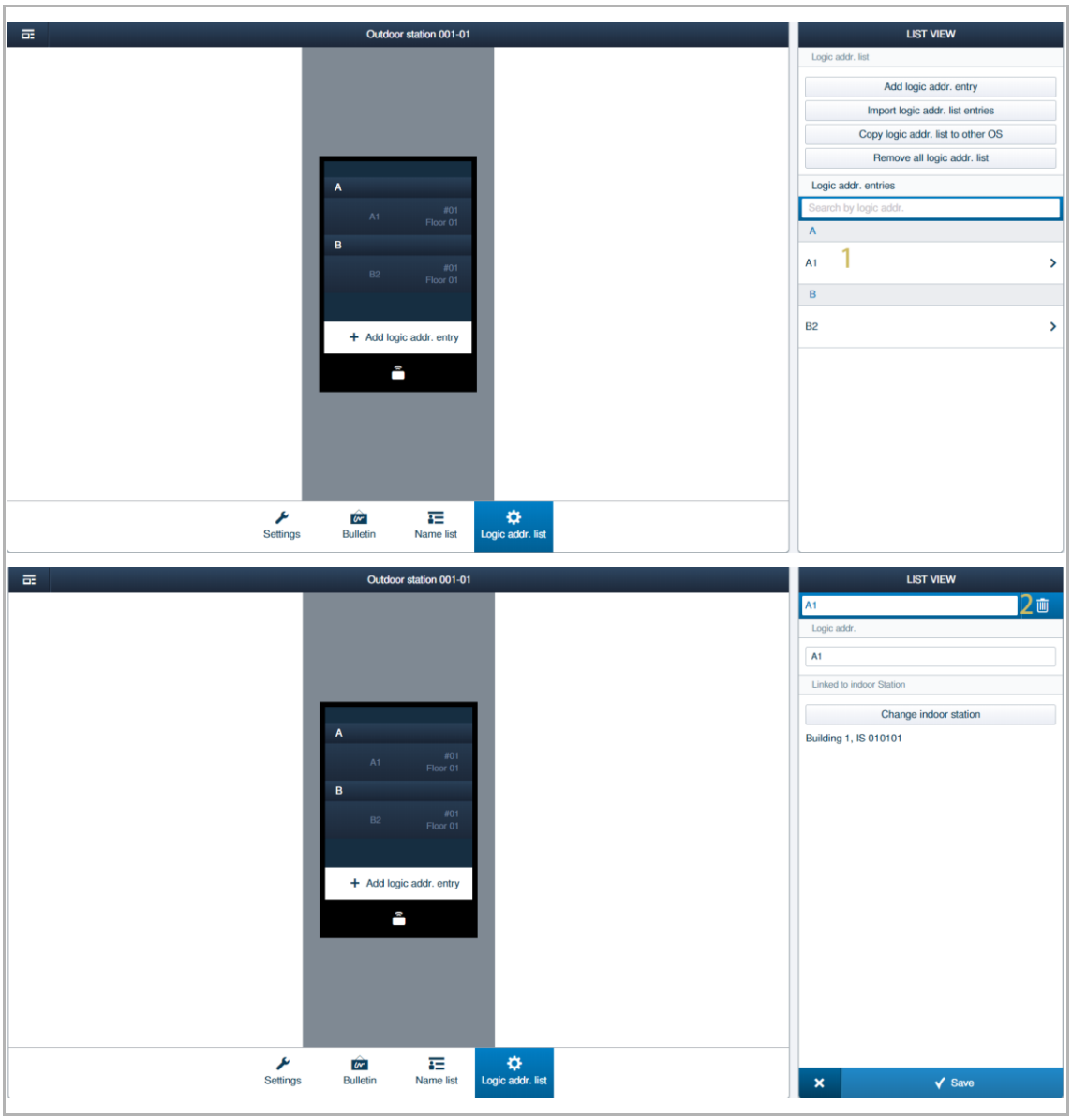


4. Logisch adres verwijderen

Volg de onderstaande stappen:

[1] Op het scherm "Lijst logische adr." klikt u op het betreffende logische adres.

[2] Klik op "" en vervolgens op "√" om te bevestigen.



Opmerking

U kunt ook op "Hele lijst logische adr. wissen" klikken om alle logische adressen te wissen.

9.5.8 Oproep initiëren via namenlijst

Dit hoofdstuk is alleen van toepassing op de IP touch 5-buitenpost.

1. Namenlijst importeren

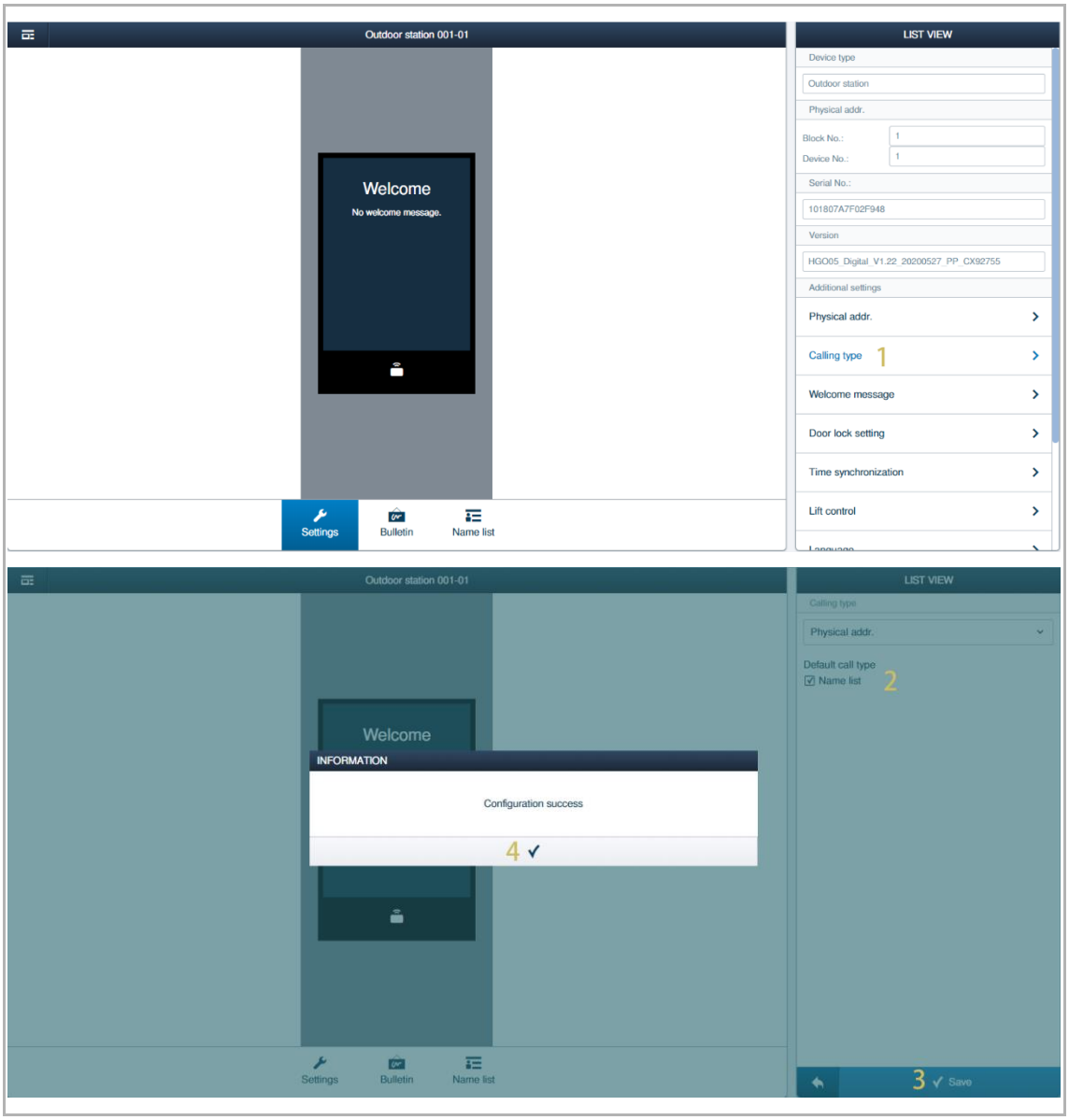
Volg de onderstaande stappen:

[1] Op het scherm van de buitenpost klikt u op "Oproeptype".

[2] "Namenlijst" activeren.

[3] Klik op "√" om op te slaan.

[4] Klik op "√" om te bevestigen.



[5] Op het scherm van de buitenpost klikt u op "Namenlijst".

Opmerking
Aanbevolen wordt om de naam van de binnenposten in te stellen voordat deze worden geïmporteerd.

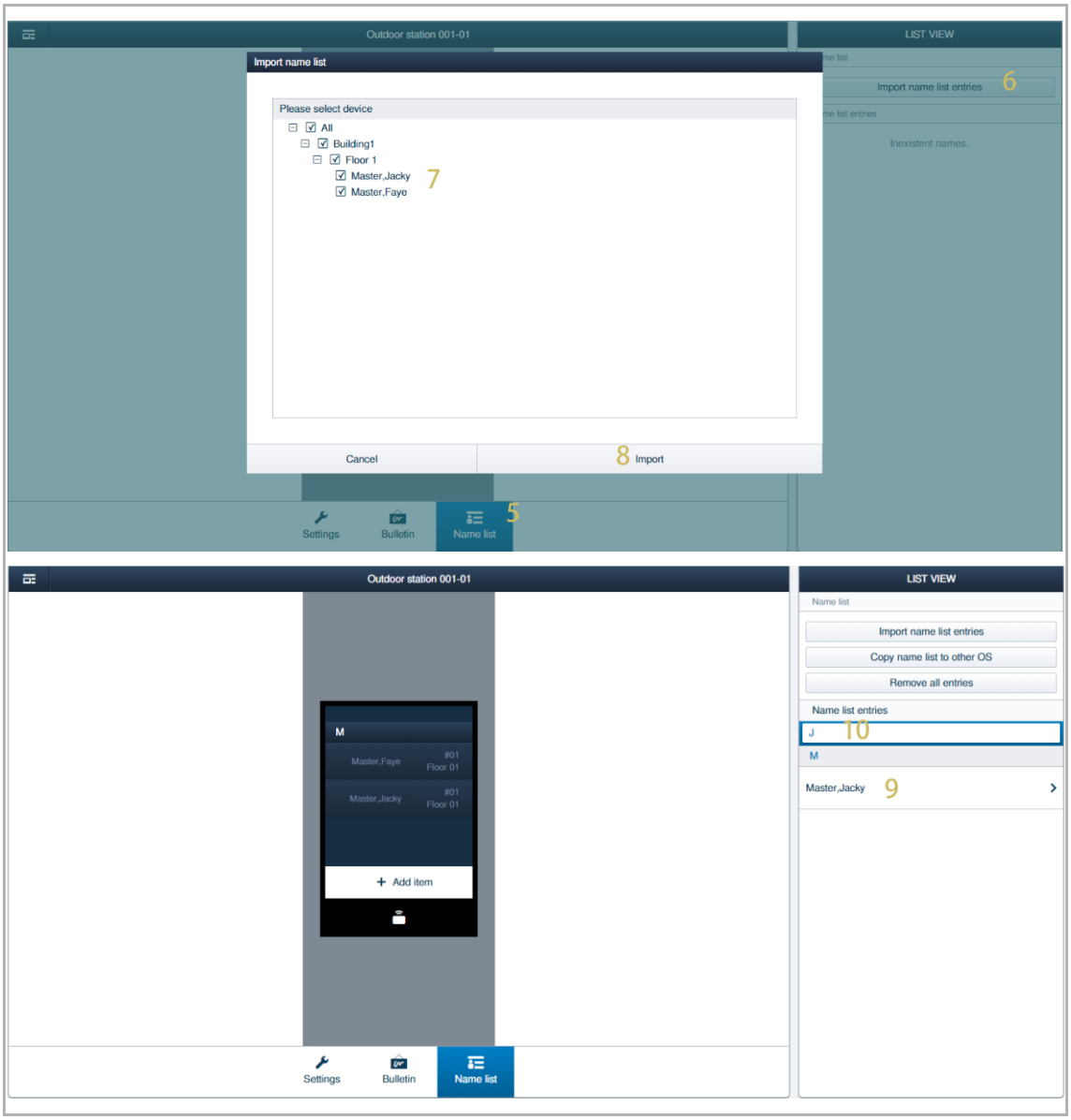
[6] Klik op "Items namenlijst importeren".

[7] Klik om de gewenste binnenposten te selecteren.

[8] Klik op "Importer." en vervolgens op "√" om te bevestigen.

[9] De namen zijn geïmporteerd in de lijst.

[10]Voer het sleutelwoord in om de zoekresultaten te filteren.

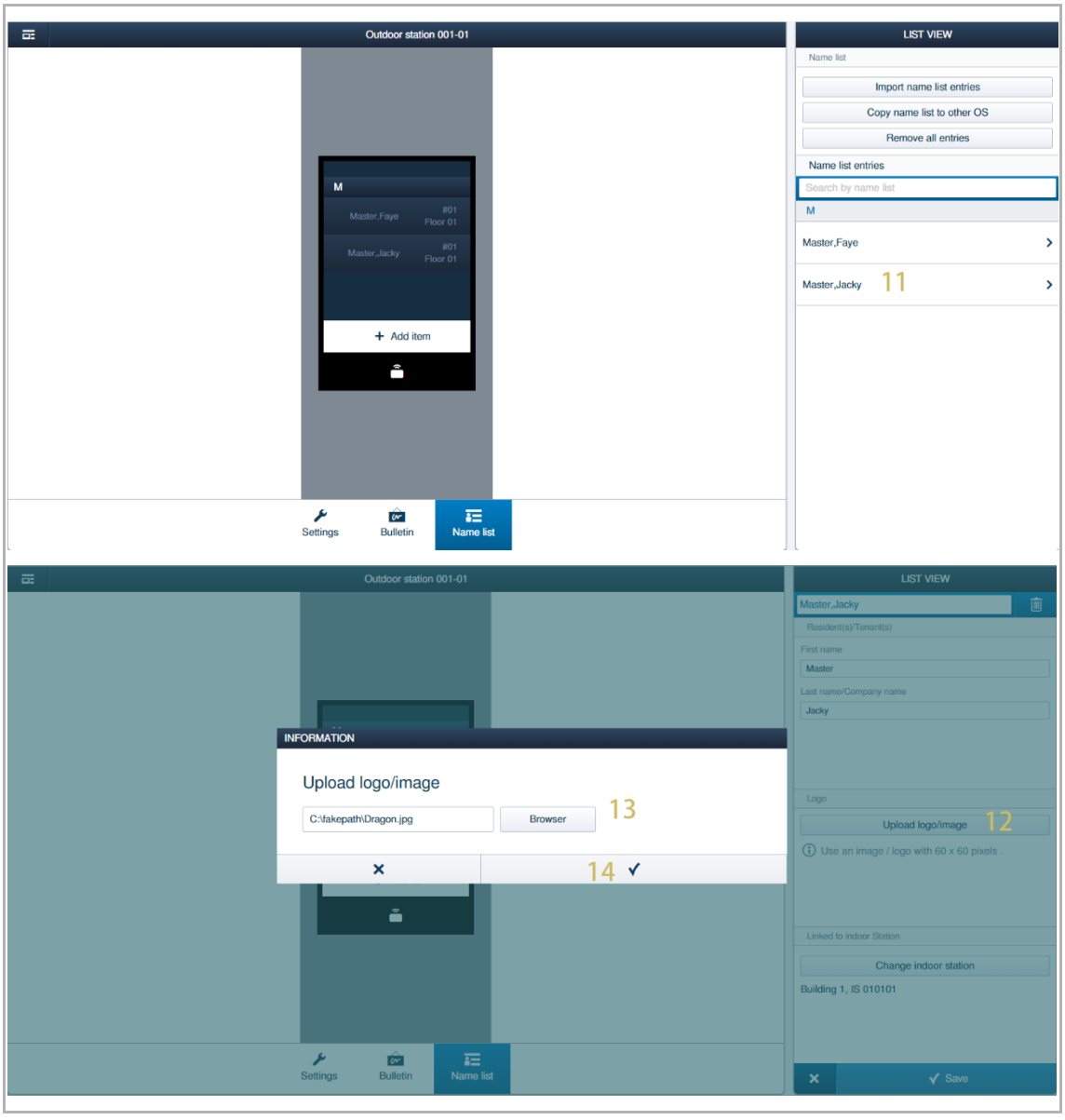


[11]Klik op de betreffende naam.

[12]Klik op "Logo/afbeelding uploaden".

[13]Klik op "Browser" om een logoafbeelding te selecteren (alleen .jpg wordt ondersteund. De maximale resolutie is 60 x 60 pixels).

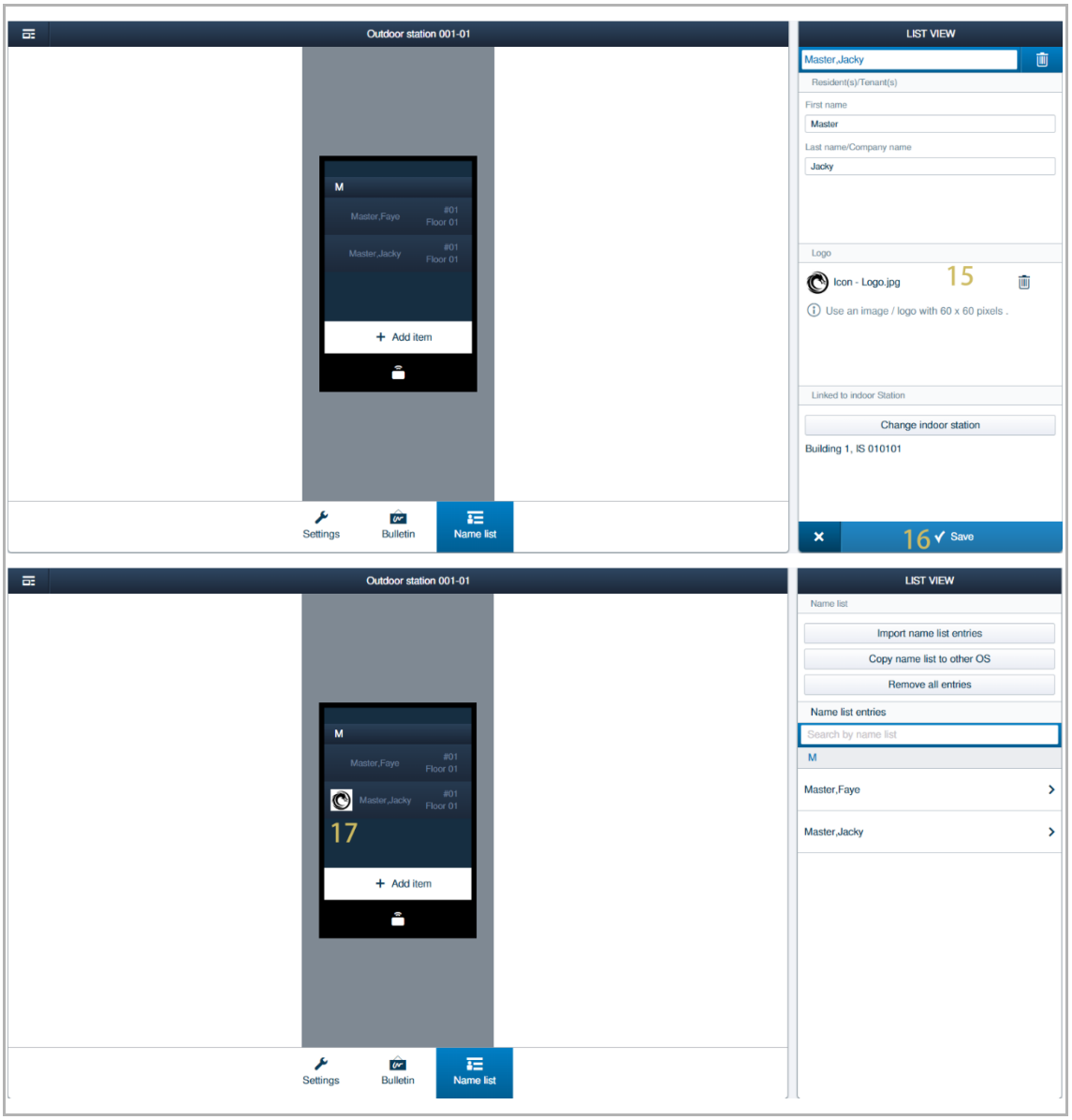
[14]Klik op "√" om te bevestigen.



[15]Het logo wordt weergegeven in de lijst.

[16]Klik op "√" om op te slaan.

[17]Het logo wordt weergegeven op het scherm van de buitenpost.



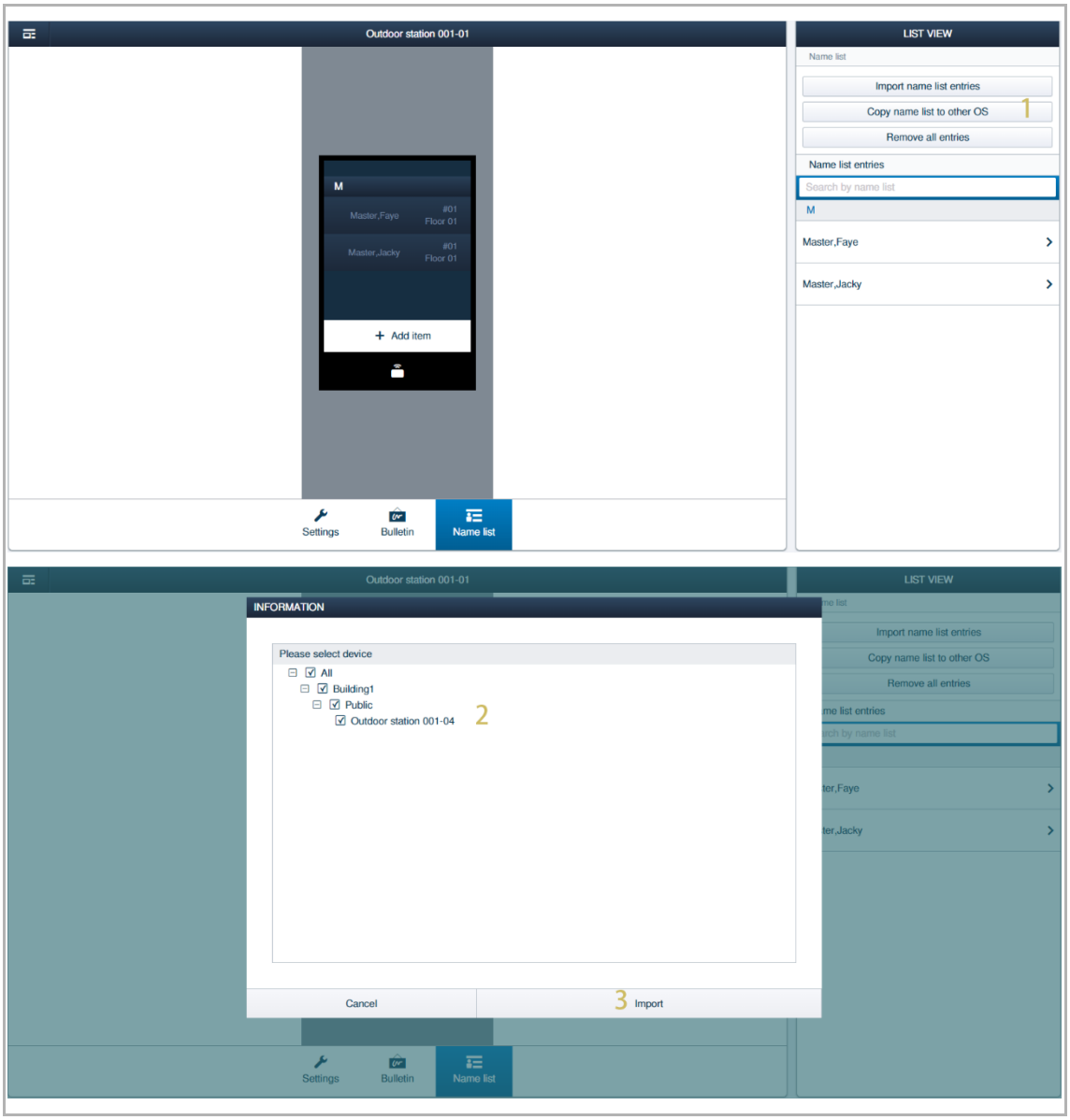
2. Namenlijst kopiëren naar een andere buitenpost

Volg de onderstaande stappen:

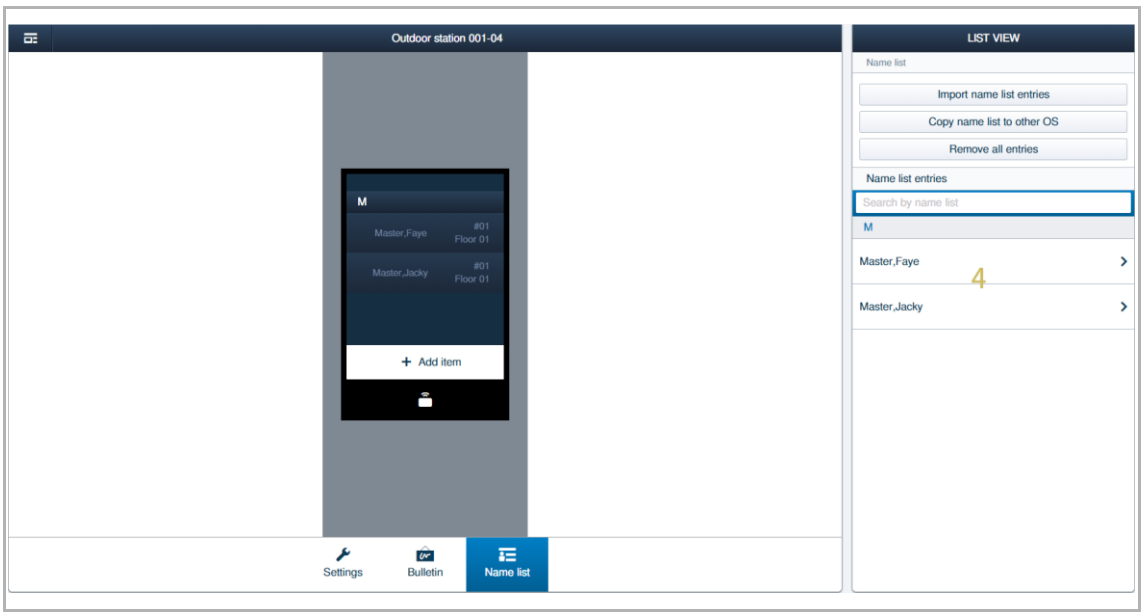
[1] Op het scherm "Namenlijst" klikt u op "Kopiëren namenlijst naar andere buitenpost".

[2] Klik om de gewenste buitenposten te selecteren (alleen ondersteund door het IP touch 5-buitenpost)

[3] Klik op "Importer." en vervolgens op "√".



[4] De namenlijst is gekopieerd naar de andere buitenpost.

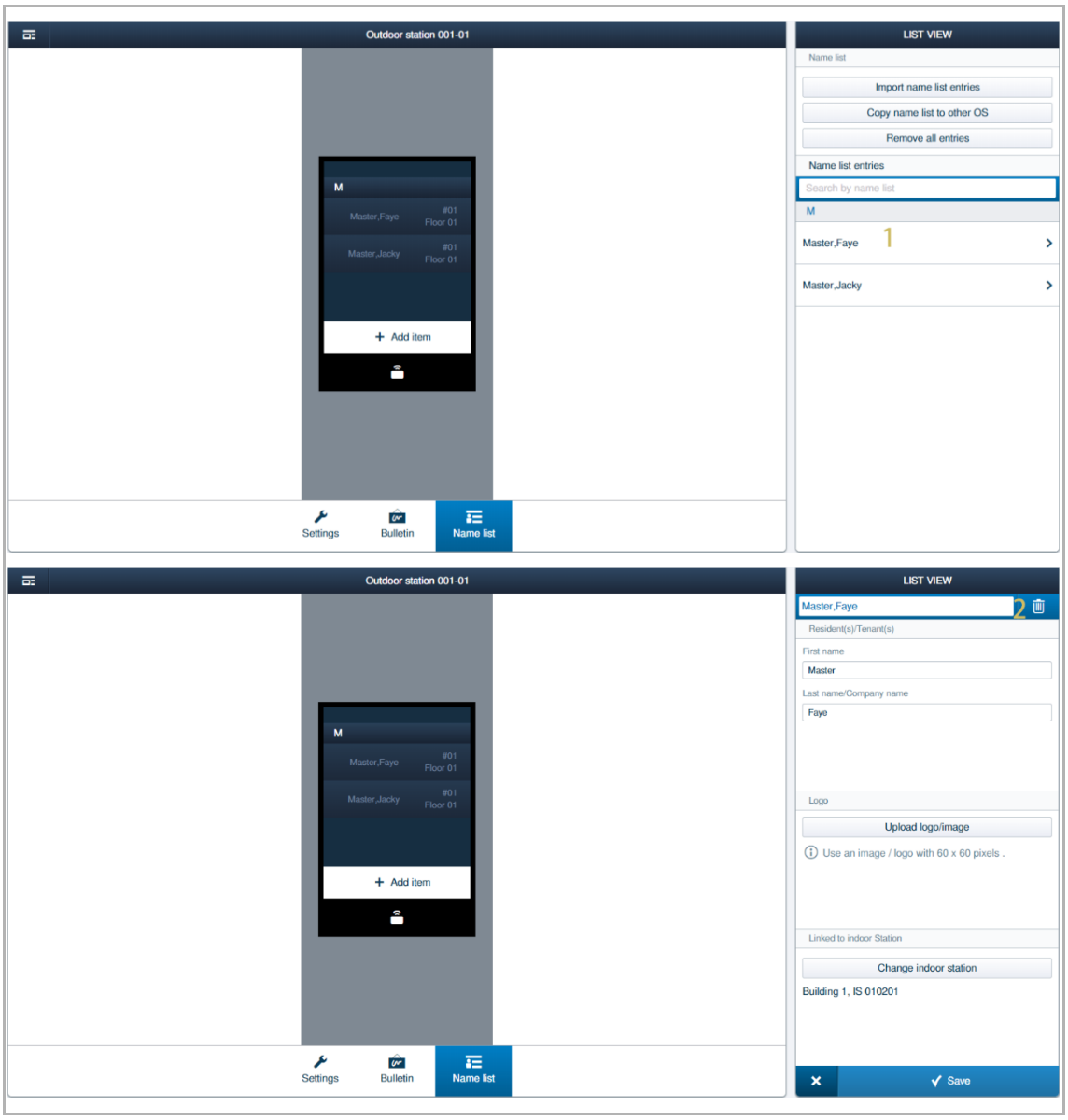


3. Logisch adres verwijderen

Volg de onderstaande stappen:

[1] Op het scherm "Lijst logische adr." klikt u op het betreffende logische adres.

[2] Klik op "" en vervolgens op "√" om te bevestigen.



Opmerking

U kunt ook klikken op "Alle items verwijderen" om de namenlijst te wissen.

9.5.9 Welkomstbericht beheren

Dit hoofdstuk is alleen van toepassing op de IP touch 5-buitenpost.

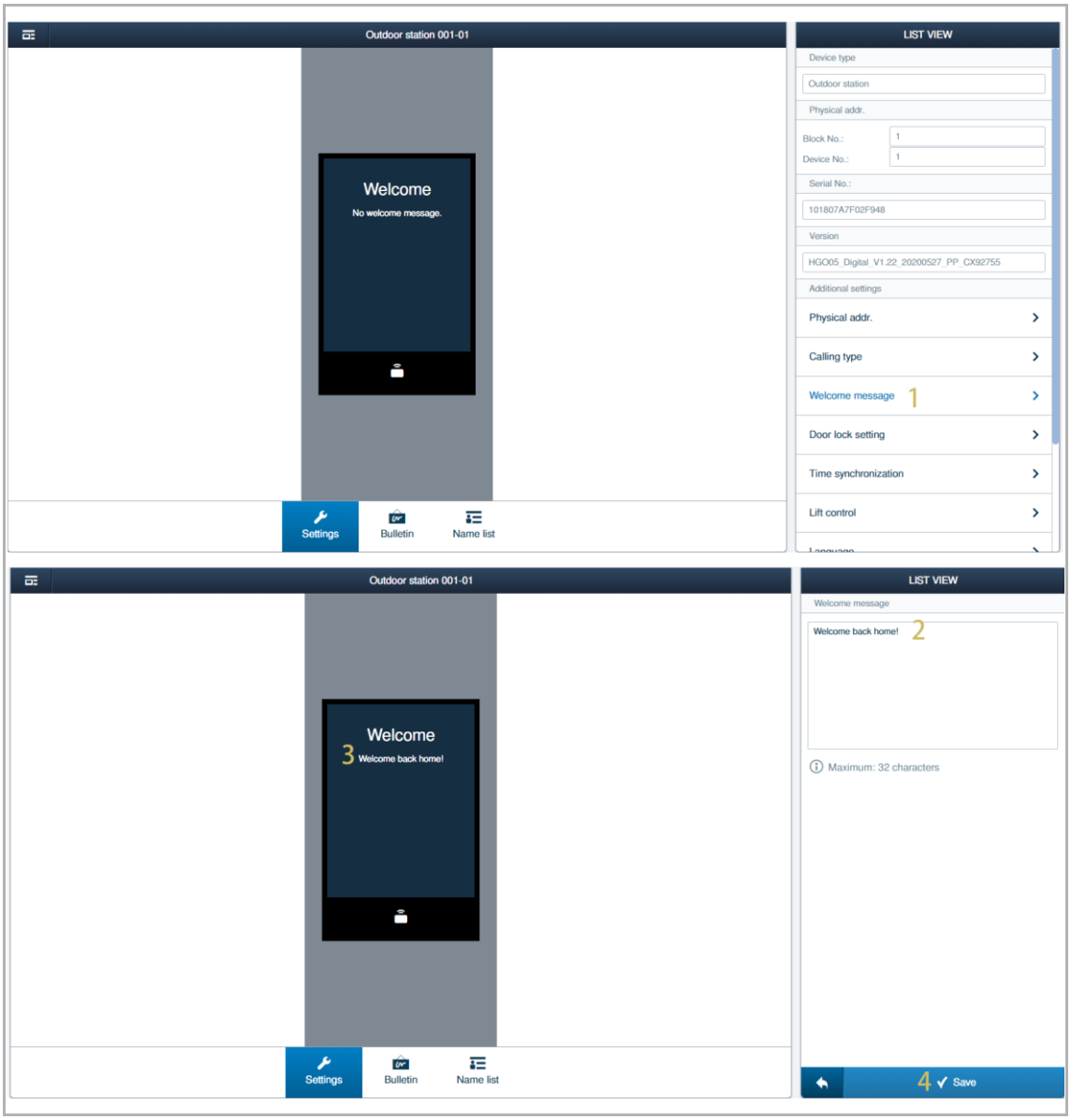
Volg de onderstaande stappen:

[1] Op het scherm van de buitenpost klikt u op "Welkomstbericht".

[2] Voer het bericht in (maximaal 32 tekens).

[3] Het logo resultaat weergegeven op het scherm van de buitenpost.

[4] Klik op "√" om op te slaan.



9.5.10 Gegevens ontwikkelaar beheren

Dit hoofdstuk is alleen van toepassing op de IP touch 5-buitenpost.

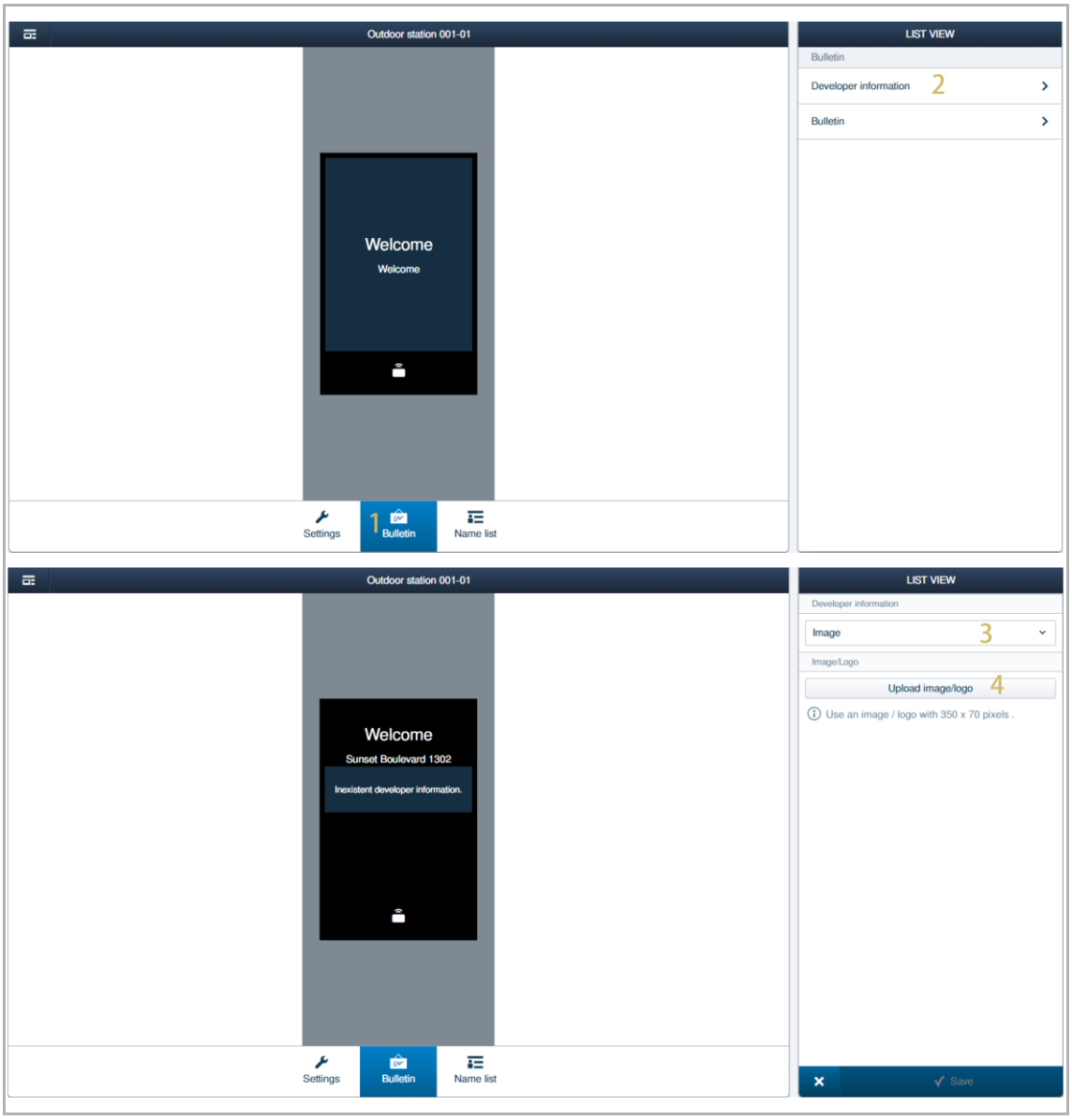
Volg de onderstaande stappen:

[1] Op het scherm van de buitenpost klikt u op "Bulletin".

[2] Klik op "Gegevens ontwikkelaar".

[3] Selecteer "Beeld" uit de keuzelijst.

[4] Klik op "Afbeelding/logo uploaden" om de afbeelding te selecteren (bijv. bedrijfslogo).



9.5.11 Bulletin beheren

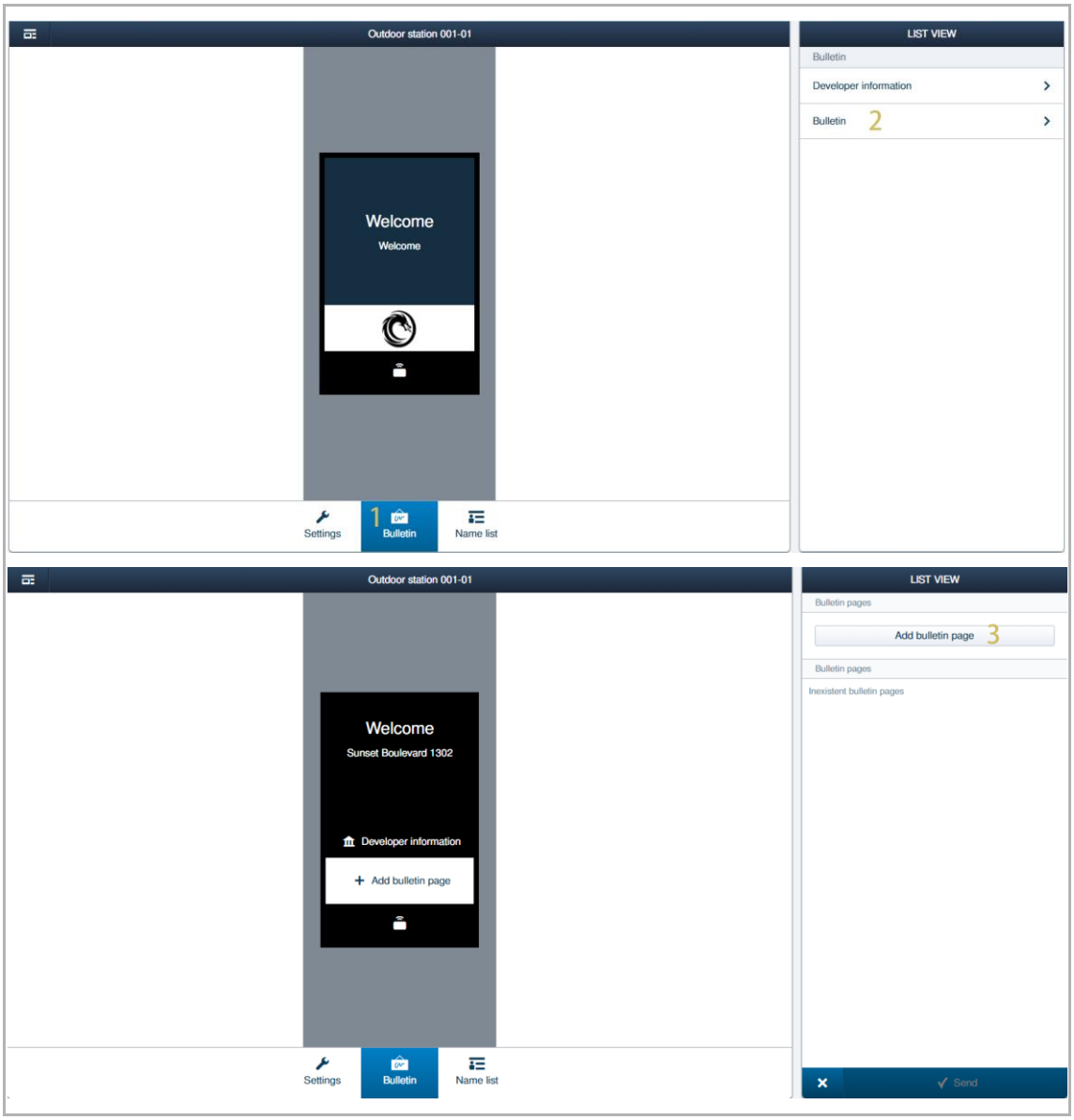
Dit hoofdstuk is alleen van toepassing op de IP touch 5-buitenpost.

Volg de onderstaande stappen:

[1] Op het scherm van de buitenpost klikt u op "Bulletin".

[2] Klik op "Bulletin".

[3] Klik op "Bulletin-pagina toevoegen" om een afbeelding te selecteren.



9.5.12 QR-code voor deblokkering beheren

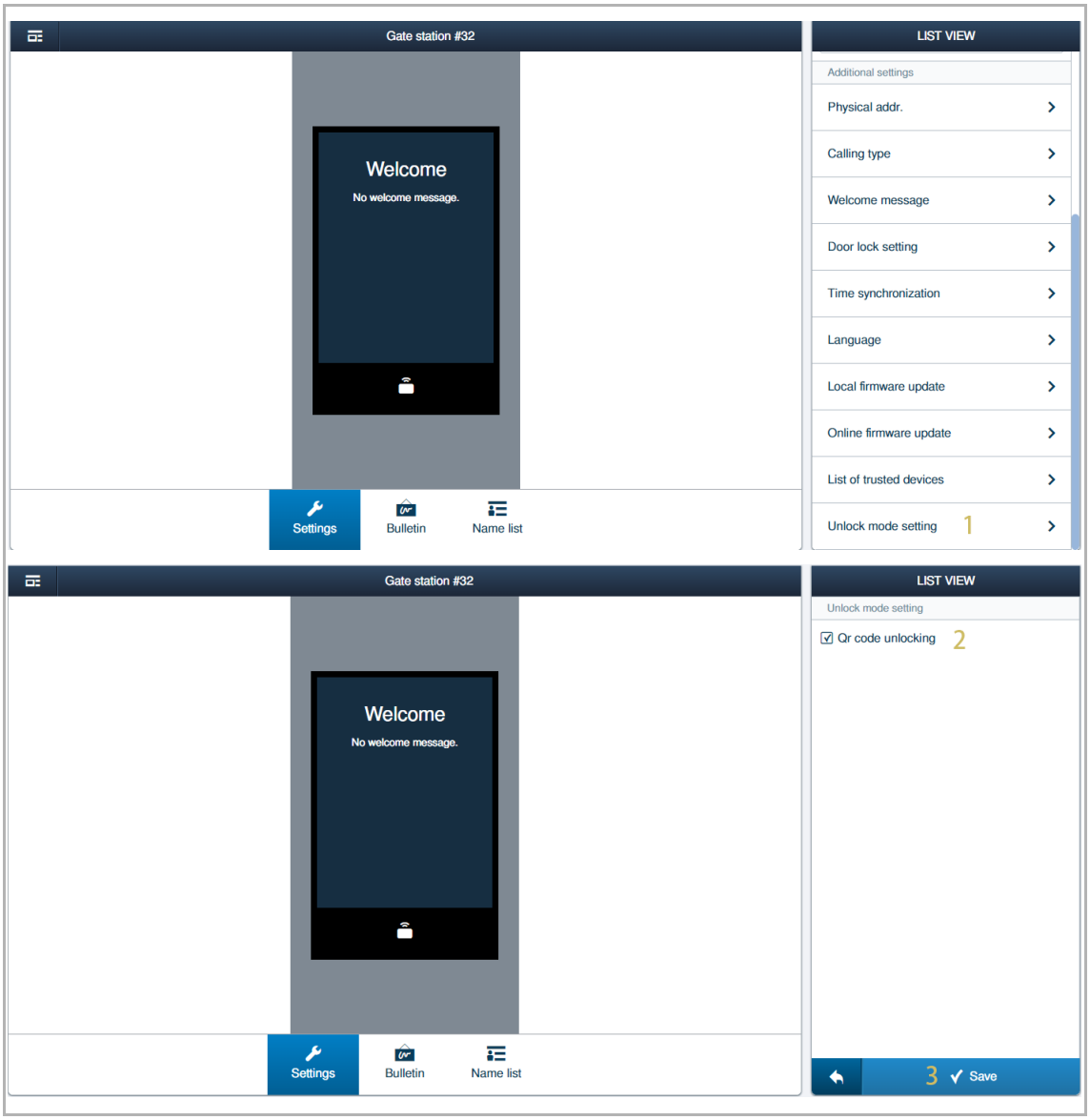
Dit hoofdstuk is alleen van toepassing op de IP touch 5-buitenpost.

Volg de onderstaande stappen:

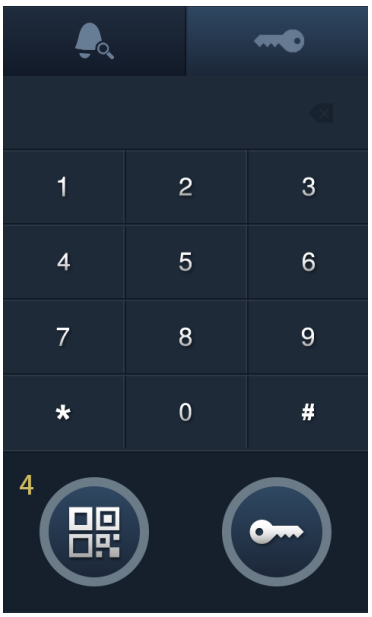
[1] Op het scherm van de buitenpost klikt u op "Instelling deblokeermodus".

[2] Vink het keuzevakje "QR-code deblokkering" aan om de functie te activeren.

[3] Klik op "√" om op te slaan.



[4] De QR-code wordt weergegeven op het deblokkeringsscherm van de IP touch 5-buitenpost.



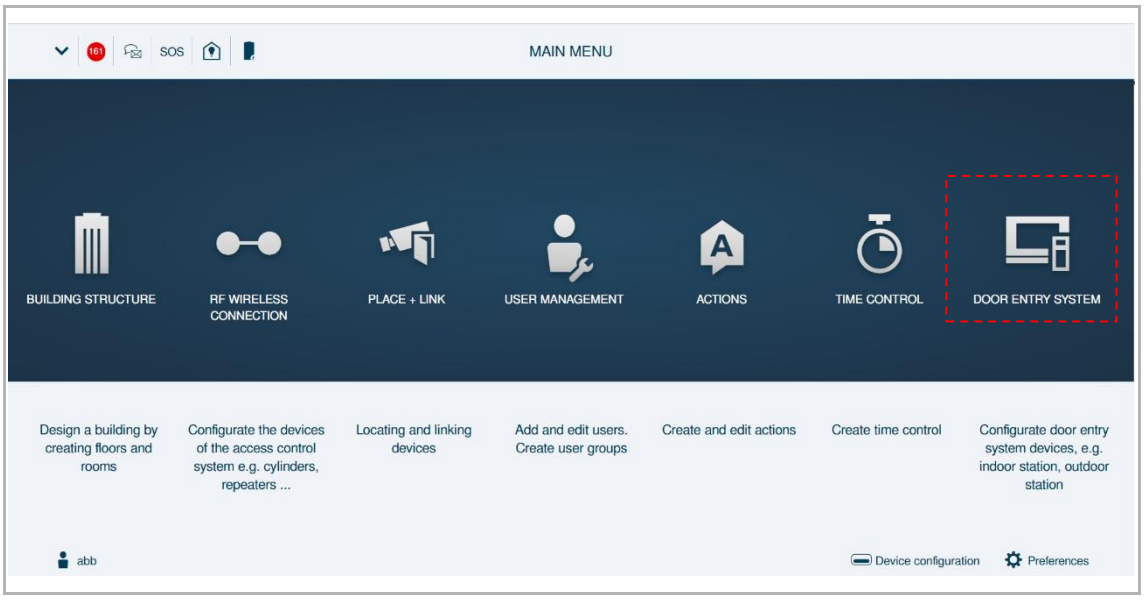
9.5.13 Firmware updaten

zie hoofdstuk 13.4 “Firmware updaten“ op pagina 272.

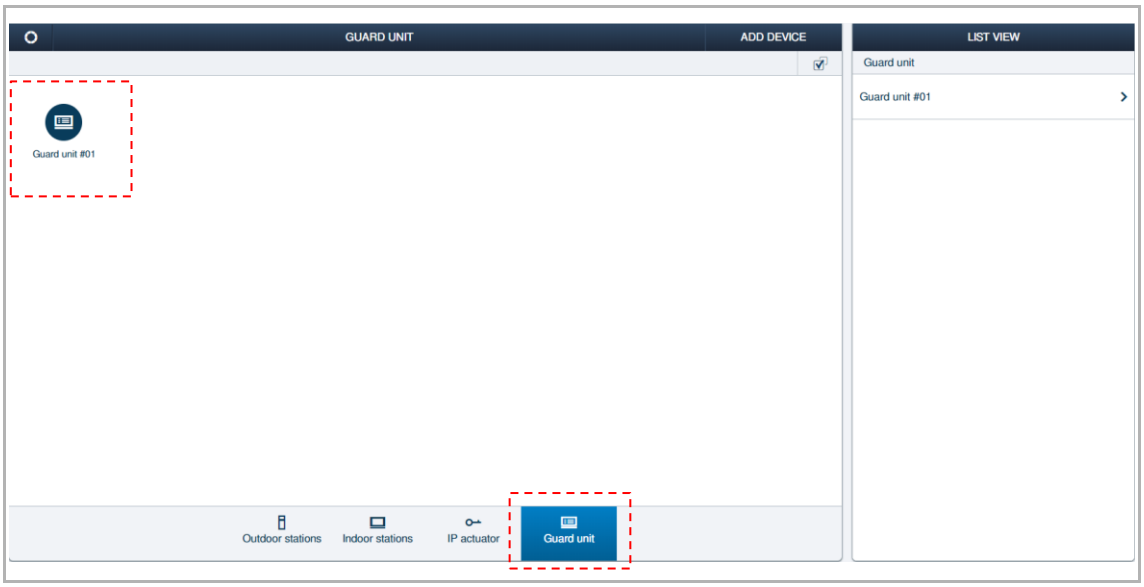
9.6 Portiercentrale configureren

Het portierscherm oproepen

Klik op het configuratiescherm op "Buiten-/binnenpost", "Portiercentrale" en vervolgens op "Portiercentrale" om het scherm "Portiercentrale" te openen.



Klik in het scherm "Buitenpost" en op de betreffende portiercentrale om het bijbehorende scherm te openen.



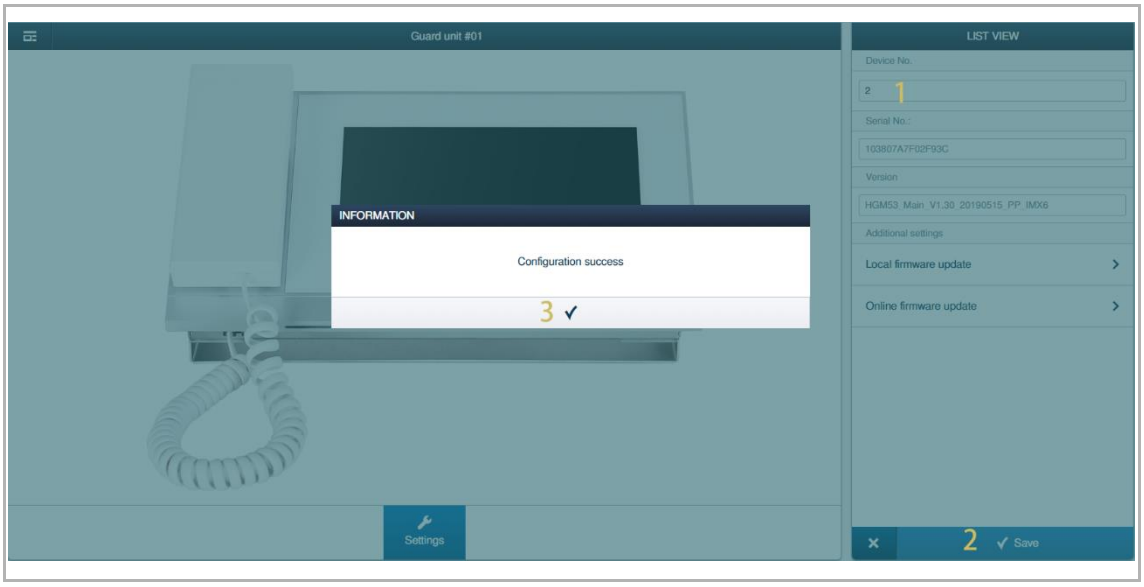
9.6.1 Apparaatnummer instellen

Volg de onderstaande stappen:

[1] Voer op het scherm van de portiercentrale een nieuw apparaatnummer in.

[2] Klik op "√" om op te slaan.

[3] Klik op "√" om te bevestigen.



9.6.2 Serienummer bekijken

Volg de onderstaande stappen:

[1] Op het scherm van de portiercentrale wordt het serienummer weergegeven. Het wordt aanbevolen om het serienummer te noteren voor verder gebruik.

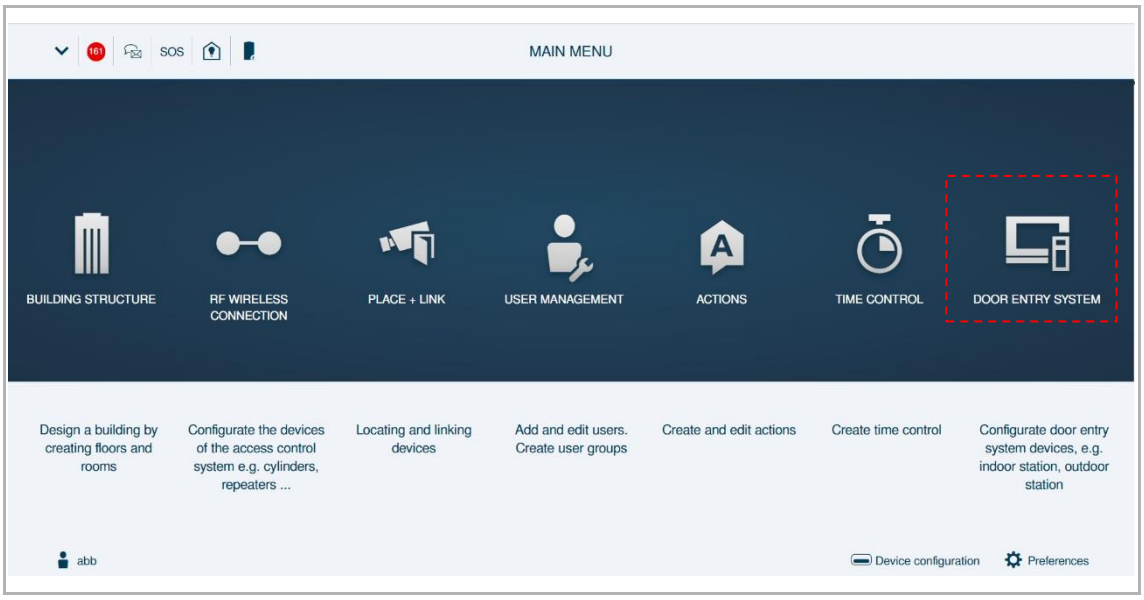
9.6.3 Firmware updaten

zie hoofdstuk 13.4 “Firmware updaten“ op pagina 272.

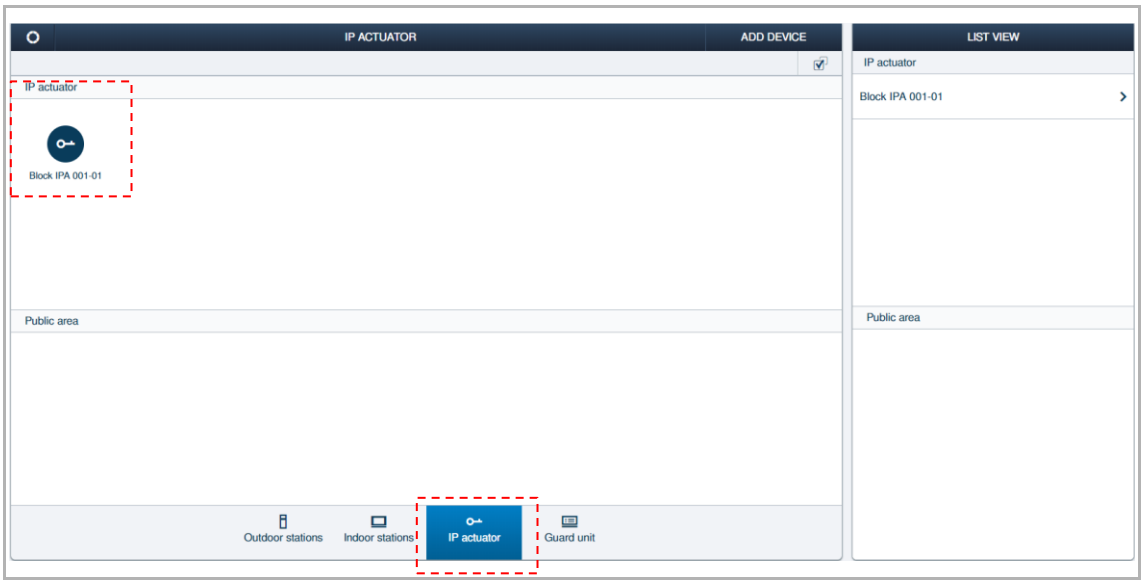
9.7 IP-aktor configureren

Het scherm van de IP-aktor oproepen

Klik op het configuratiescherm op "Buiten-/binnenpost" en vervolgens op "IP-aktor" om het scherm van de IP-aktor te openen.



Klik in het scherm "IP-aktor" en op de betreffende IP-aktor om het bijbehorende scherm te openen.



9.7.1 Serienummer bekijken

Volg de onderstaande stappen:

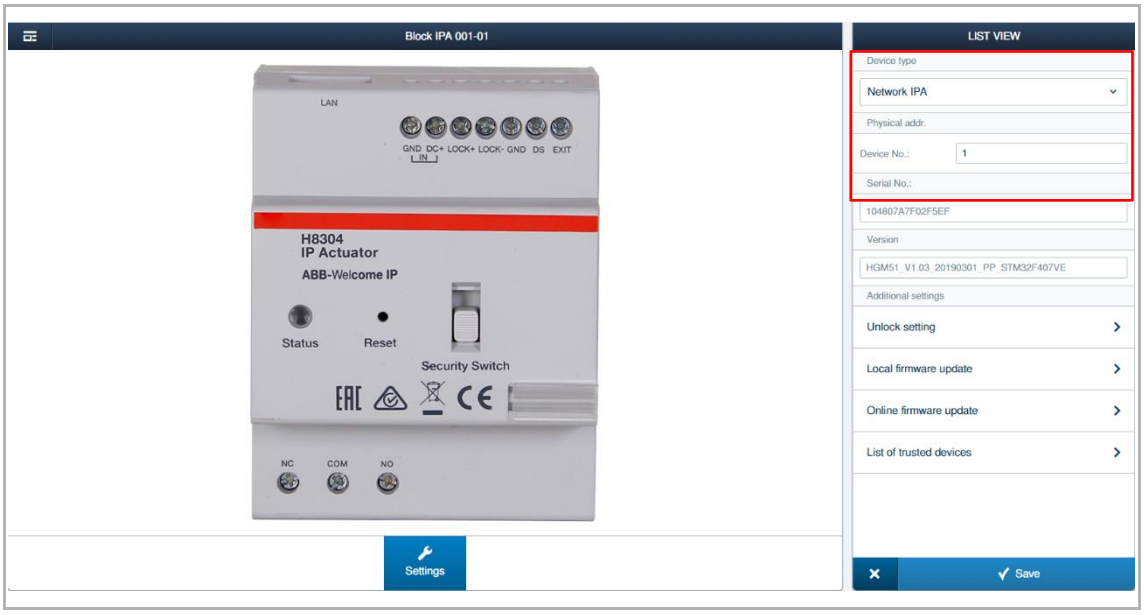
[1] Op het scherm van de IP-aktor wordt het serienummer weergegeven. Het wordt aanbevolen om het serienummer te noteren voor verder gebruik.

9.7.2 Fysiek adres beheren

Er kan worden gekozen uit 3 typen apparaten.

1. Netwerk-IPA

Als het "Apparaattype" is ingesteld op "Netwerk-IPA", moet u het apparaatnummer instellen (1-32).



2. Gebouw-IPA

Als het "Apparaattype" is ingesteld op "Gebouw-IPA", moet u het bloknummer (1-999) en het apparaatnummer instellen (1-32).

3. Private IPA

Als het "Apparaattype" is ingesteld op "Private IPA", moet u het bloknummer (1-999), het etagenummer (1-63), het ruimtenummer (1-32) en het apparaatnummer (1-32) instellen.

9.7.3 Ontgrendelinstelling

Volg de onderstaande stappen:

[1] Op het scherm van de IP-aktor klikt u op "Ontgrendelinstelling".

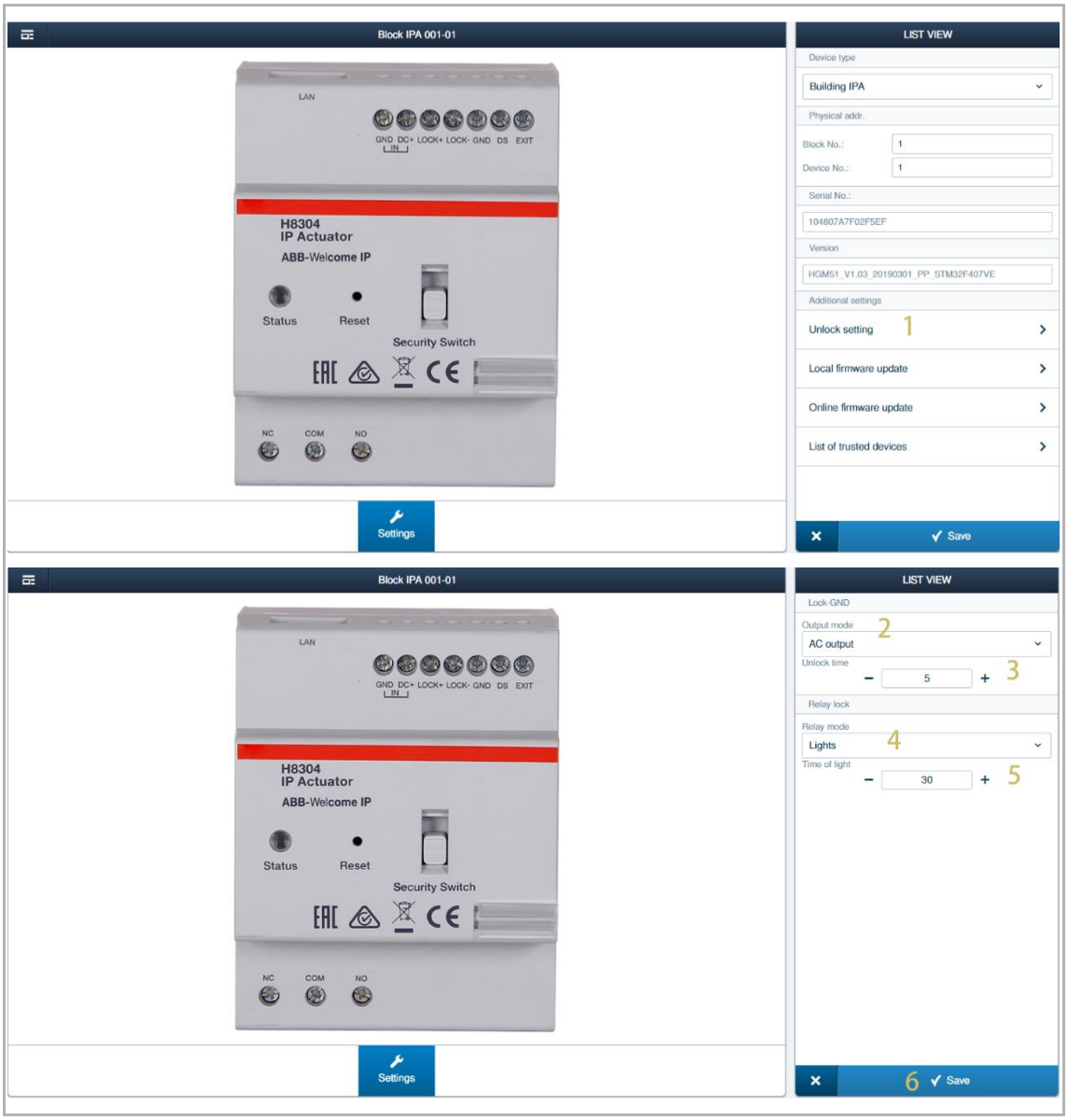
[2] Stel de uitgangsmodus voor "LOCK-GND" op "AC-uitgang", "DC-uitgang (NC)" of "DC-uitgang (NO)".

[3] Stel de deblokkeringstijd in voor "LOCK-GND".

[4] Stel de uitgangsmodus voor "Relaisblokkering" in op "Deblokkeren" of "Licht".

[5] Stel de deblokkeringstijd in voor "Relaisblokkering".

[6] Klik op "√" om op te slaan.



9.7.4 Vertrouwde apparaten beheren

zie hoofdstuk 9.3.2 “Vertrouwde apparaten voor de IP-aktor beheren“ op pagina 69.

9.7.5 Aan buitenpost gerelateerde IP-aktor deblokkeren

Volg de onderstaande stappen:

[1] Op het scherm van de buitenpost klikt u op "Inst. deurvergrendeling".

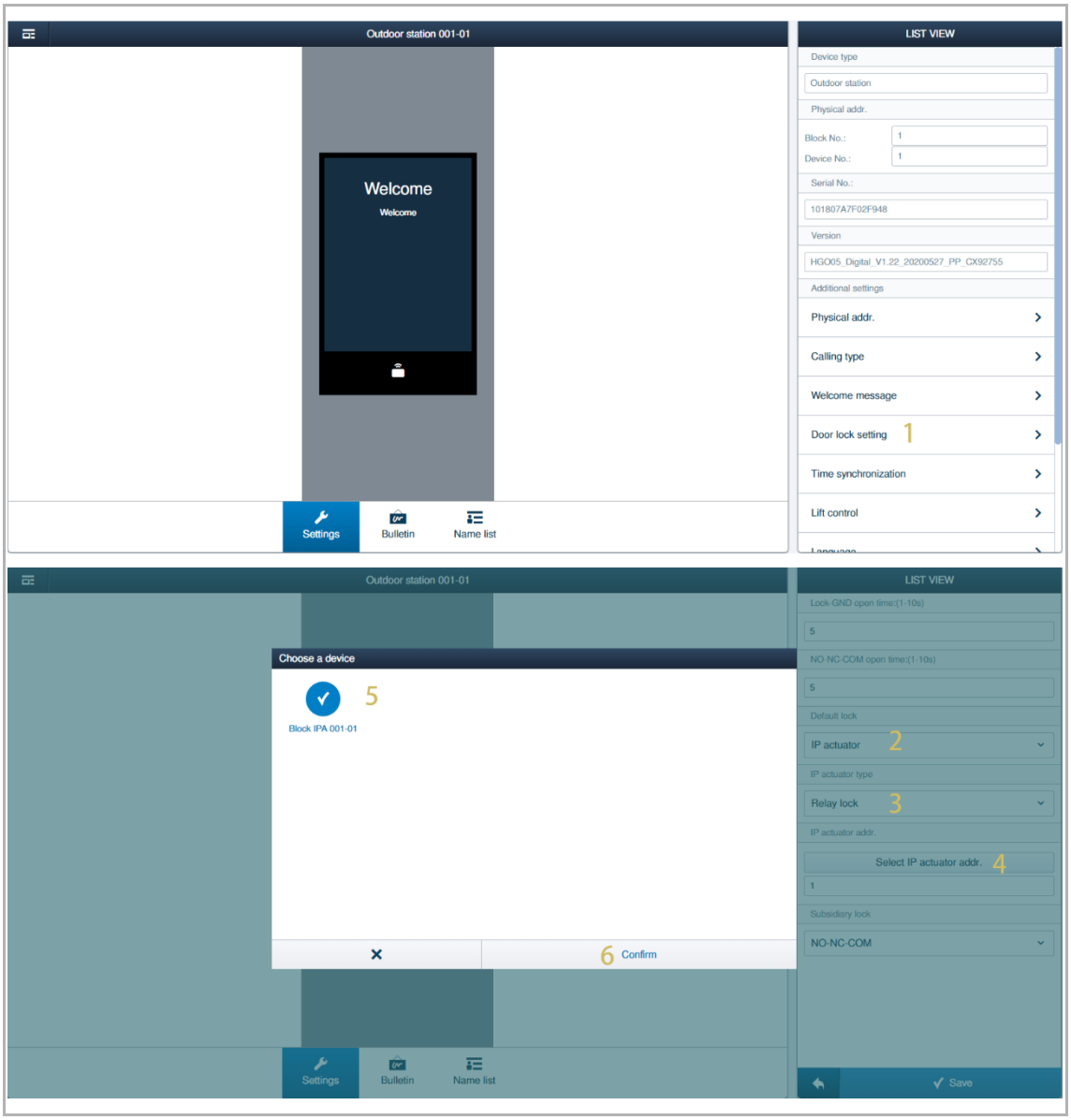
[2] Stel het deurtype in op "IP-aktor.

[3] Selecteer het type IP-aktor in op "Power lock" of "Relaisblokkering".

[4] Klik op "Selecteer IP-aktoradres".

[5] Klik om de betreffende IP-aktor te selecteren.

[6] Klik op "Bevestigen".

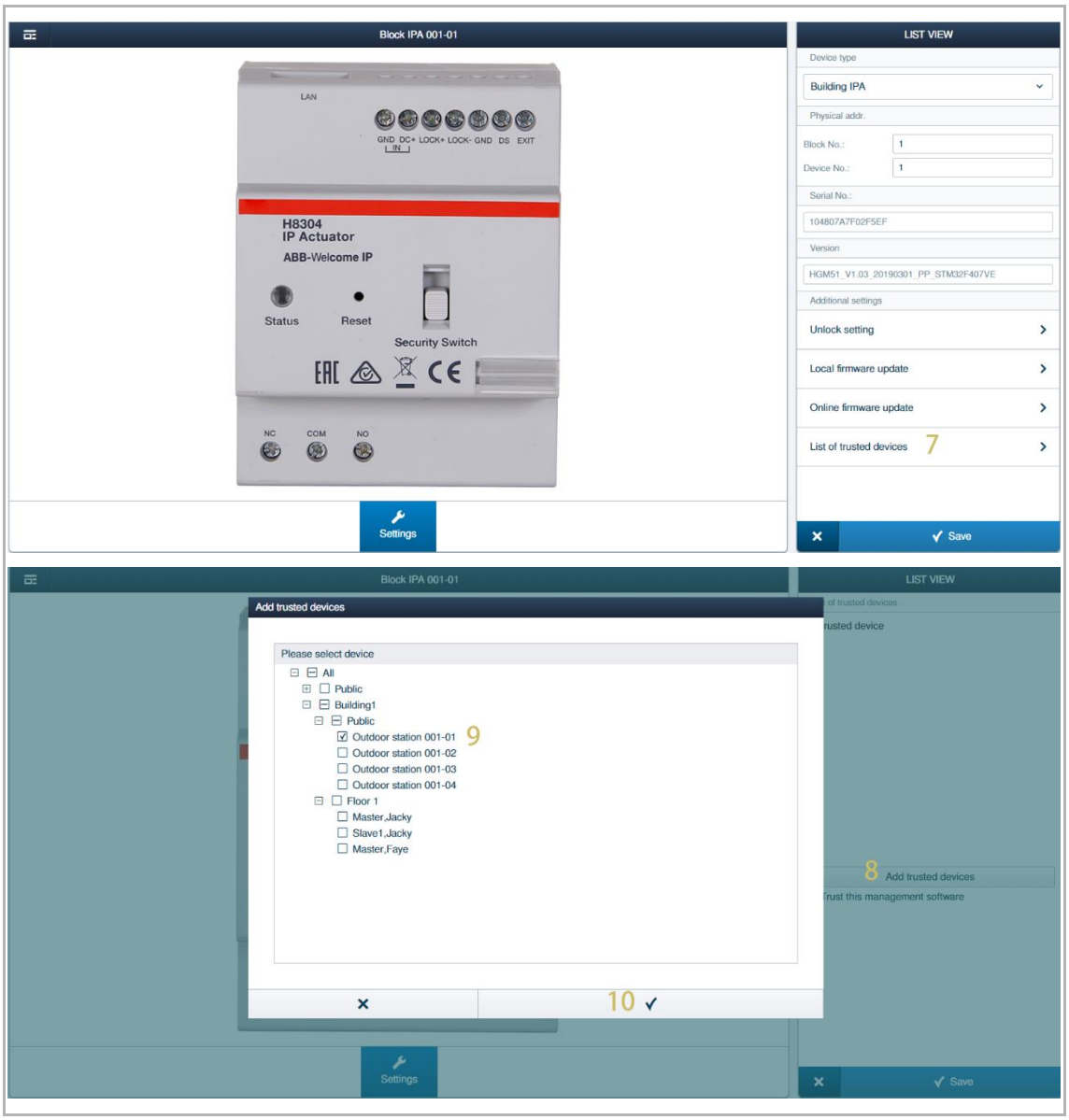


[7] Op het scherm van de IP-aktor klikt u op "Lijst met vertrouwde apparaten".

[8] Klik op "Vertr. app.toevoegen".

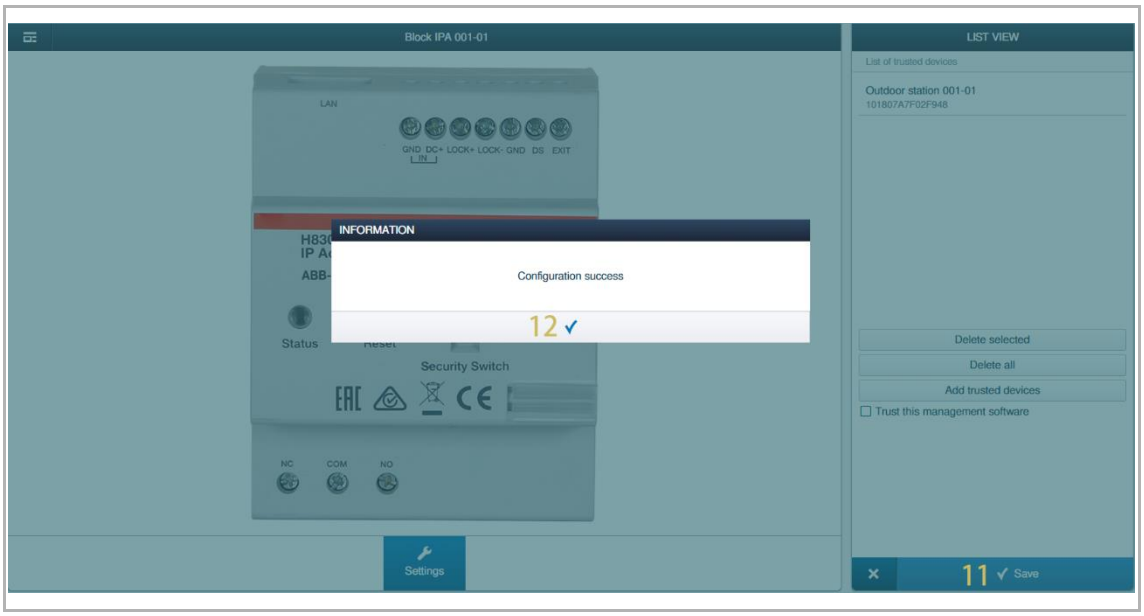
[9] Klik op de gewenste buitenpost.

[10]Klik op "√" om op te slaan.



[11]Klik op "√" om op te slaan.

[12]Klik op "√" om te bevestigen.



9.8 Apparaten verwijderen

9.8.1 Apparaten één voor één verwijderen

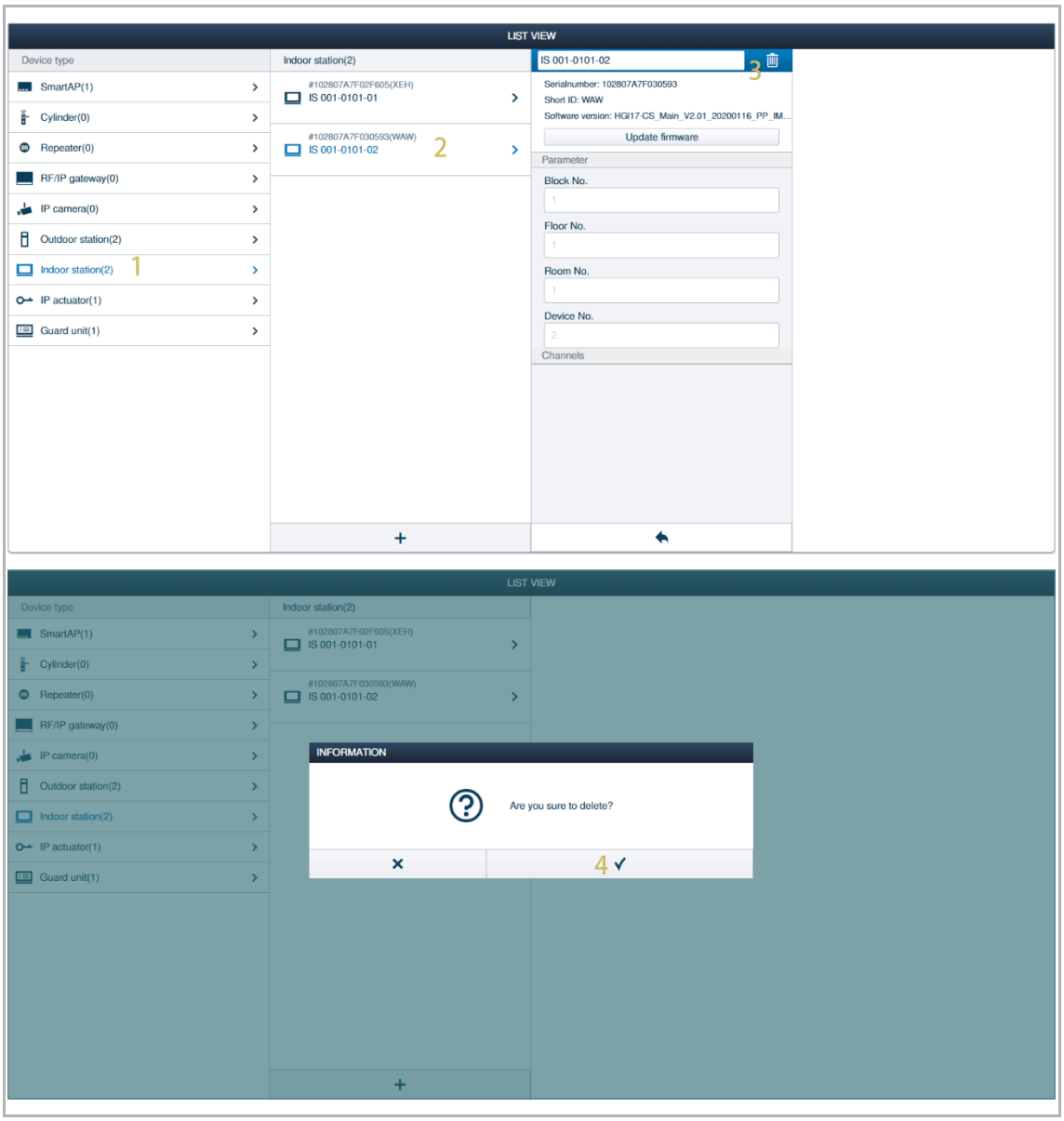
Volg de onderstaande stappen:

[1] Klik in het scherm "Apparaatconfiguratie" klikt u op een apparaat (bijv. "Binnenpost").

[2] Klik op het betreffende apparaat (bijvoorbeeld "Binnenpost 2").

[3] Klik op " ".

[4] Klik op "√" om te bevestigen.



9.8.2 Apparaten in batches verwijderen

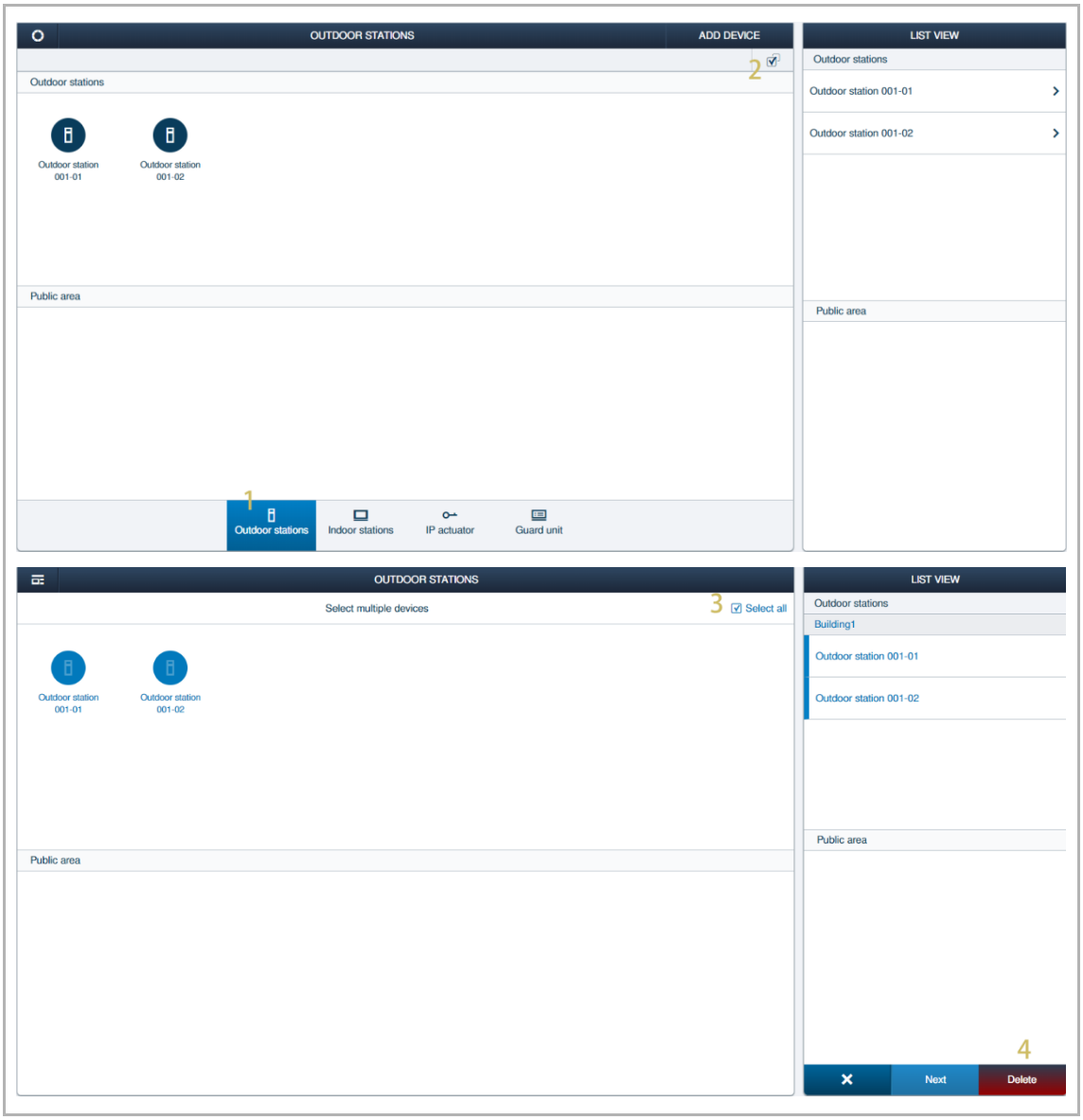
Volg de onderstaande stappen:

[1] Klik in het scherm "Apparaatconfiguratie" klikt u op buiten-/binnenpost (bijv. "Buitenpost").

[2] Klik op " ".

[3] Klik op "Alles selecteren" om alle apparaten te selecteren of klik één voor één op het betreffende apparaat om meerdere apparaten te selecteren.

[4] Klik op "Wissen".



10 AccessControl-apparaten bedienen

10.1 AccessControl-topologie

Scenario 1: Een klein aantal elektronische slotcilinders wordt gebruikt bij een korte afstand tussen de apparaten.

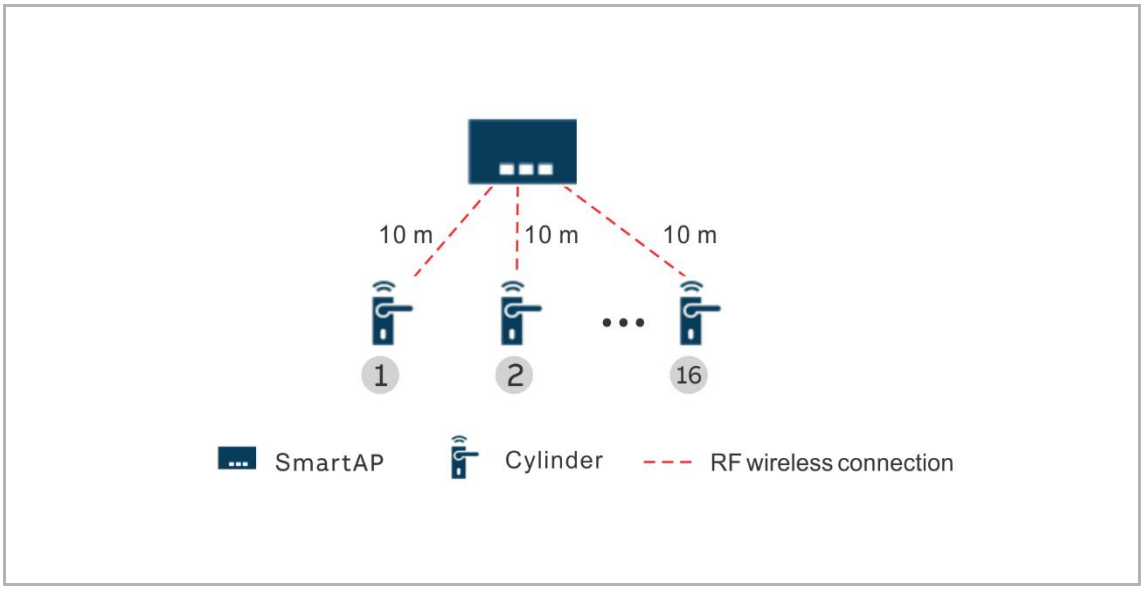
1. Voorwaarden

- Het aantal elektronische slotcilinders dat door het "Smart Access Point" wordt bediend bedraagt ≤ 16 stuks.
- De afstand van de verste elektronische slotcilinder tot "Smart Access Point" bedraagt ≤ 10 meter.

2. Capaciteit

- Het radiobereik tussen de RF-apparaten bedraagt ≤ 10 meter.
- Er kunnen 16 elektronische slotcilinders worden bediend via één "Smart Access Point".

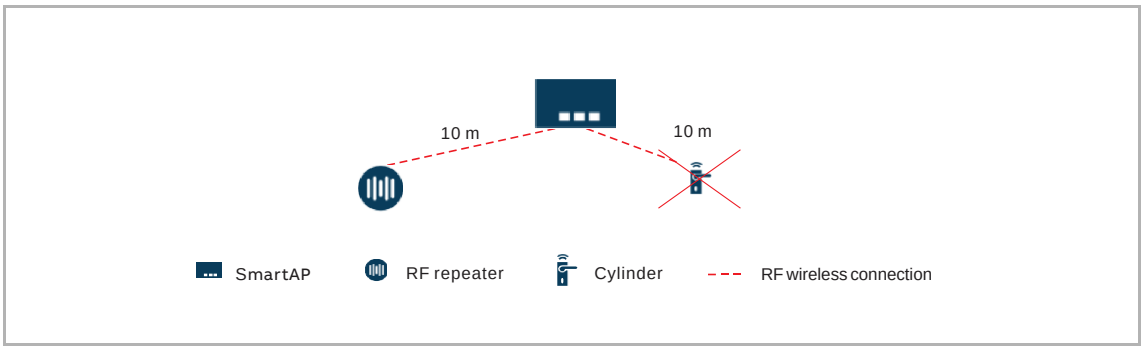
3. Topologie



Scenario 2: Een klein aantal elektronische slotcilinders wordt gebruikt bij een gemiddelde afstand tussen de apparaten.

1. Voorwaarden

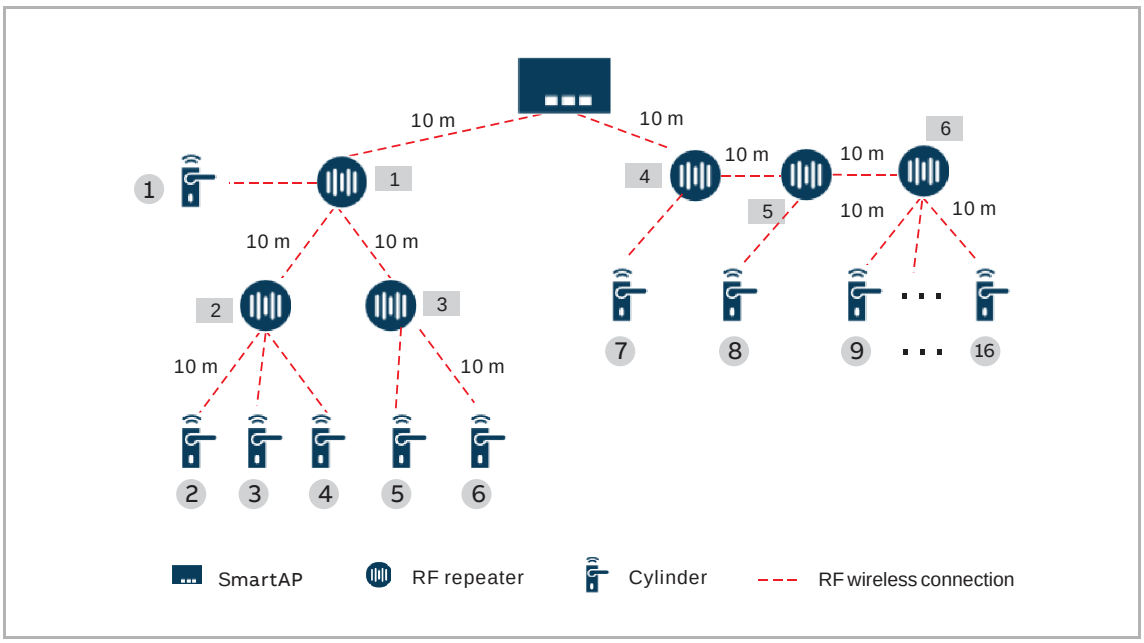
- Het aantal elektronische slotcilinders dat door het "Smart Access Point" wordt bediend bedraagt ≤ 16 eenheden.
- De afstand van de verste elektronische slotcilinder tot "Smart Access Point" bedraagt ≤ 40 meter.
- RF-repeater is nodig om het radiobereik te vergroten, elke RF-repeater vergroot het radiobereik met 10 meter.
- Een elektronische slotcilinder en een RF-repeater kunnen niet tegelijkertijd slave-apparaten van het "Smart Access Point" zijn.



2. Capaciteit

- Het radiobereik tussen de RF-apparaten bedraagt ≤ 10 meter.
- Er kunnen 16 elektronische slotcilinders worden bediend via één "Smart Access Point".
- Er kunnen 6 RF-repeaters worden bediend via één "Smart Access Point".
- Er kunnen maximaal 3 RF-repeaters in serie worden aangesloten op het "Smart Access Point" in een radiolijn.
- Elke RF-repeater kan tot 2 slave-repeaters hebben.
- De elektronische slotcilinders kunnen vrij worden toegewezen aan de RF-repeater in de radiolijn.
- Het maximale radiobereik tussen een elektronische slotcilinder en het "Smart Access Point" bedraagt 40 meter.

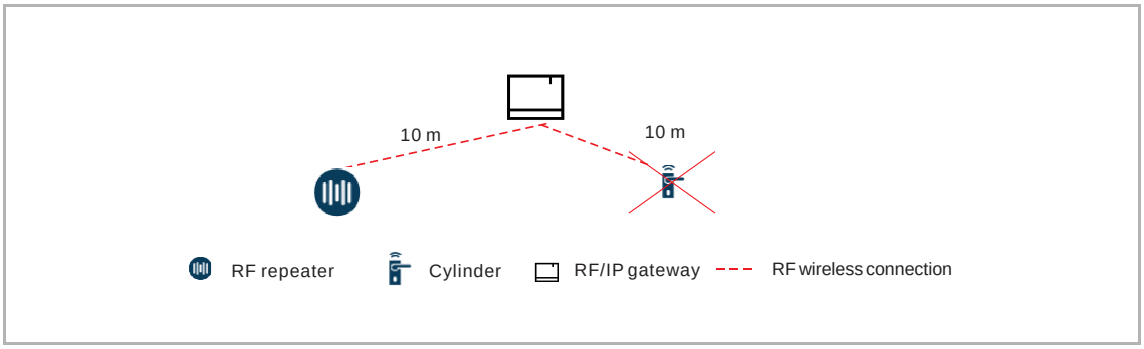
3. Topologie


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

Scenario 3: Een groot aantal elektronische slotcilinders wordt gebruikt bij een lange afstand tussen de apparaten.

1. Voorwaarden

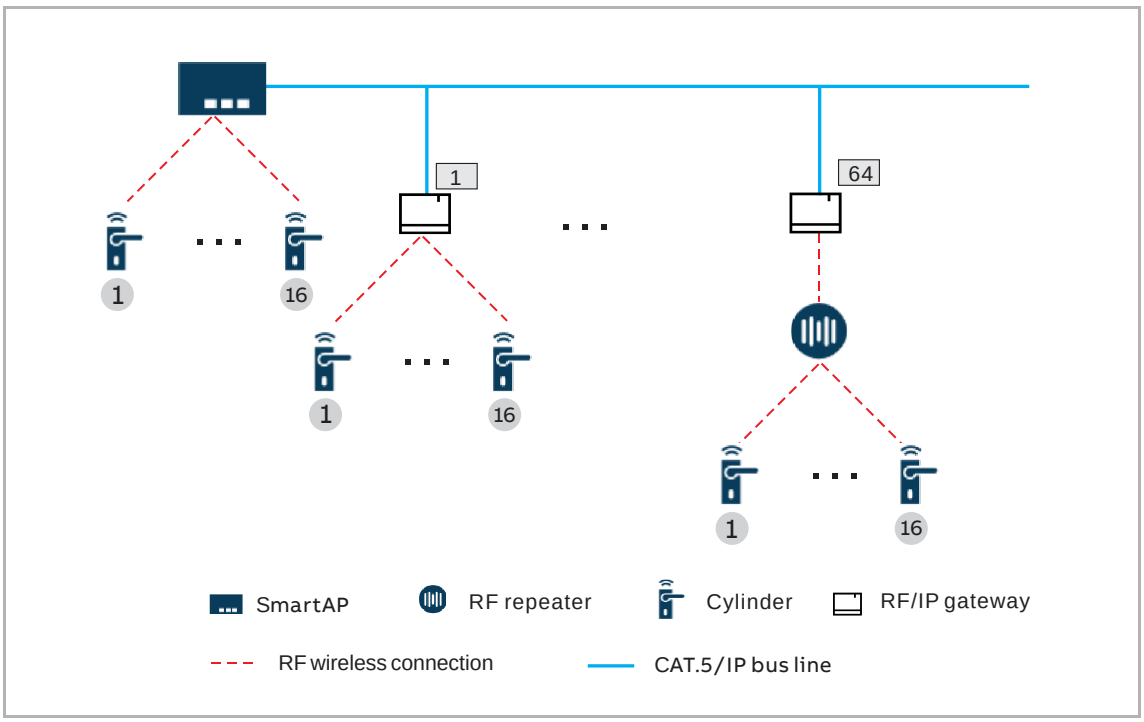
- Het aantal elektronische slotcilinders dat door het "Smart Access Point" wordt bediend bedraagt ≤ 600 eenheden.
- Er is een RF/IP-gateway is nodig om het radiobereik uit te breiden, elke RF/IP-gateway kan gezien worden als het "Smart Access Point" in een radiolijn.
- Een elektronische slotcilinder en een RF-repeater kunnen niet tegelijkertijd slave-apparaten van een RF/IP-gateway zijn.



2. Capaciteit

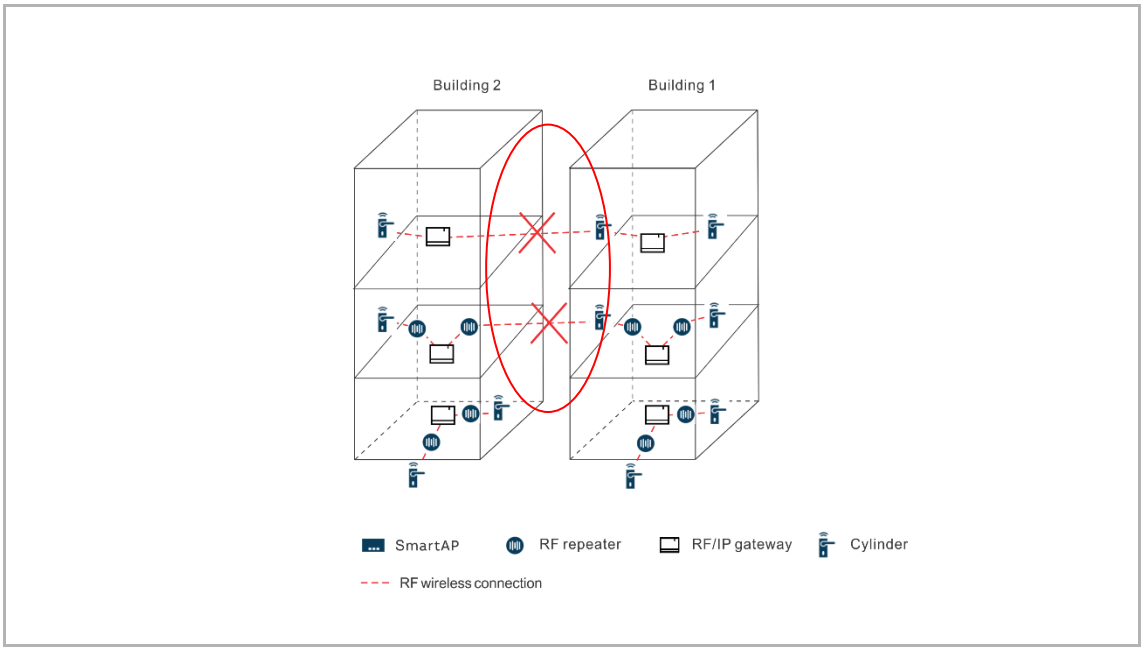
- Het radiobereik tussen de RF-apparaten bedraagt ≤ 10 meter.
- Er kunnen 64 RF/IP-gateways worden bediend via één "Smart Access Point".
- Door de beperkte systeemprestaties kunnen 500 elektronische slotcilinders worden bediend via een "Smart Access Point".
- Er kunnen 16 elektronische slotcilinders worden bediend via één RF/IP-gateway.
- Er kunnen 6 RF-repeaters worden bediend via één RF/IP-gateway.
- Er kunnen maximaal 3 RF-repeaters in serie worden aangesloten op één RF/IP-gateway in een radiolijn.
- Elke RF-repeater kan tot 2 slave-repeaters hebben.
- De elektronische slotcilinders kunnen vrij worden toegewezen aan de RF-repeater in de radiolijn.

3. Topologie



Opmerking

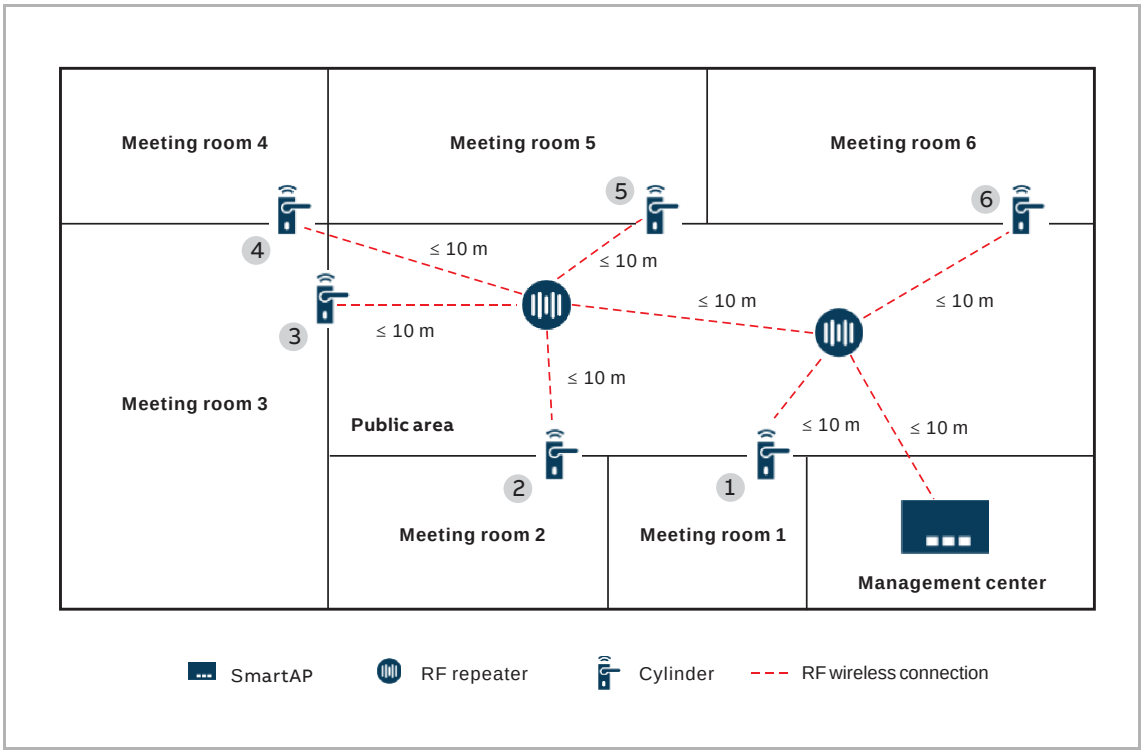
De elektronische slotcilinder kan niet buiten gebouwen om worden aangesloten (zie onderstaand schema).



Demonstratie

Deze demonstratie is bedoeld om u vertrouwd te maken met de werking van AccessControl-apparaten.

U dient uw handelingen aan te passen wanneer u een echt project implementeert.



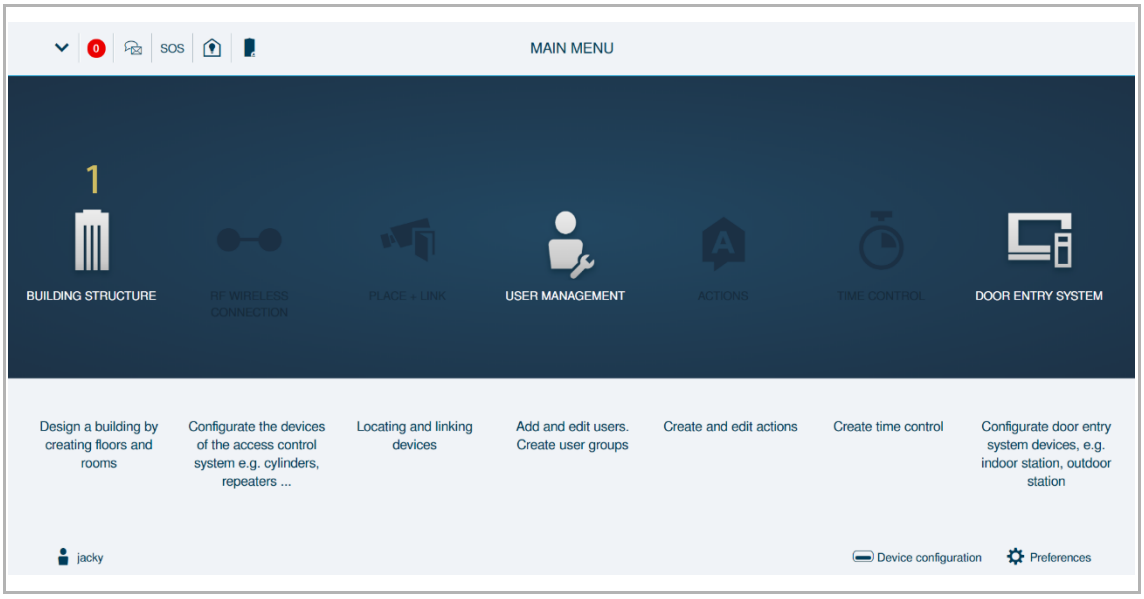
10.2 Een gebouw maken

10.2.1 Een gebouw maken via "Smart Access Point"

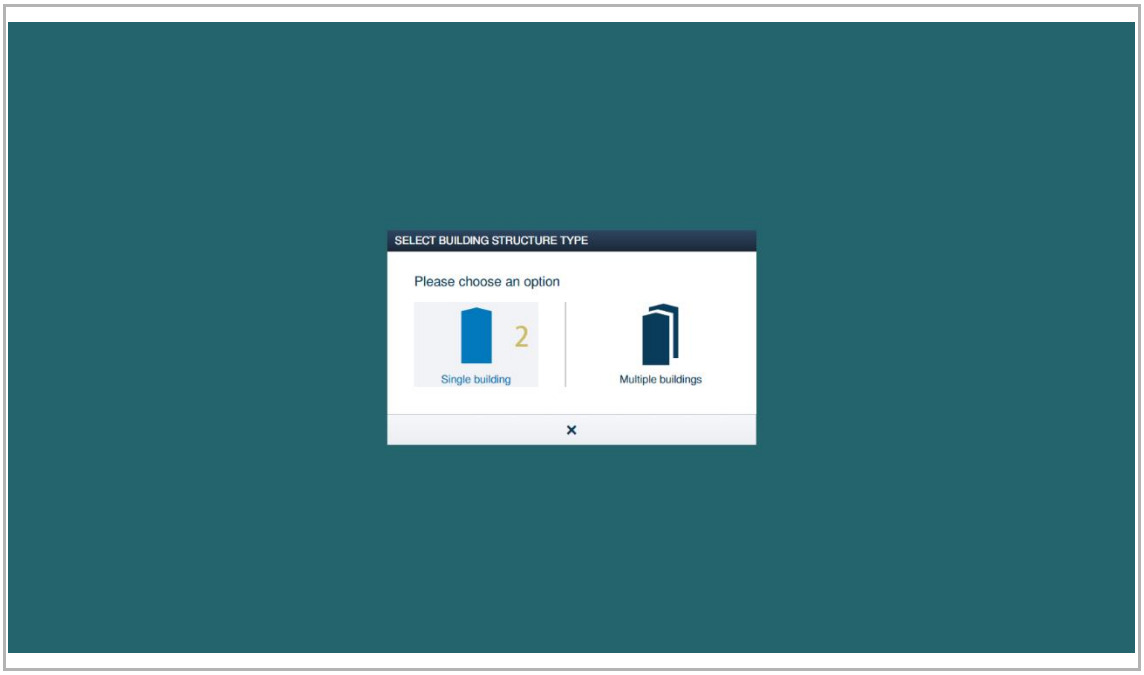
De volgende handelingen zijn gebaseerd op demonstratie 1.

Volg de onderstaande stappen:

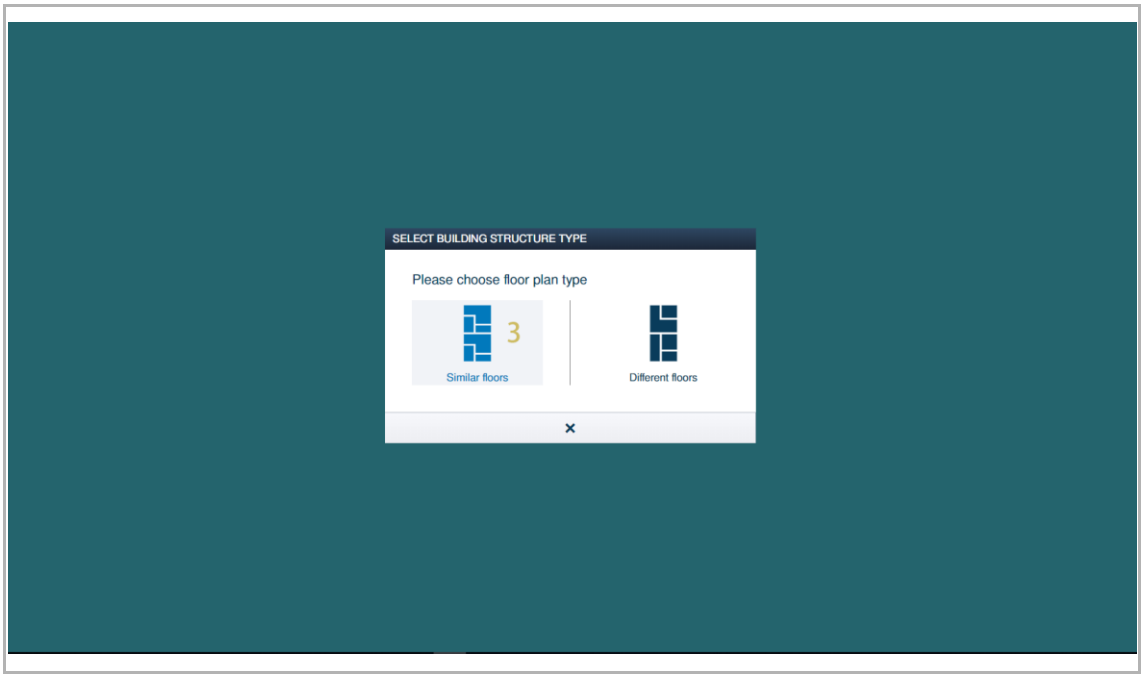
[1] Klik in het configuratiescherm op "Gebouwstructuur".



[2] Klik op "Individueel gebouw".



[3] Klik op "Soortgelijke etages".



[4] Sleep het gebouw-symbool naar de plattegrond.

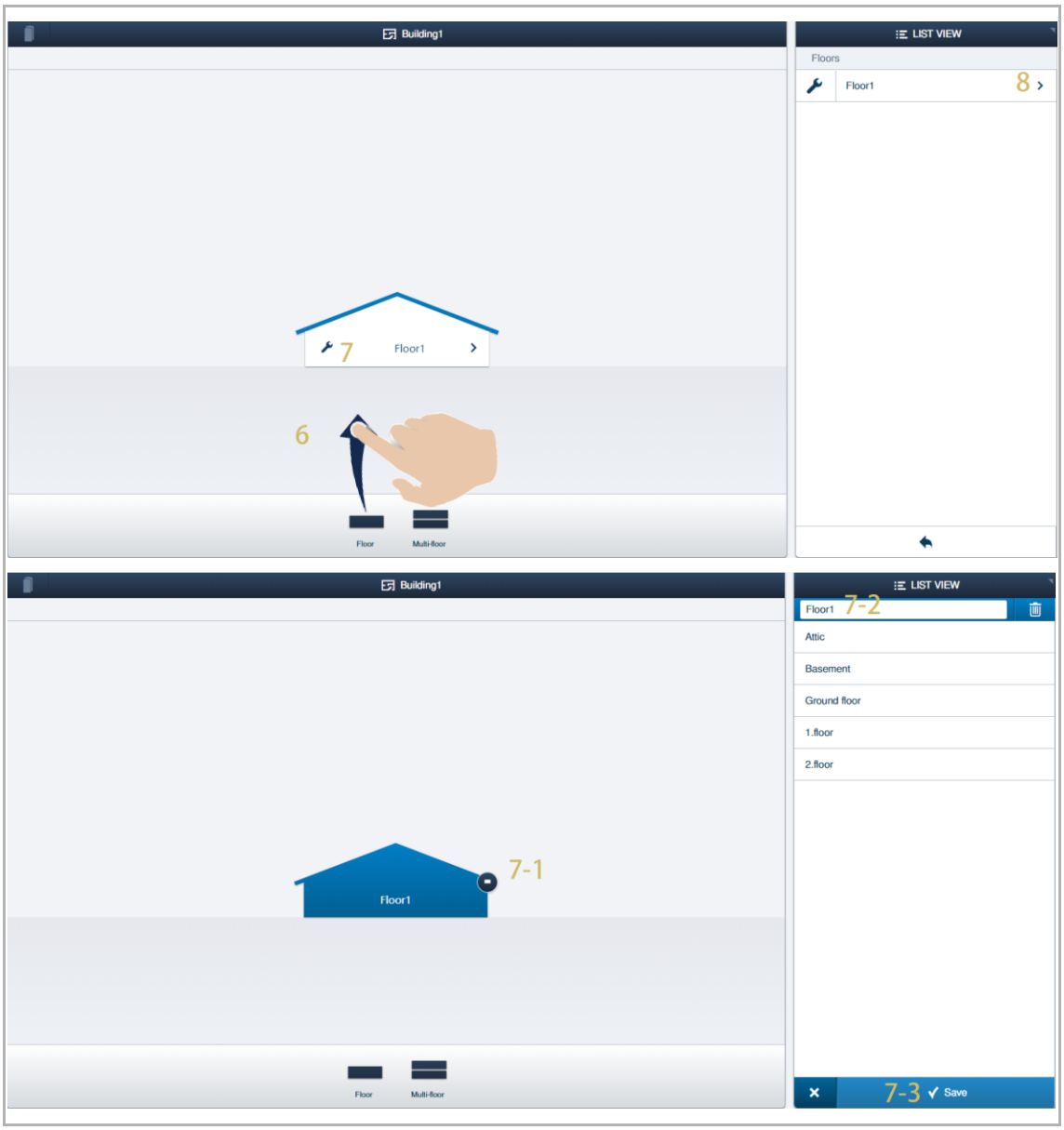
[5] Klik op ">" om door te gaan.

[6] Sleep het etage-symbool naar de plattegrond.

[7] Klik op " " om de etage te bewerken (optioneel).

- 7-1, klik op het symbool om de etagevorm te veranderen.
- 7-2, de naam van de etage.
- 7-3, sla de wijziging op.

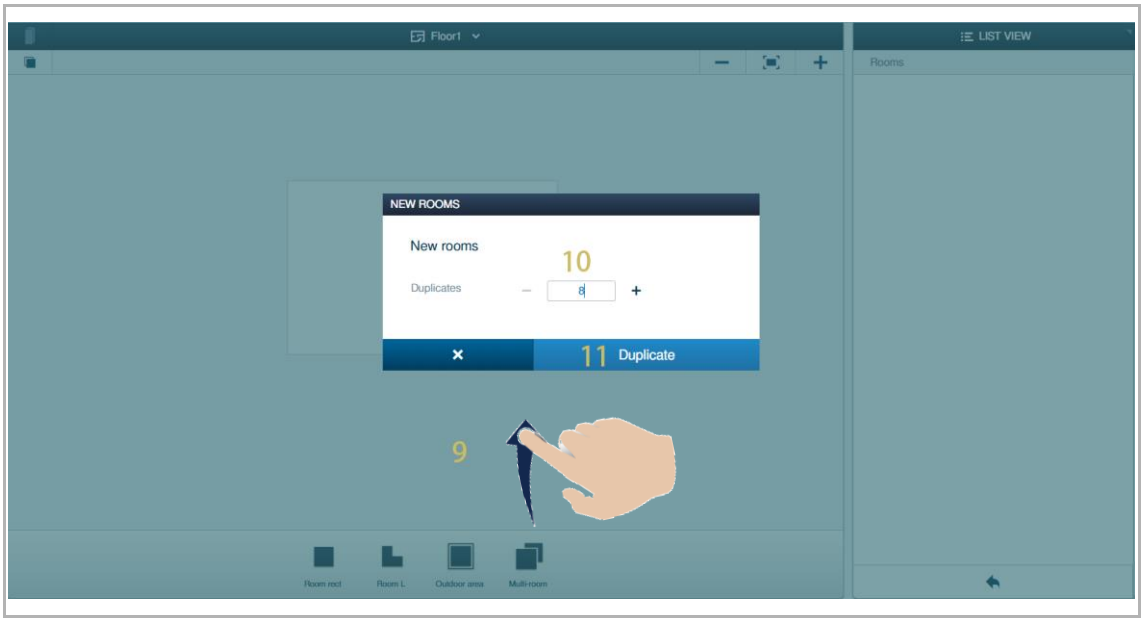
[8] Klik op ">" om door te gaan.



[9] Sleep het symbool voor meerdere kamers naar de plattegrond.

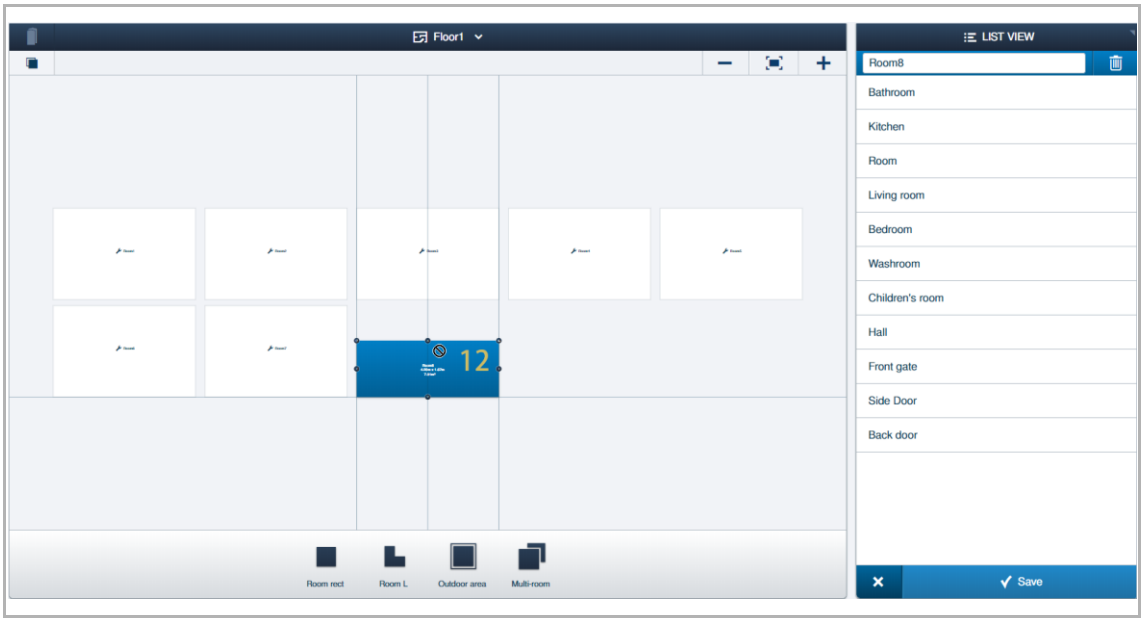
[10]Voer het aantal kamers in (bijv. "8" voor demonstratie 1).

[11]Klik op "Kopiëren".



[12]Klik op de ruimte om de vorm van de ruimte aan te passen.

- Klik op het symbool " " om de hoogte of de breedte van de vorm van de ruimte te veranderen.
- Klik op het symbool " " om de vorm van de ruimte te herstellen.
- Klik op het symbool " " om de vorm van de ruimte te veranderen van "Rechthoek" naar "L".
- Klik op het symbool " " om de vorm van de ruimte te veranderen van "L" naar "Rechthoek".



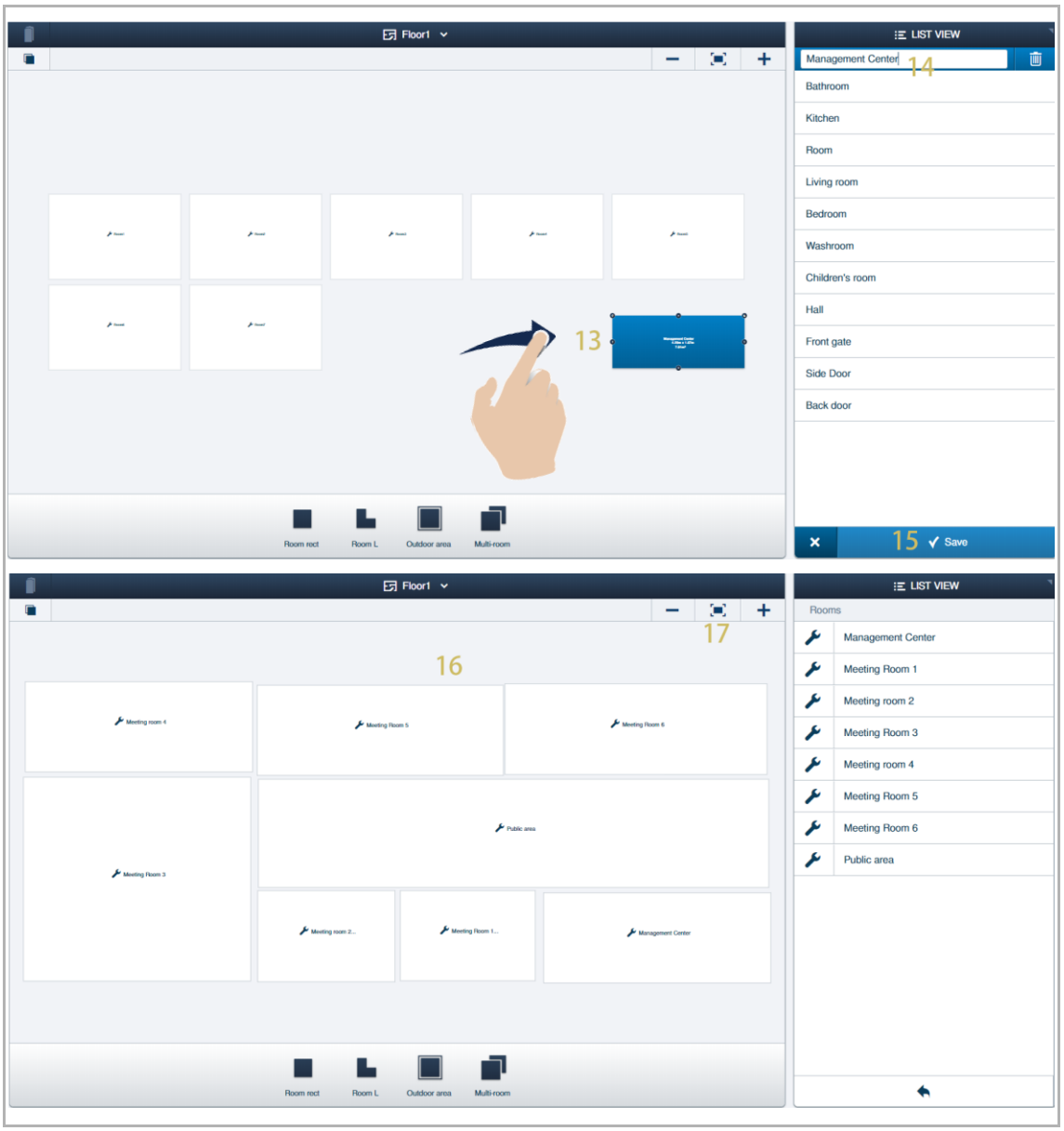
[13]Sleep de ruimte om deze te verplaatsen.

[14]Wijzig de naam van de ruimte.

[15]Klik op "√" om op te slaan.

[16]Herhaal de stappen van 12~15 om andere ruimtes één voor één te veranderen.

[17]Als laatste klikt u op "" om alle ruimte op de plattegrond weer te geven.

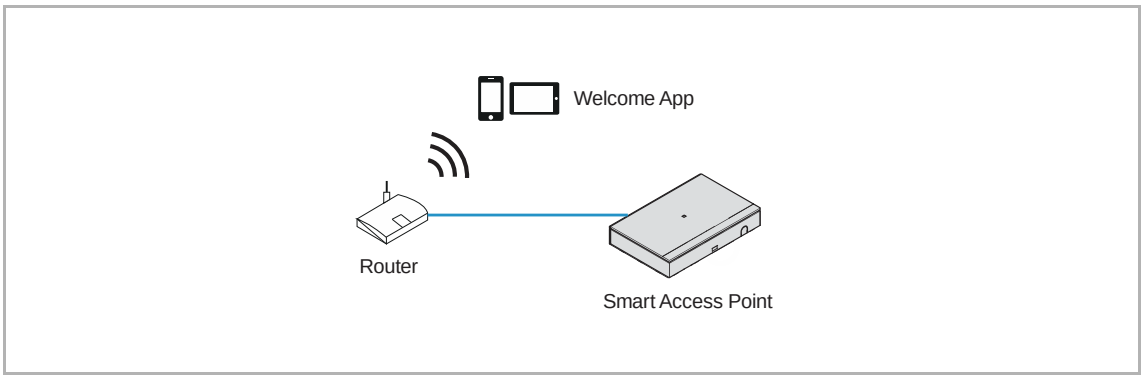


10.2.2 Een gebouw maken via de Welcome-app

"Smart Access Point" kan het gebouw dat is aangemaakt op Welcome-app importeren. U kunt één gebouw eenmalig of meerdere gebouwen in batches importeren.

Voorwaarde

- Welkom-app moet zich in hetzelfde netwerk bevinden als "Smart Access Point".
- Het gebouw is gemaakt in de Welcome-app. Zie voor meer details de producthandleiding voor de Welcome-app.



Importregel

De structuur van het gebouw wordt overschreven volgens de onderstaande regels:

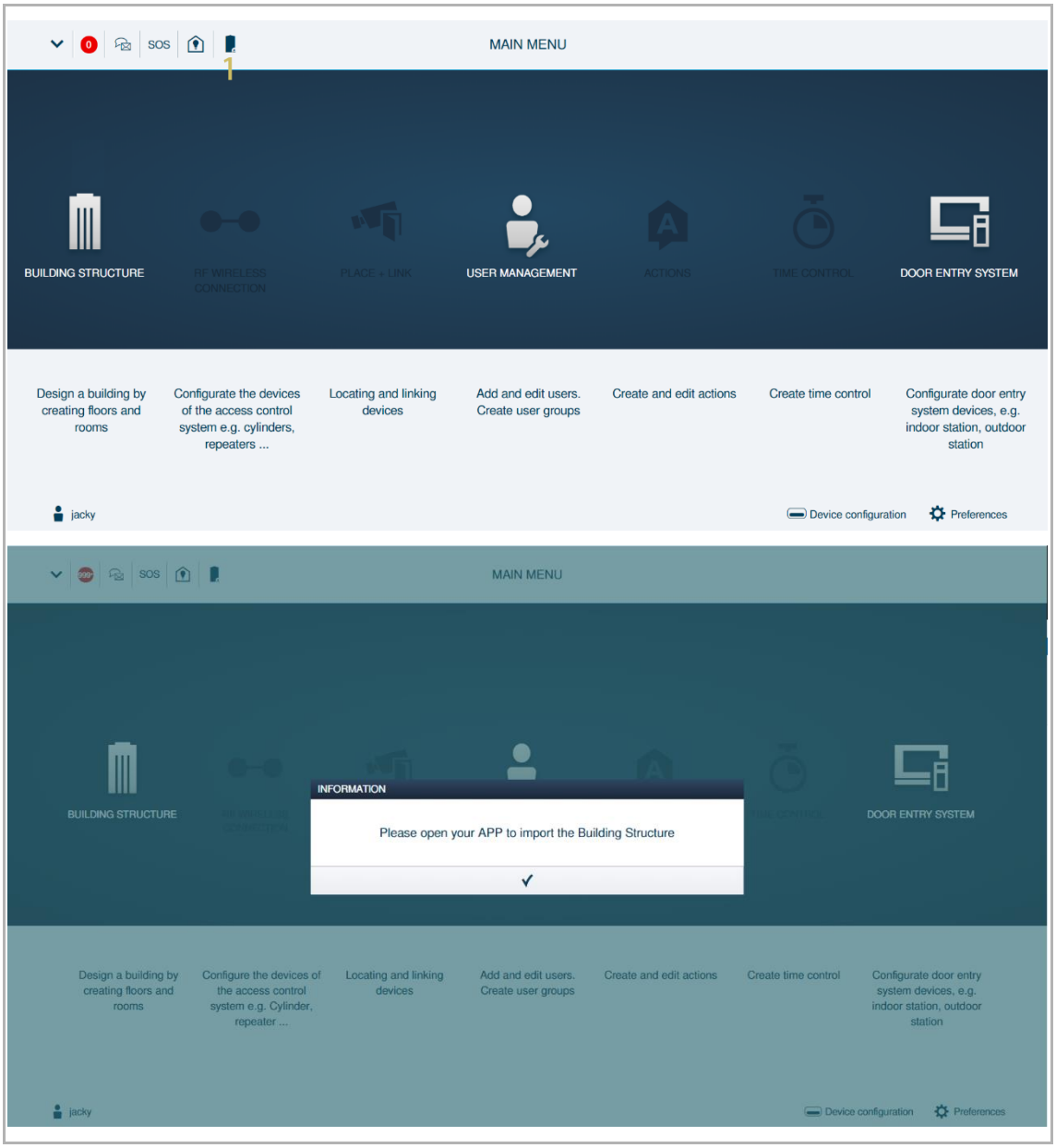
- A, B, C, D, E, F geeft het gebouwnummer aan.
- B en B+ hebben hetzelfde gebouwnummer.
- + betekent dat de structuur van het gebouw is veranderd.

Welcome-app	"Smart Access Point" ervoor	"Smart Access Point" erna
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

Het gebouw uit de Welcome-app importeren

Volg de onderstaande stappen:

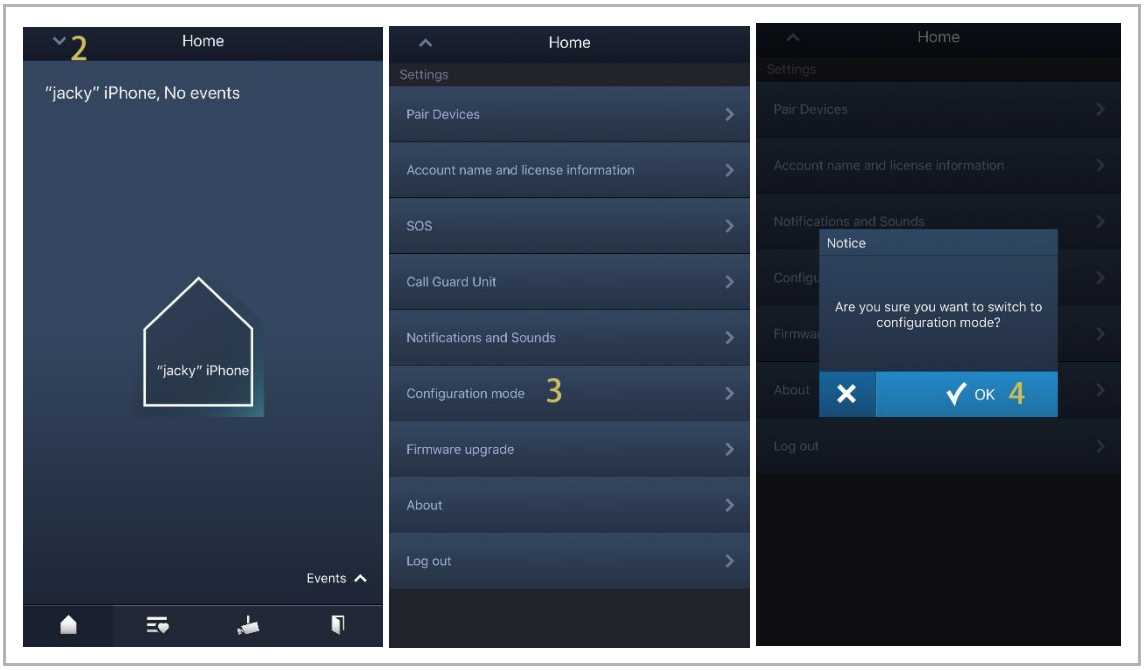
[1] In het configuratiescherm klikt u op " ": er verschijnt een pop-upvenster.



[2] Op het startscherm van de Welcome-app tikt u op "v".

[3] Tik op "Configuratiemodus".

[4] Tik op "√" om door te gaan.



[5] Op het scherm "Projecten" veegt u de projectnaam naar rechts.

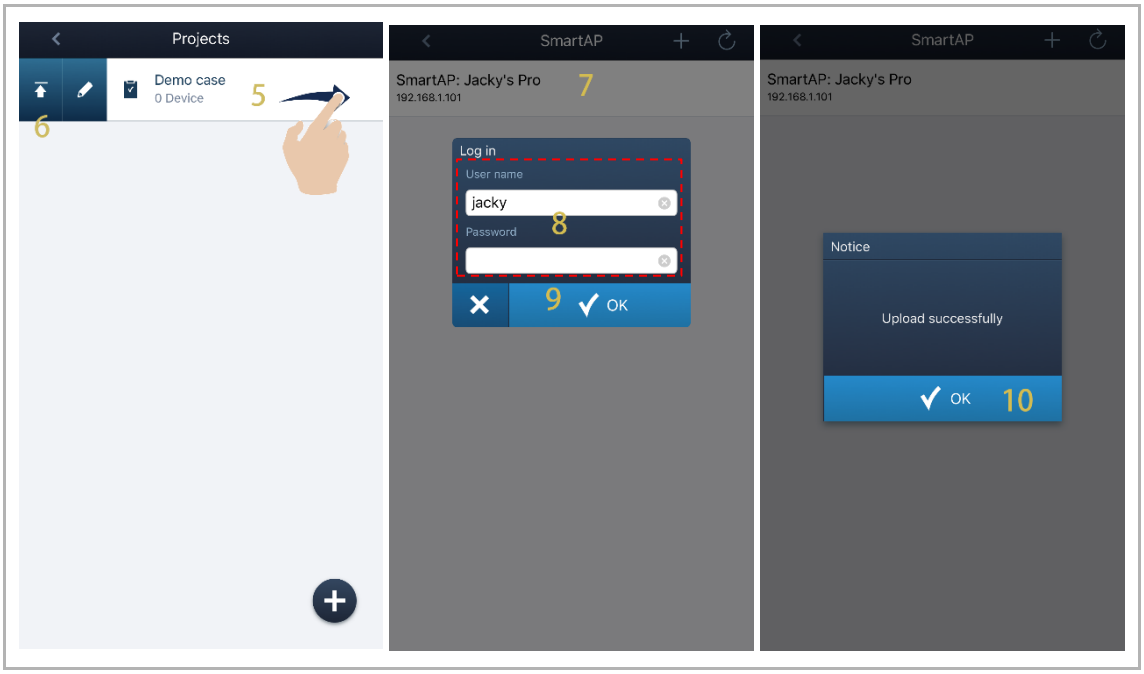
[6] Tik op " ".

[7] Tik op het betreffende "Smart Access Point".

[8] Voor de accountnaam en het wachtwoord in voor het "Smart Access Point".

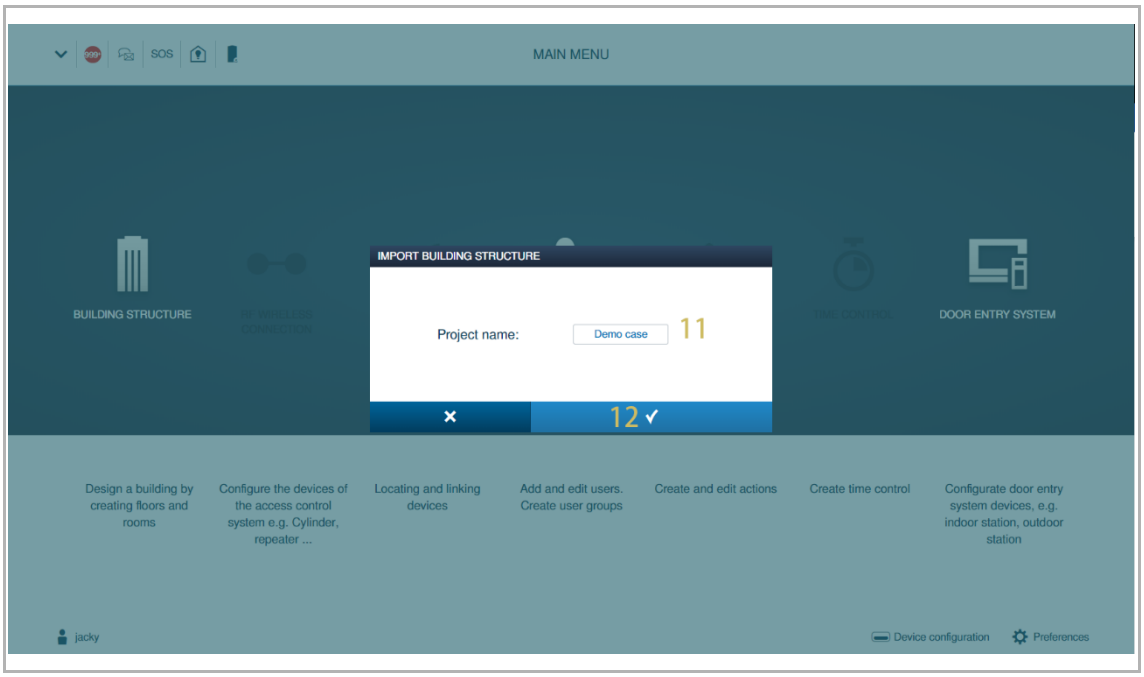
[9] Tik op "√" om door te gaan.

[10] Tik op "√" om te voltooien.

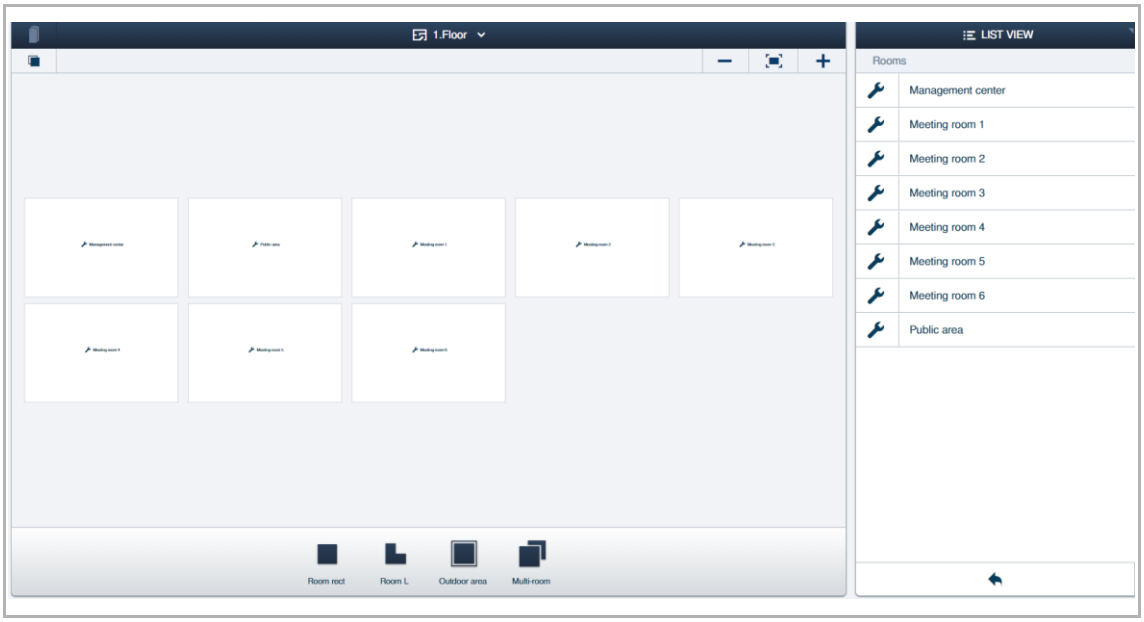


[11]Ga terug naar het configuratiescherm van het "Smart Access Point" : er verschijnt een pop-upvenster met de importstatus.

[12]Klik op "√" om te voltooien.



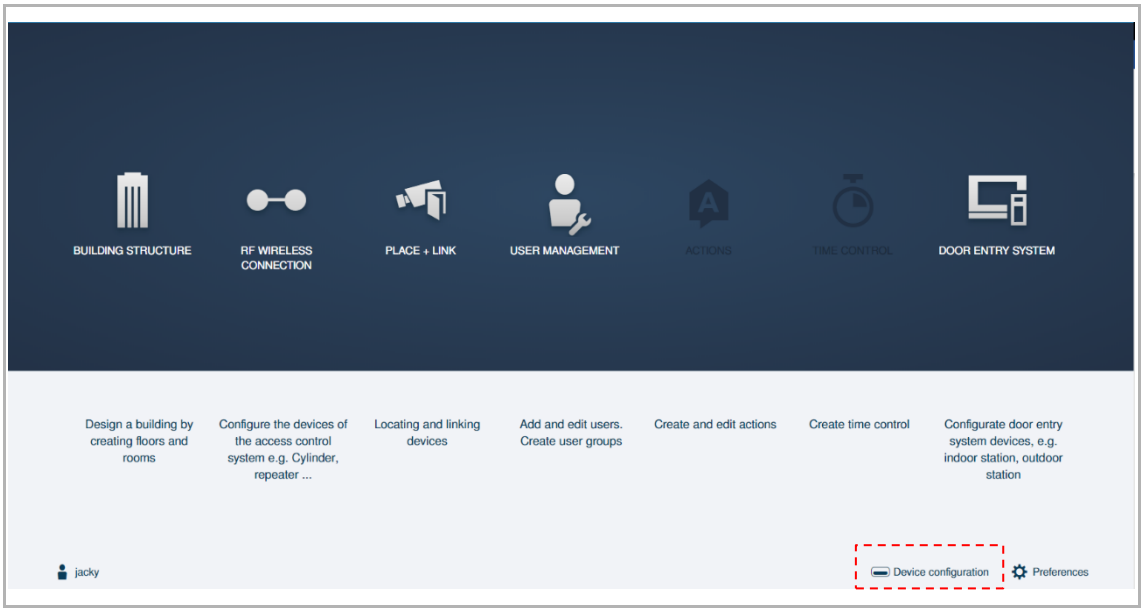
Het gebouw dat wordt geïmporteerd uit de Welcome-app bevat geen vorm of locatie. U dient deze aan te passen op het "Smart Access Point". zie hoofdstuk 10.2.1 “Een gebouw maken via "Smart Access Point"“ op pagina 145.



10.3 Vertrouwde apparaten toevoegen en lokaliseren

Scherm "Apparaatconfiguratie" oproepen

Klik in het configuratiescherm op "Apparaatconfiguratie" om het bijbehorende scherm te openen.



10.3.1 "Smart Access Point" lokaliseren

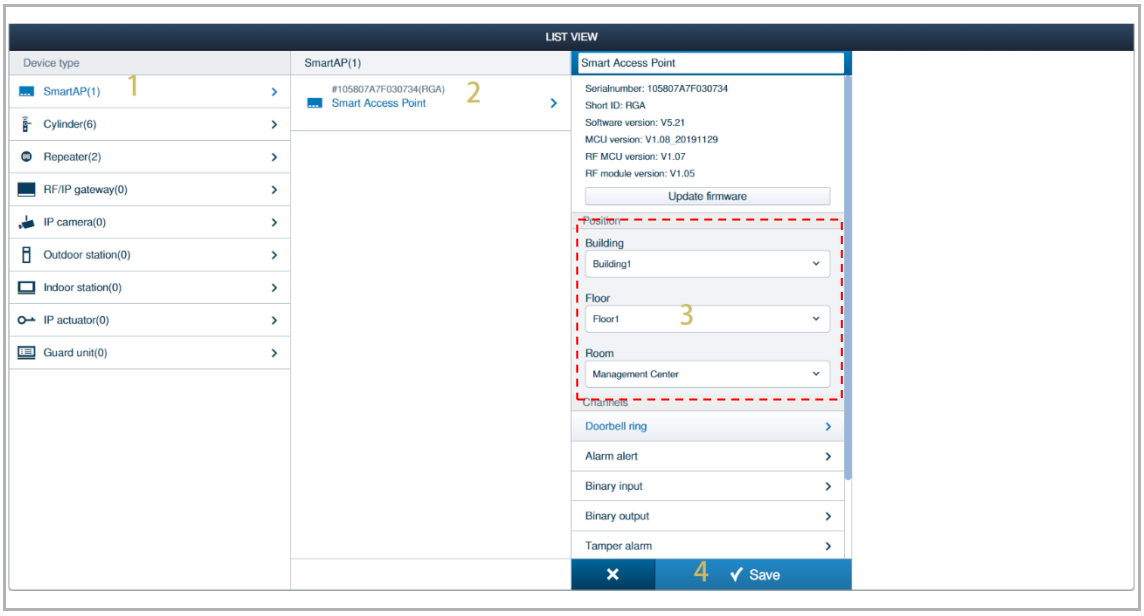
Volg de onderstaande stappen:

[1] Klik in het scherm "Apparaatconfiguratie" op "SmartAP".

[2] Klik op "Smart Access Point".

[3] Kies de positie uit de keuzelijst (bijv. "Gebouw 1>>Etage 1>>Openbaar bereik" voor demonstratie 1).

[4] Klik op "√" om op te slaan.



10.3.2 Toevoegen en lokaliseren van de "elektronische slotcilinder"

Volg de onderstaande stappen:

[1] Klik in het scherm "Apparaatconfiguratie" op "Cilinder".

[2] Klik op "+".

[3] Klik op "Cilinder".

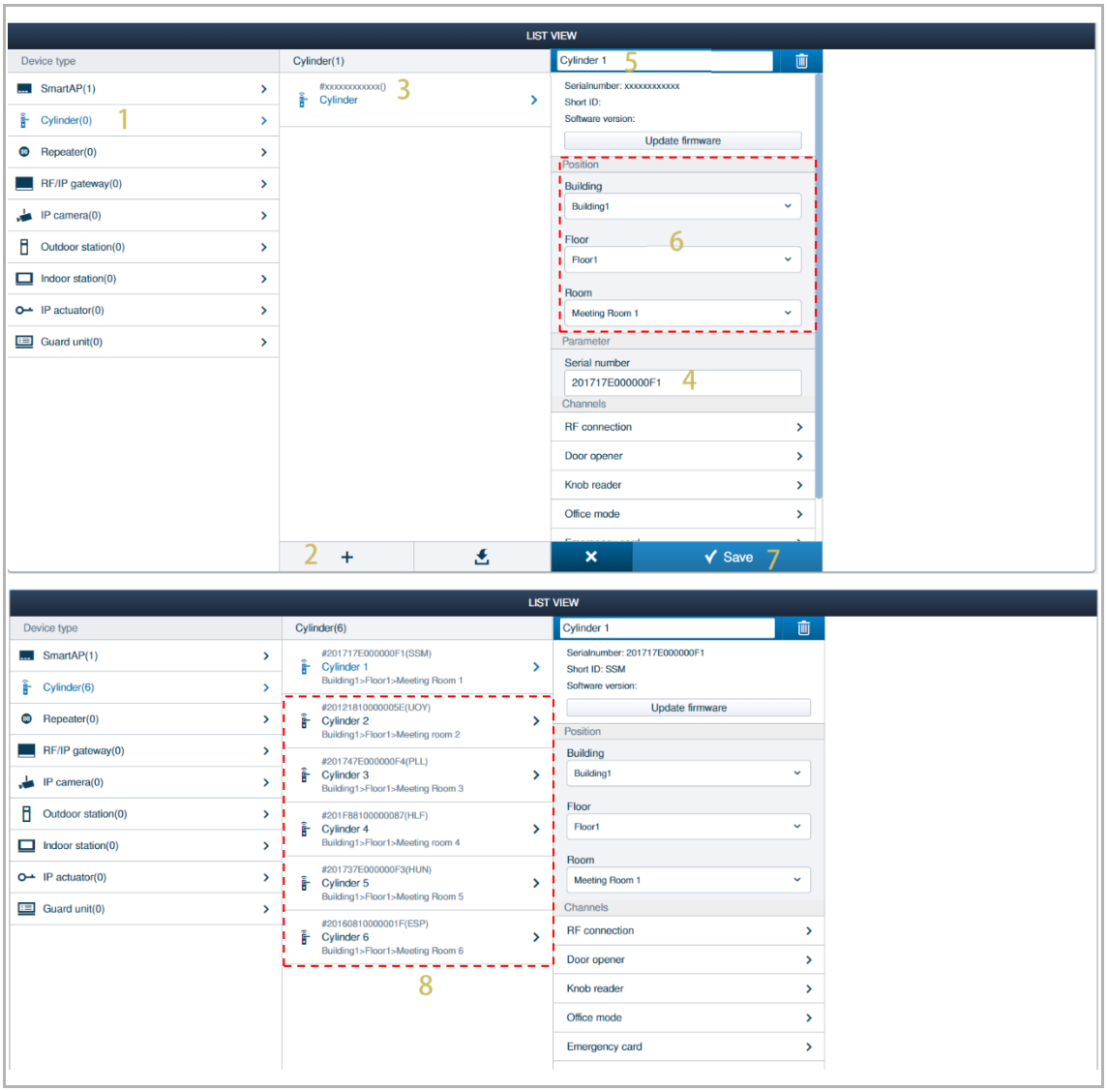
[4] Voer het serienummer van de elektronische slotcilinder in.

[5] Wijzig de naam van de "elektronische slotcilinder" in.

[6] Kies de positie uit de keuzelijst (bijv. "Gebouw 1>>Etage 1>>Vergaderzaal 1" voor demonstratie 1).

[7] Klik op "√" om op te slaan.

[8] Herhaal de stappen 2-7 om de "elektronische slotcilinders" één voor één toe te voegen (bijv. "Cilinder 2-Cilinder 6" voor demonstratie 1).



10.3.3 Toevoegen en lokaliseren van een "RF-repeater"

Volg de onderstaande stappen om een "RF-repeater" toe te voegen.

[1] Klik in het scherm "Apparaatconfiguratie" op "Repeater".

[2] Klik op "+".

[3] Klik op "Repeater".

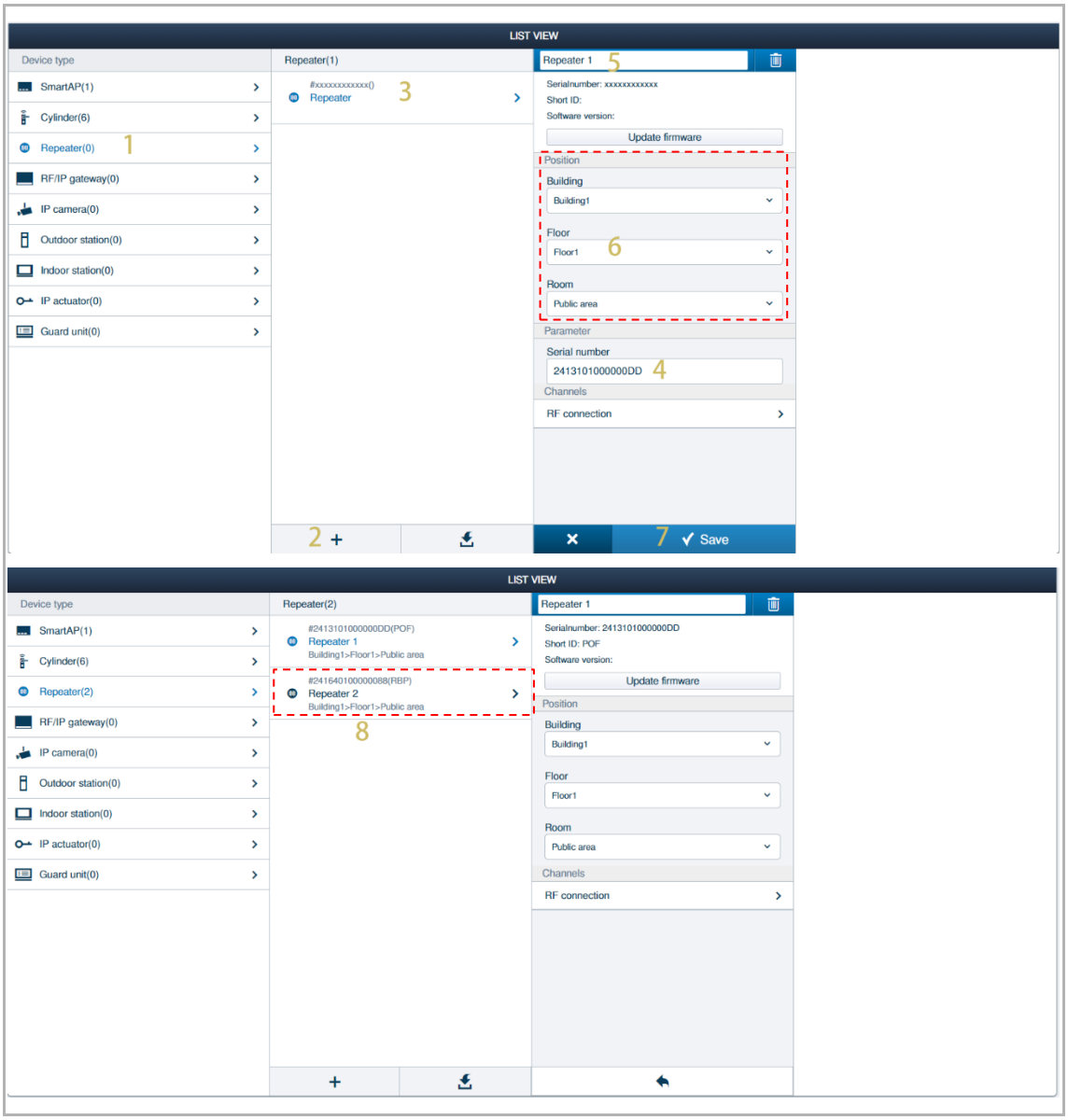
[4] Voer het serienummer van de "RF-repeater" in.

[5] Wijzig de naam van de "RF-repeater".

[6] Kies de positie uit de keuzelijst (bijv. "Gebouw 1>>Etage 1>>Openbaar bereik" voor demonstratie 1).

[7] Klik op "√" om op te slaan.

[8] Herhaal stap 2-7 om de "RF-repeater" toe te voegen. (bijv. "Repeater 2" voor demonstratie 1).



10.3.4 Toevoegen en lokaliseren van een "RF/IP-gateway".

Volg de onderstaande stappen om een "RF/IP-gateway" toe te voegen.

[1] Klik in het scherm "Apparaatconfiguratie" op "BLE".

[2] Klik op " ".

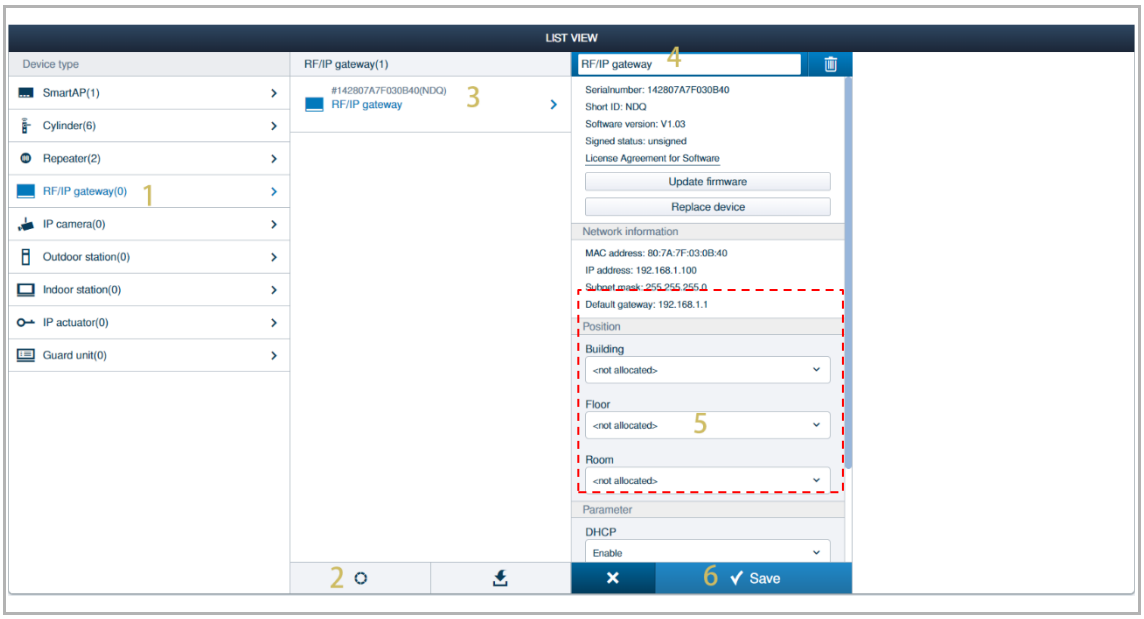
[3] Klik op "BLE".

[4] Wijzig de naam van de "elektronische slotcilinder" in.

[5] Kies een positie uit de keuzelijst.

[6] Klik op "√" om op te slaan.

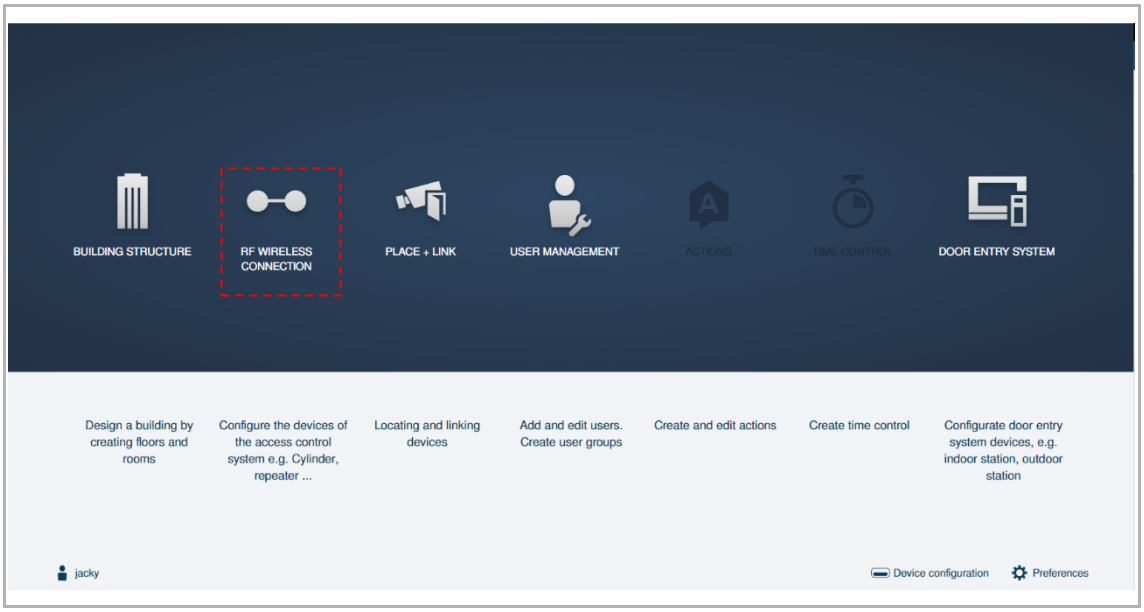
Herhaal stap 2-7 om de RF/IP-gateway één voor één toe te voegen.



10.4 Apparaten aansluiten

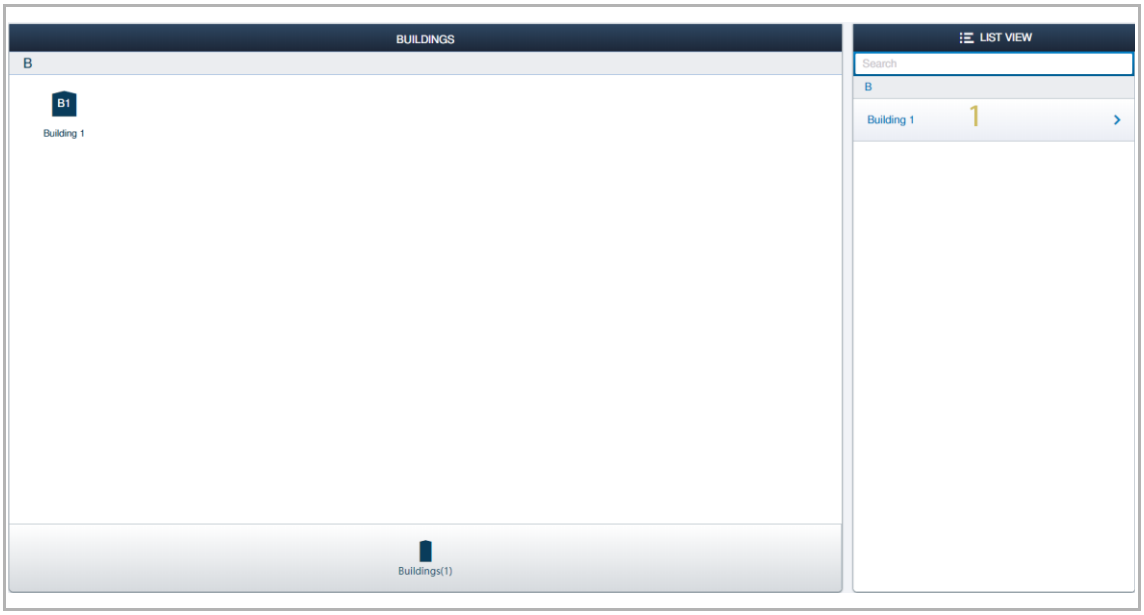
Ga naar het scherm RF-verbinding

Klik in het configuratiescherm op "Toegangscontrole" om het bijbehorende scherm te openen.

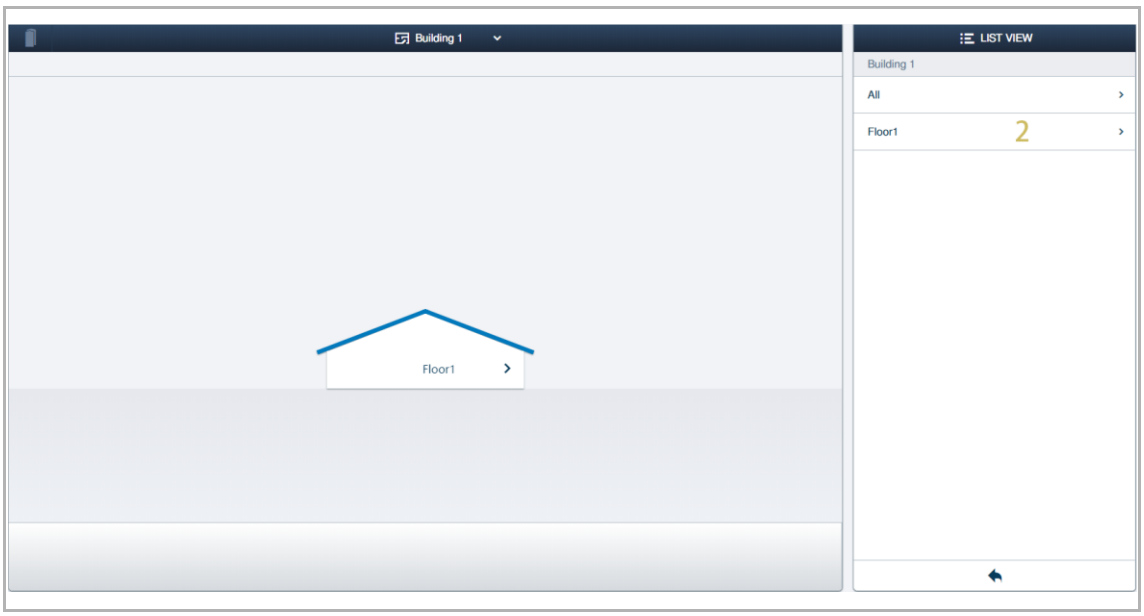


Volg de onderstaande stappen:

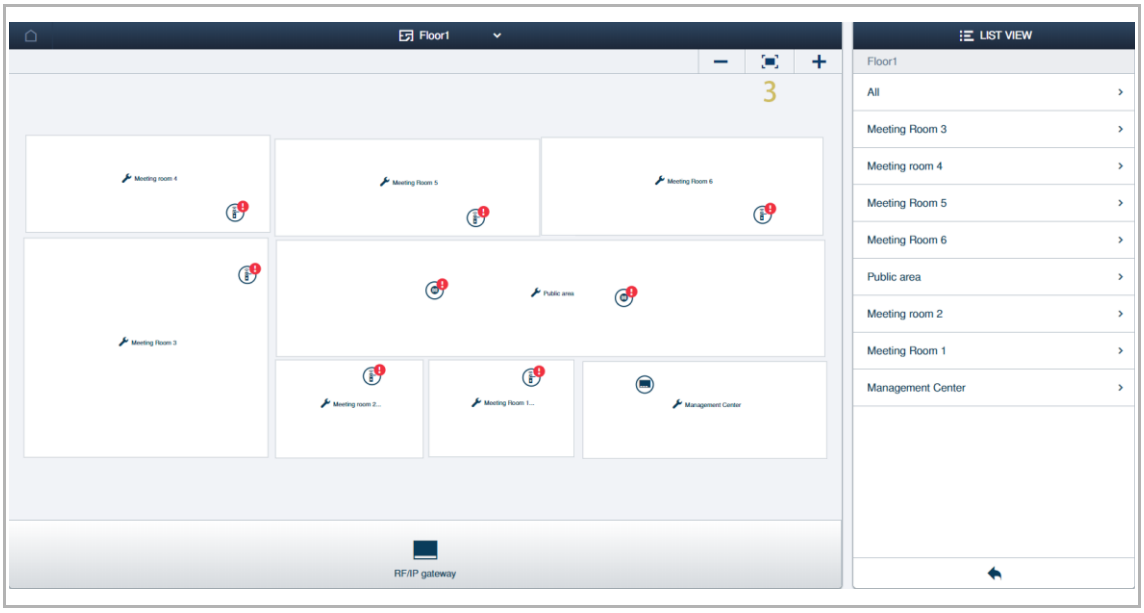
[1] Op het scherm "Gebouw" klikt u op het benodigde gebouw (bijv. "Gebouw 1" voor demonstratie 1).



[2] Klik op de benodigde etage (bijv. "Etage 1" voor demonstratie 1).



[3] Klik op " " om alle apparaten op het etagescherm te bekijken, u kunt de symbolen naar een geschikte positie slepen.



AccessControl-apparaten in een sequentie aansluiten

Sluit de AccessControl-apparaten in een radiolijn aan volgens de onderstaande volgorde:

[1] Sluit het "Smart Access Point" of de "RF/IP-gateway" aan met de slave-apparaten.

[2] Sluit de "RF-repeater" aan op de bijbehorende slave-apparaten.

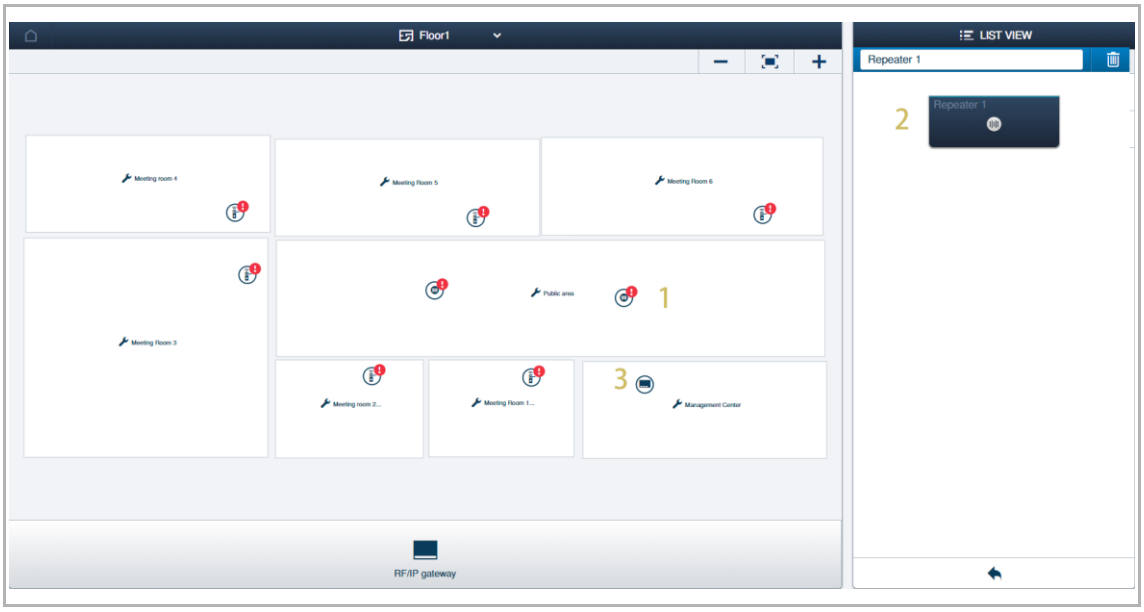
10.4.1 "RF-repeater aansluiten"

Volg de onderstaande stappen:

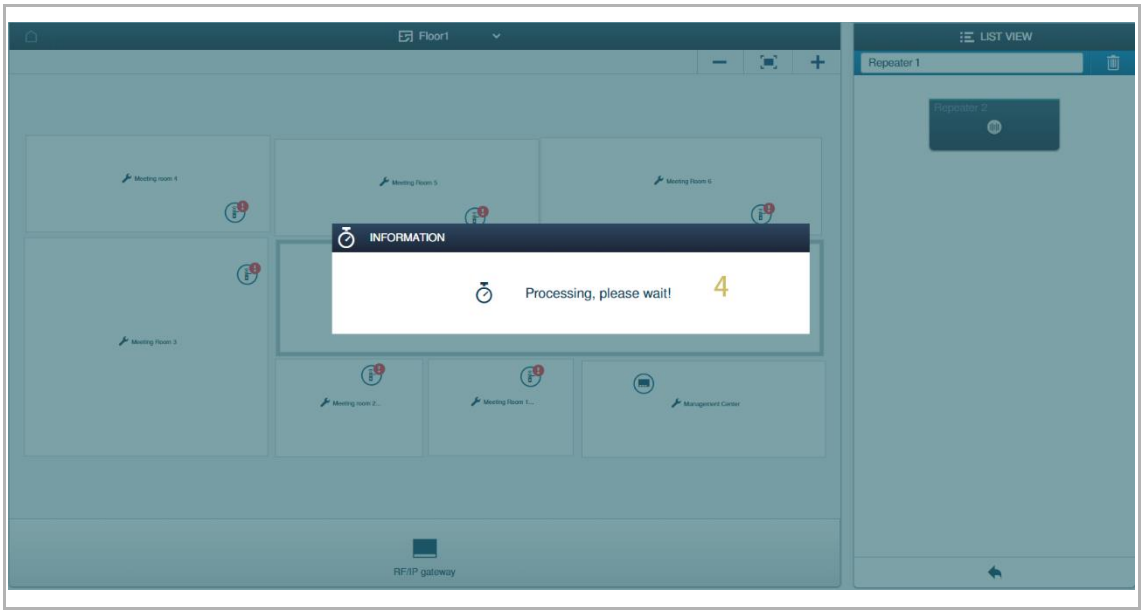
[1] Klik op het etagescherm op een "RF-repeater" (bijv. "Repeater 1" voor demonstratie 1).

[2] Op dit moment wordt geen hoger apparaat in de lijst weergegeven.

[3] Klik op het hogere apparaat op de etageplattegrond (bijv. "Smart Access Point" voor demonstratie 1).



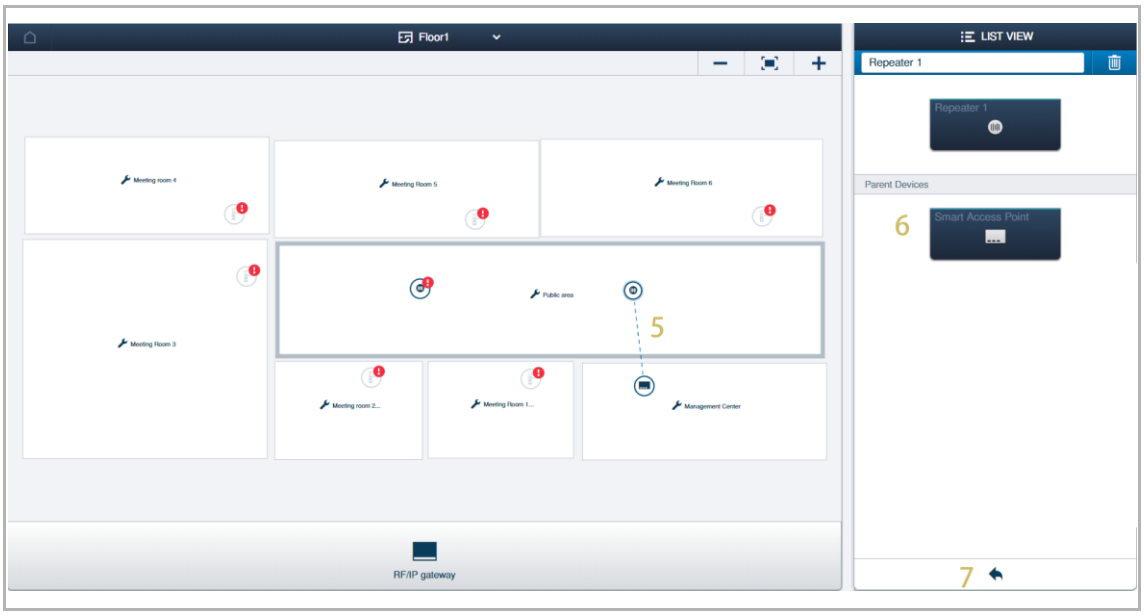
[4] Wachten op de koppeling



[5] Een geslaagde koppeling tussen de twee apparaten wordt aangegeven met een stippellijn.

[6] Hoger apparaat wordt weergegeven in de lijst.

[7] Klik op " " om terug te gaan naar het etagescherm.



Opmerking

De "RF Repeater" moet zichzelf ontkoppelen van het hogere apparaat voordat het kan worden gekoppeld aan een nieuw apparaat. zie hoofdstuk 10.11.2 “"RF-repeater" loskoppelen“ op pagina 221.

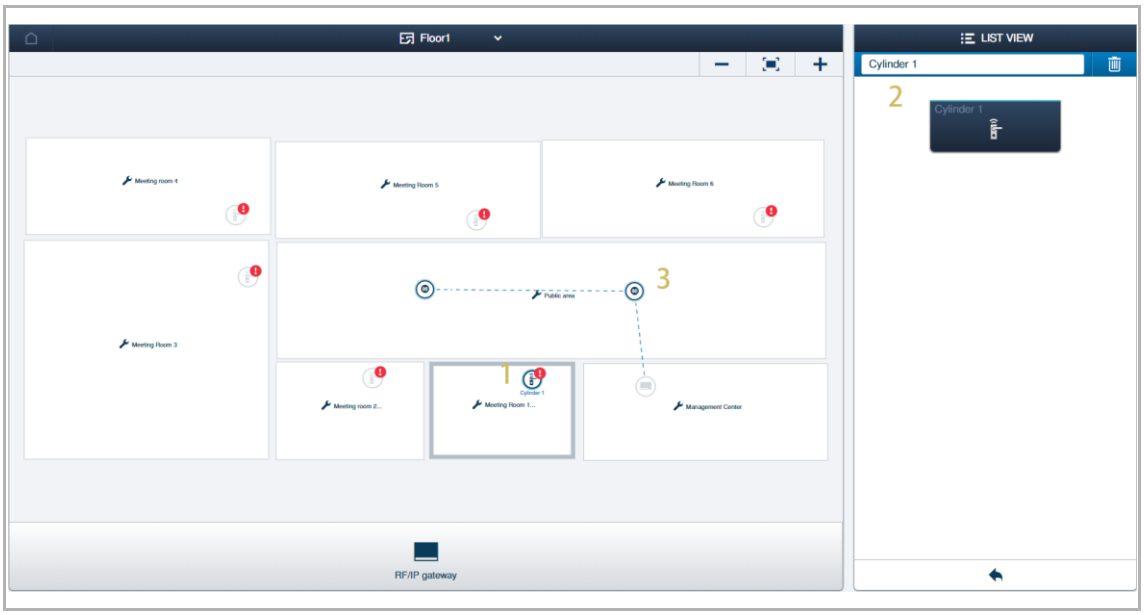
10.4.2 "Elektronische slotcilinder" verbinden

Volg de onderstaande stappen:

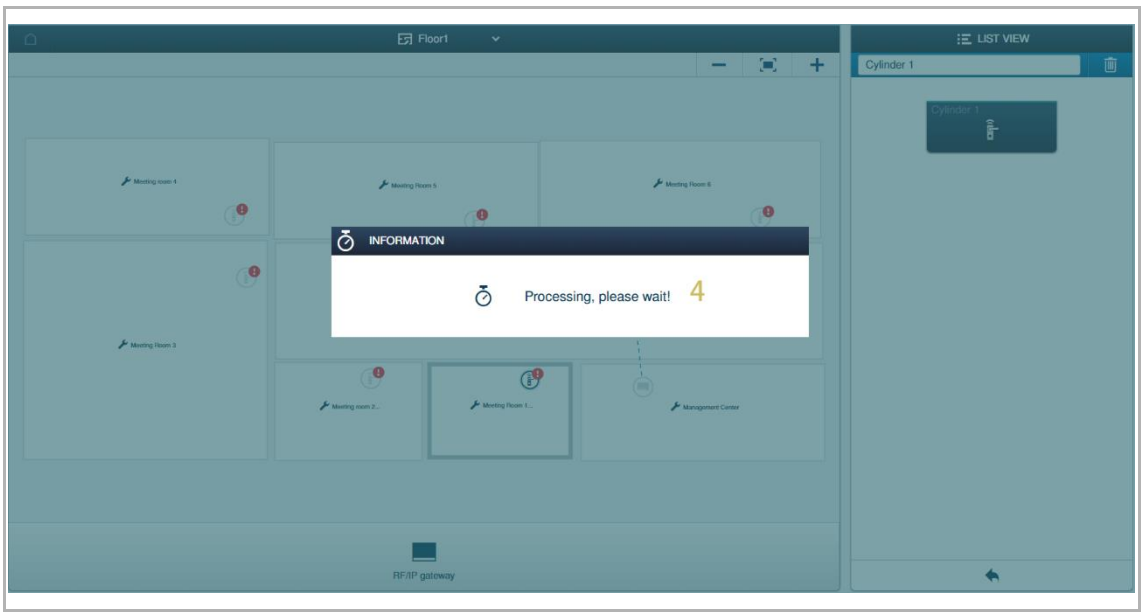
[1] Klik op het etagescherm op een "elektronische slotcilinder" (bijv. "Cilinder 1" voor demonstratie 1).

[2] Op dit moment wordt geen hoger apparaat in de lijst weergegeven.

[3] Klik op het hogere apparaat op de etageplattegrond (bijv. "Repeater 1" voor demonstratie 1).

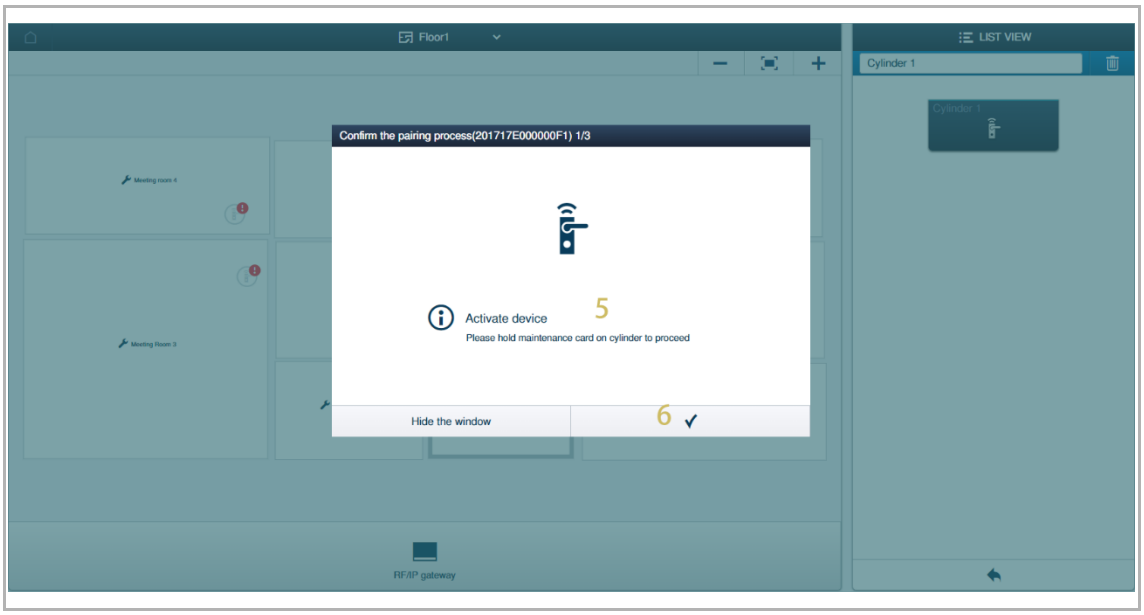


[4] Wacht op de koppeling.

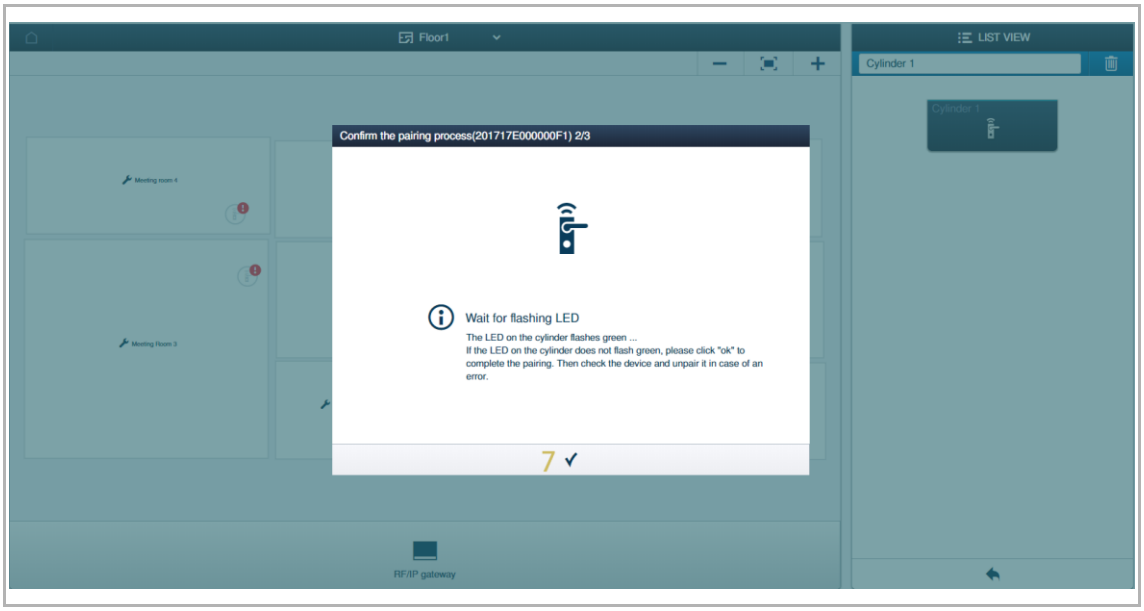


[5] Houd de onderhoudskaart tegen de elektronische slave-cilinder.

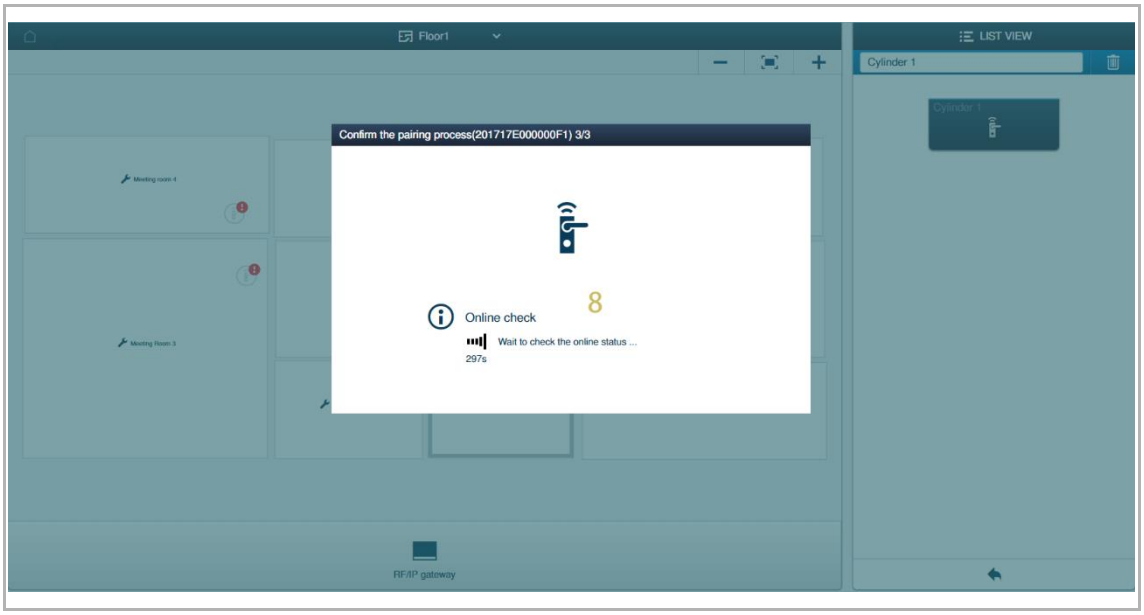
[6] Klik op "√" om door te gaan.



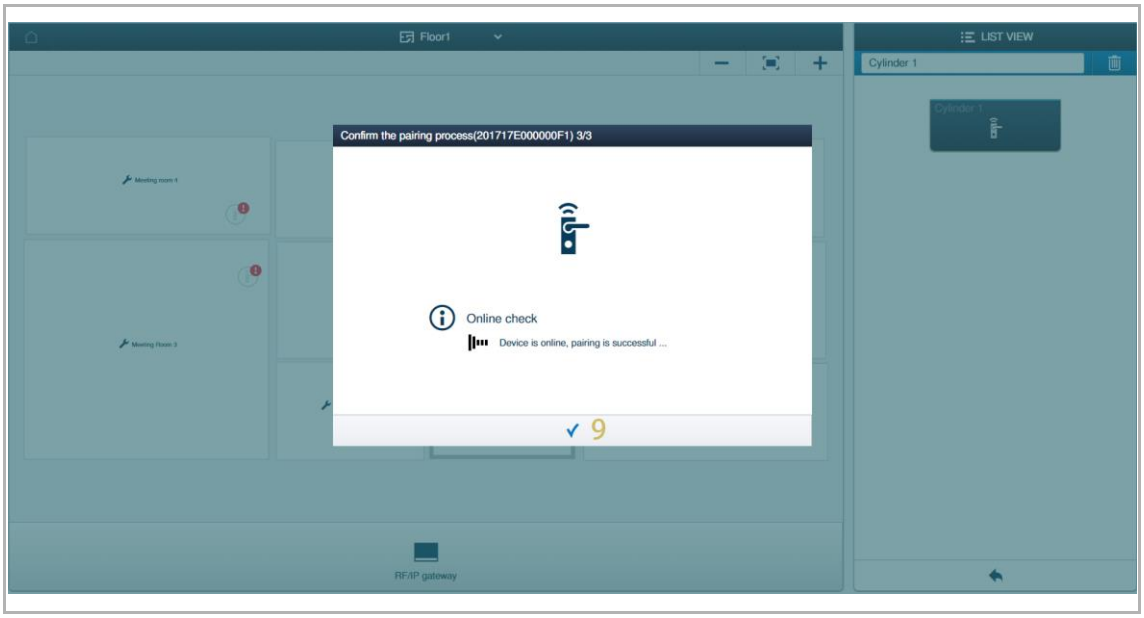
[7] Als de LED op de "elektronische slotcilinder" groen knippert of als de "elektronische slotcilinder" een pieptoon geeft, klikt u op "√" om door te gaan.



[8] Wacht op de online check.



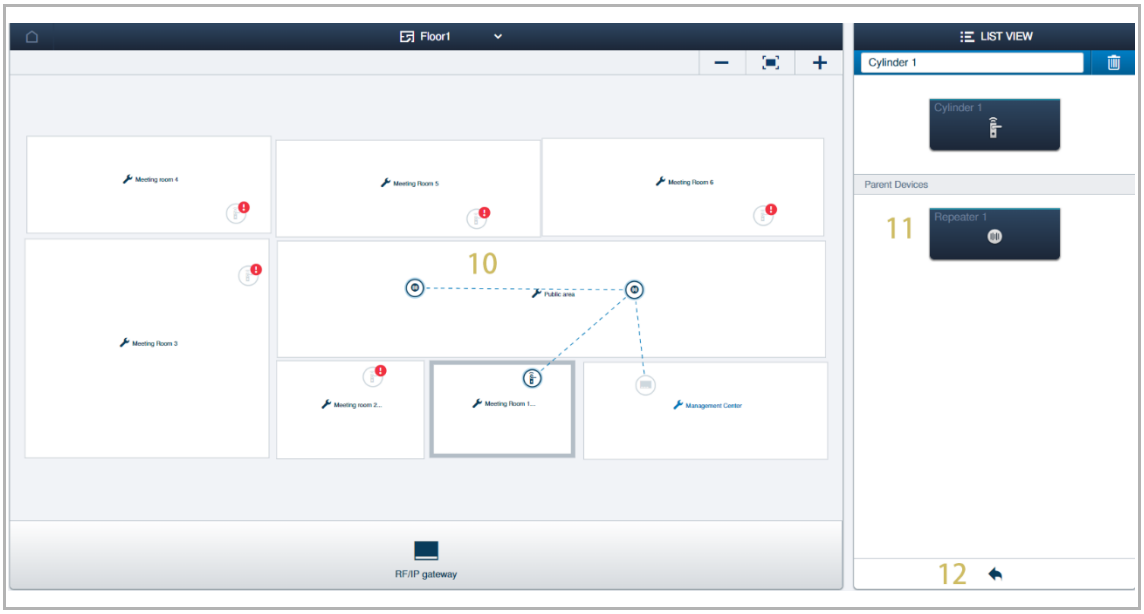
[9] Als de "elektronische slotcilinder" online is, klikt u op "√" om door te gaan. Anders moet u 300 s wachten voordat u de volgende stap uitvoert.



[10]Pair Een geslaagde koppeling tussen de twee apparaten wordt aangegeven met een stippellijn.

[11]The p Hoger apparaat wordt weergegeven in de lijst.

[12]Klik op " " om terug te gaan naar het etagescherm.



Opmerking

De elektronische slotcilinder moet zichzelf ontkoppelen van het hogere apparaat voordat het kan worden gekoppeld aan een nieuw apparaat. Pagina 217.

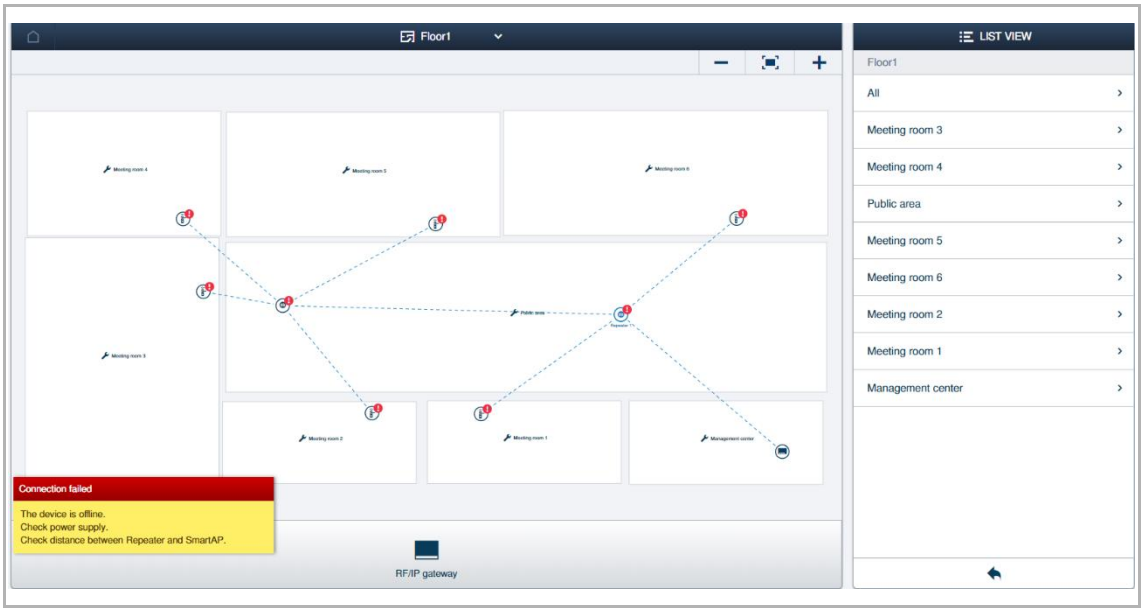
10.4.3 AccessControl-apparaat is offline

Er wordt een offlinesymbool " " weergegeven op het AccessControl-apparaat als het offline is.

1. "RF-repeater" is offline

Wanneer u " " op een "RF-repeater" ziet, voert u volgende handelingen uit:

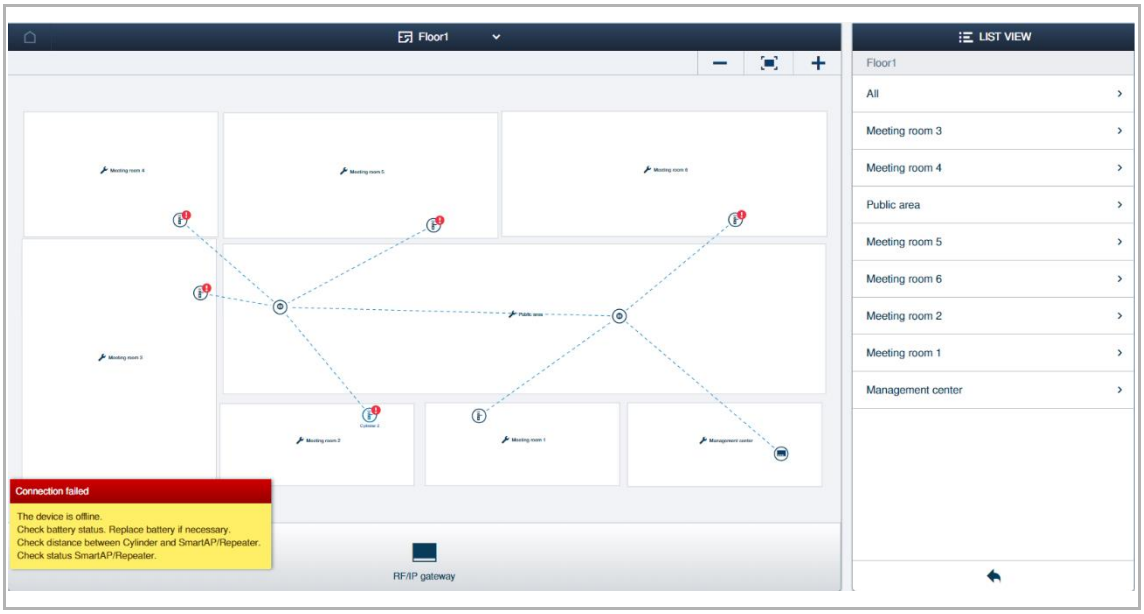
- Controleer of de RF-repeater ingeschakeld is.
- Controleer of de hogere RF-repeater ingeschakeld is.
- Controleer of de afstand tussen de RF-repeater en het hogere apparaat meer dan 10 meter bedraagt.



2. "Elektronische slotcilinder" is offline

Wanneer u " " op een "elektronische slotcilinder" ziet, voert u volgende handelingen uit:

- Controleer of de batterij van de elektronische slotcilinder leeg is. Pagina 178.
- Controleer of het hogere apparaat ingeschakeld offline is.
- Controleer of de afstand tussen de elektronische slotcilinders en het hogere apparaat meer dan 10 meter bedraagt.



Opmerking

In sommige gevallen kunt u de onderhoudskaart tegen de betreffende "elektronische slotcilinder" houden om deze te activeren.

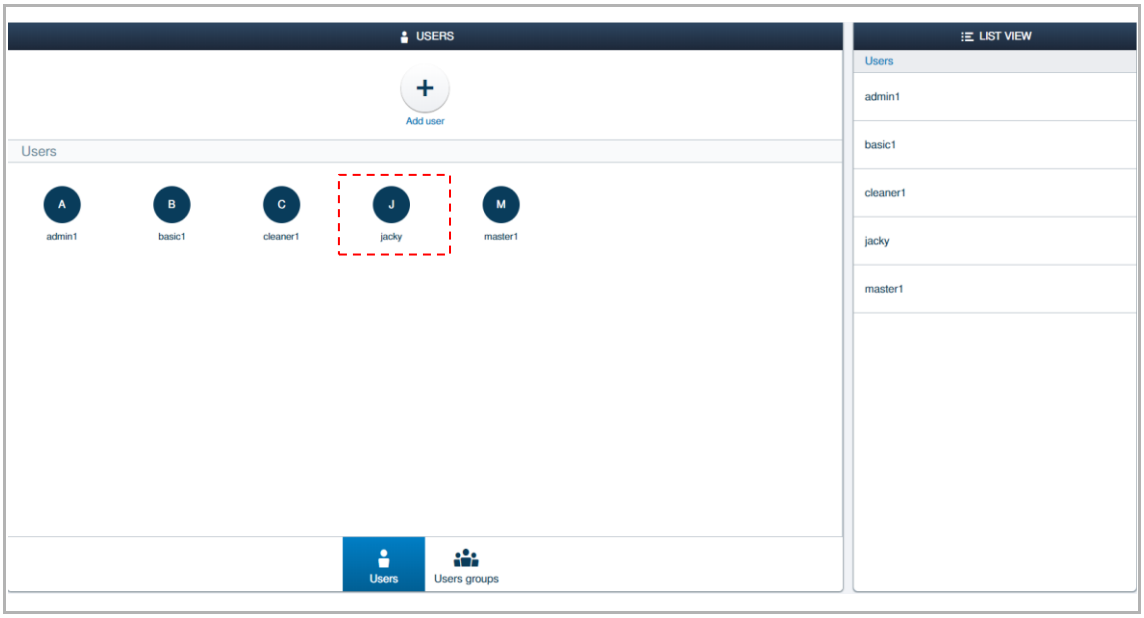
10.5 Goedkeuringen toewijzen

10.5.1 Rechten toewijzen aan een gebruiker

U kunt rechten aan een gebruiker toewijzen door zowel de ID-authenticaties als de "elektronische slotcilinder" aan de gebruiker toe te wijzen.

Het gebruikersscherm oproepen

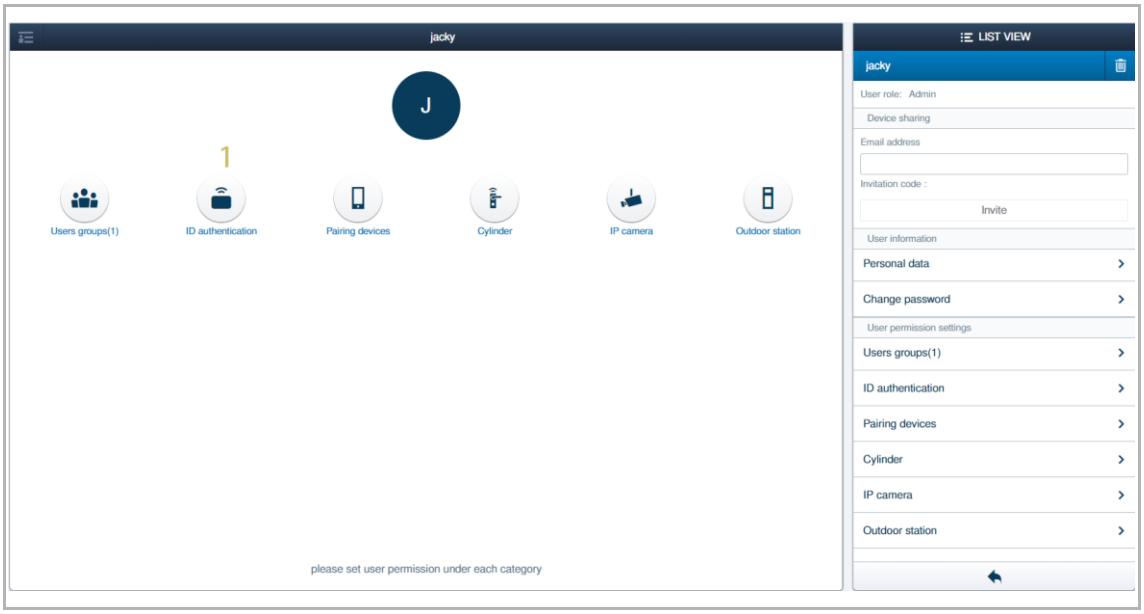
Op het scherm "Gebruikers" klikt u op de gebruiker om toegang te krijgen tot het scherm van de gebruiker.



1. De ID-authenticaties aan een gebruiker toewijzen

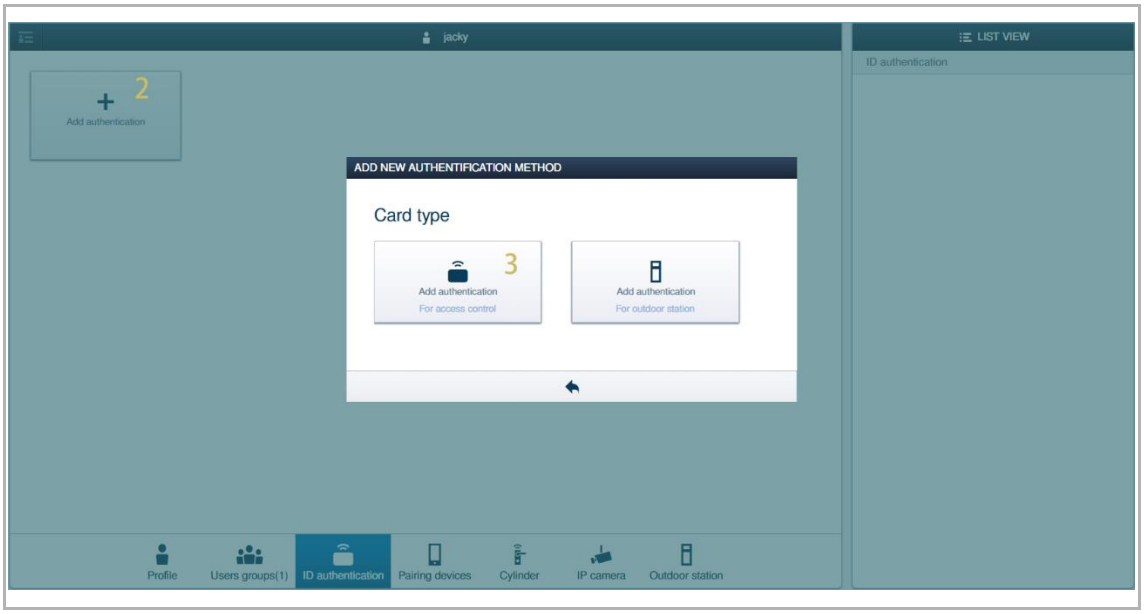
Volg de onderstaande stappen:

[1] Op het betreffende gebruikersscherm klikt u op "ID-authenticatie".



[2] Klik op "Authenticatie toevoegen".

[3] Klik op "Authenticatie toevoegen voor toegangsbeheer".



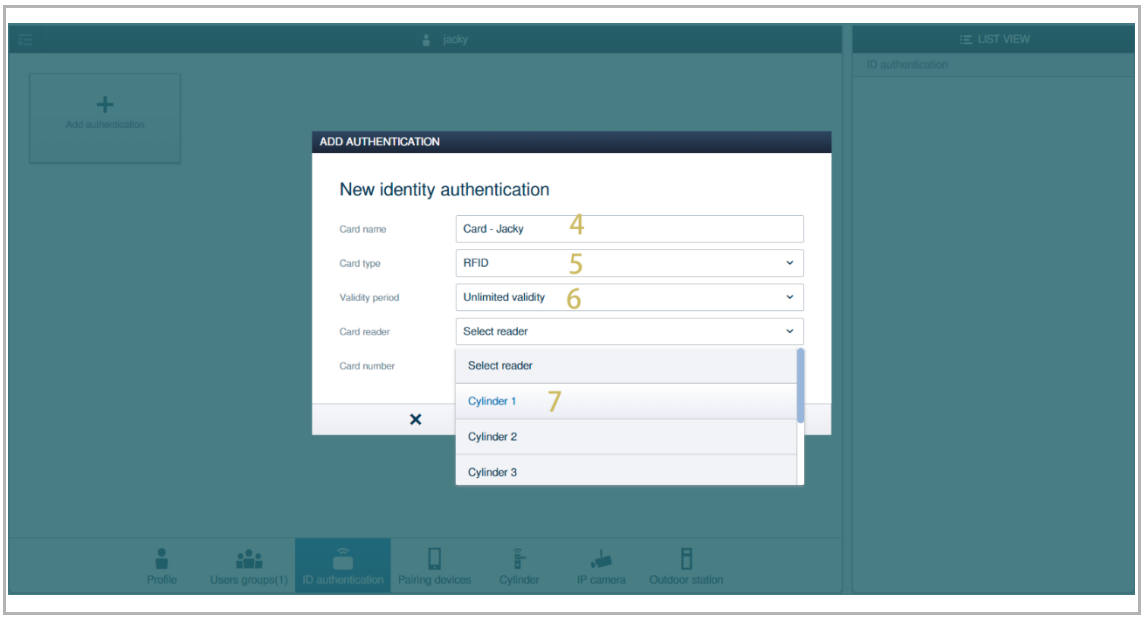
[4] Voer de naam van de kaart in.

[5] Stel het kaarttype in op "RFID".

[6] Stel de geldigheidsperiode in; er zijn 2 opties:

- Onbeperkte geldigheid, als dit type is geselecteerd, kunt u doorgaan naar de volgende stap.
- Beperkte geldigheid, als dit type is geselecteerd, moet u de begin- en einddatum instellen door op " 31 " te klikken.

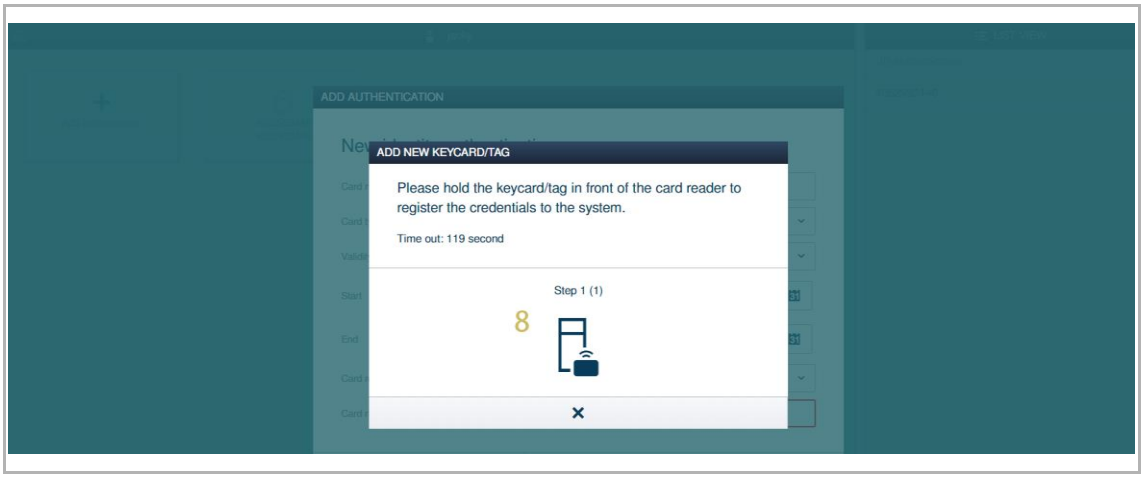
[7] Selecteer een willekeurige elektronische slotcilinder in de keuzelijst voor het vegen van de ID-authenticaties.



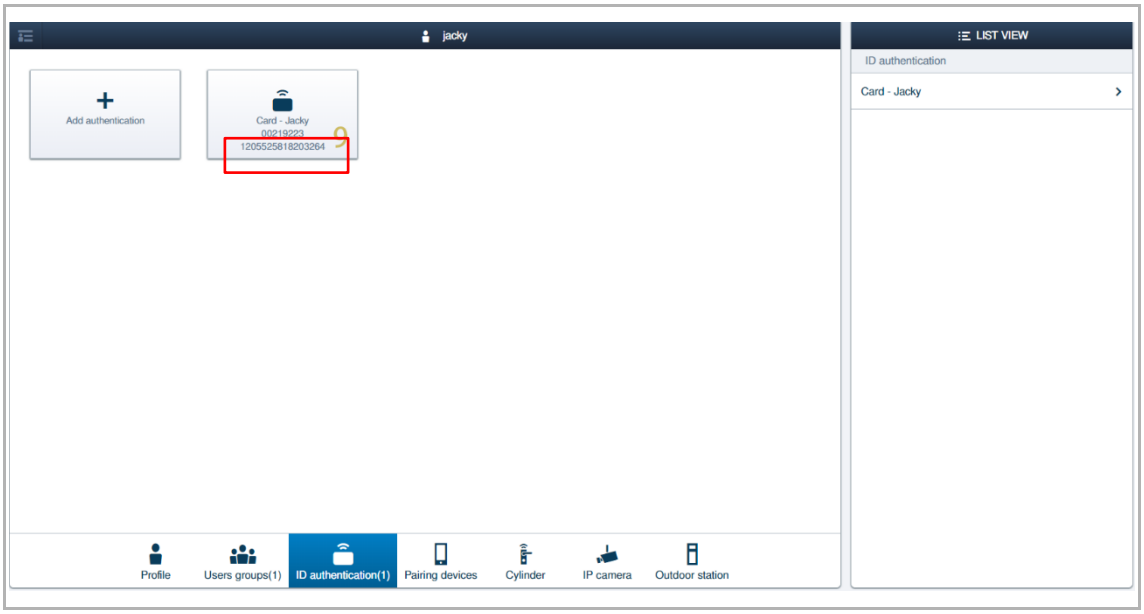
Opmerking

De elektronische slotcilinder moet in een radiolijn worden gekoppeld voordat de ID-authenticaties worden geveegd. zie hoofdstuk 10.4.2 “"Elektronische slotcilinder" verbinden“ op pagina 163.

[8] Houd de sleutelkaart of de tag voor de elektronische slotcilinder. Indien dit gelukt is knippert de led van de elektronische slotcilinder groen of er klinkt een pieptoon.



[9] Het kaartnummer wordt weergegeven op het scherm.



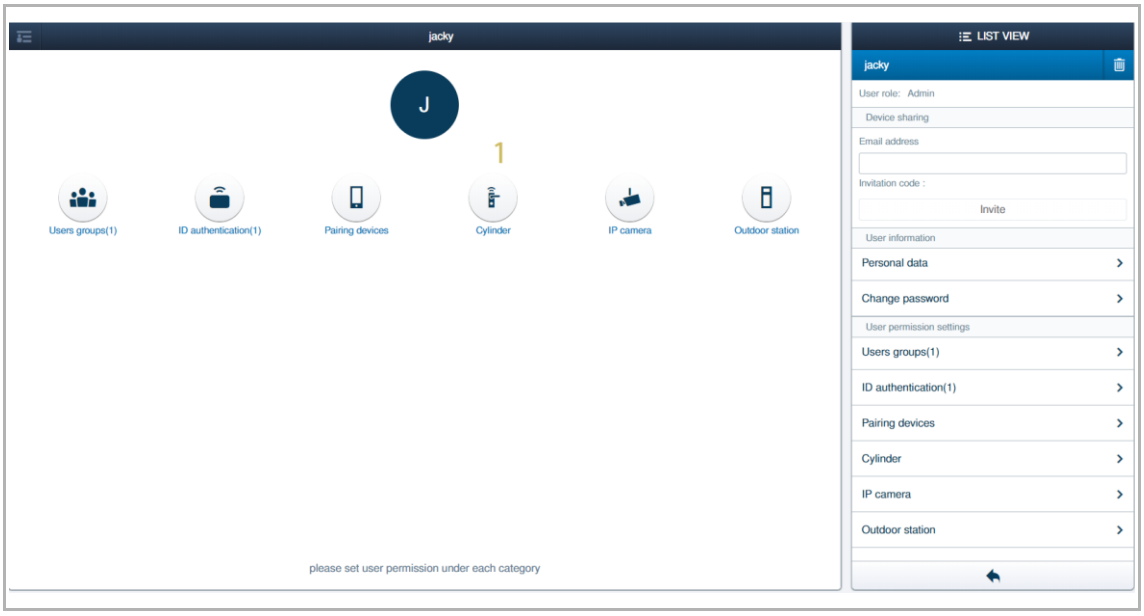
Herhaal de stappen van 2-9 om de ID-authenticaties één voor één toe te wijzen.

Opmerking
Tot 200 ID-authenticaties kunnen aan één gebruiker worden toegewezen.

2. De "elektronische slotcilinder" aan een gebruiker toewijzen.

Volg de onderstaande stappen:

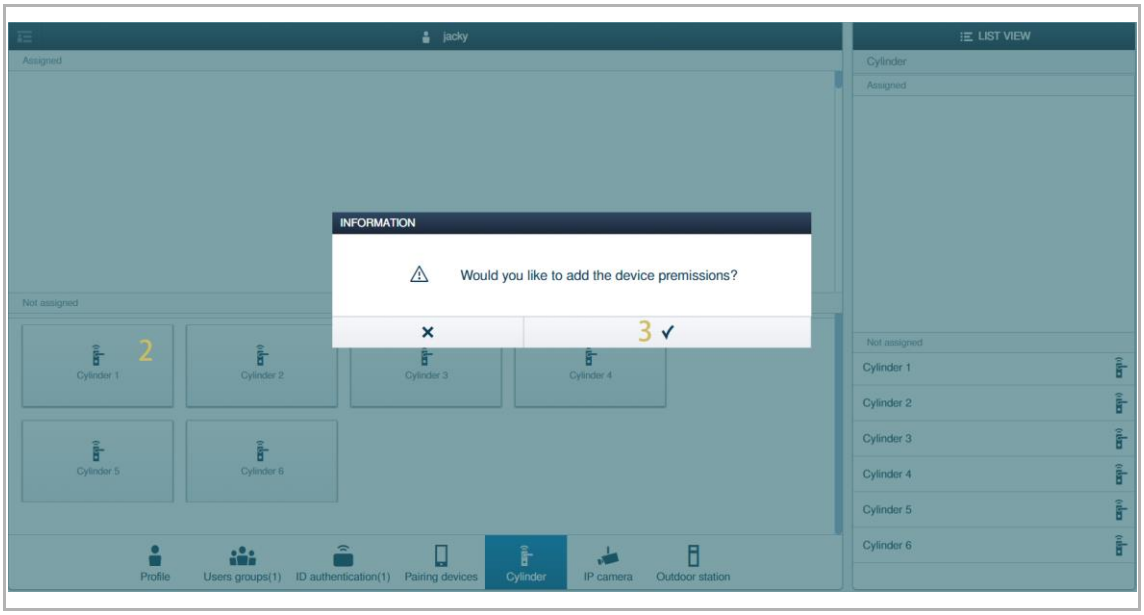
[1] Op het betreffende gebruikersscherm klikt u op "Cilinder".



[2] Klik op de "Elektronische slotcilinder" in de sectie "Niet toegewezen".

[3] Klik op "√" om te bevestigen.

Herhaal de stappen van 2-3 om de elektronische slotcilinders één voor één toe te wijzen.



10.5.2 Rechten toewijzen aan gebruikers

U kunt de rechten aan meerdere gebruikers toewijzen door de rechten toe te wijzen aan de gebruikersgroep.

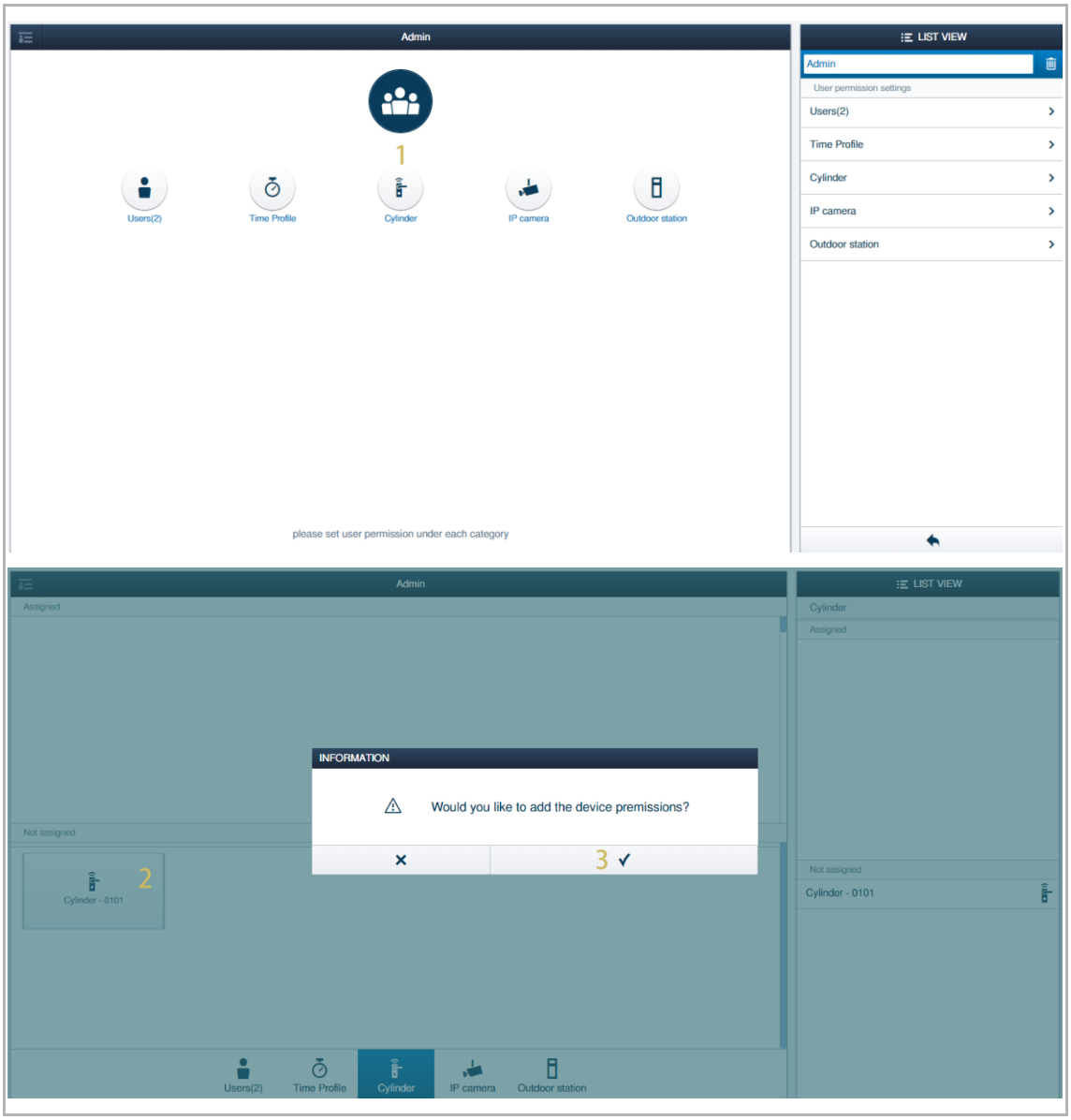
Volg de onderstaande stappen:

[1] Op het betreffende groepsscherm klikt u op "Cilinder".

[2] Klik op de "Elektronische slotcilinder" in de sectie "Niet toegewezen".

[3] Klik op "√" om te bevestigen.

Herhaal de stappen van 2-3 om de elektronische slotcilinders één voor één toe te wijzen.



10.5.3 Offline-dag instellen

In sommige gevallen is de "elektronische slotcilinder" offline. zie hoofdstuk 10.4.3 “AccessControl-apparaat is offline“ op pagina 167.

In dit geval kunnen alleen noodkaarten en de kaarten die overeenkomen met de offline dag worden gebruikt.

Opmerking
Aanbevolen wordt om de kaarten voor de offline dag of voor noodgevallen voorafgaande aan het gebruik in te stellen.

Offline dag

Wanneer een "elektronische slotcilinder" offline is, kunnen alleen de ID-authenticaties binnen de offline dagen worden gebruikt.

Als de offline dag bijvoorbeeld is ingesteld op "5", kunnen alleen de ID-authenticaties die binnen 5 dagen gebruikt zijn, worden gebruikt. De ID-authenticaties die 6 dagen geleden werden gebruikt, kunnen niet meer worden gebruikt.

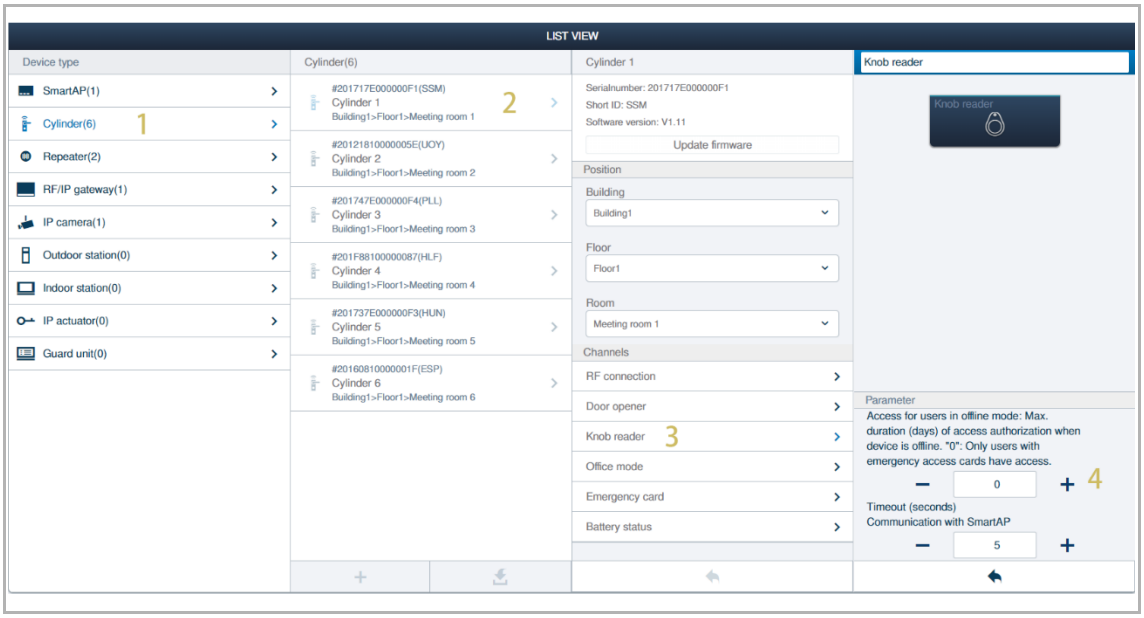
Volg de onderstaande stappen:

[1] Klik in het configuratiescherm op "Apparaatconfiguratie" en vervolgens op "Cilinder".

[2] Klik op de "Elektronische slotcilinder".

[3] Klik op "Deurgreep-lezer".

[4] Voer het nummer voor de offline dag in. Als de offline dag op "0" staat, kunnen alleen noodkaarten worden gebruikt. zie hoofdstuk 10.5.4 “Noodkaarten beheren“ op pagina 176.



10.5.4 Noodkaarten beheren

Noodkaarten kunnen worden gebruikt wanneer de "elektronische slotcilinder" offline is.

1. Noodkaarten toevoegen

Volg de onderstaande stappen:

[1] Klik in het configuratiescherm op "Apparaatconfiguratie" en vervolgens op "Cilinder".

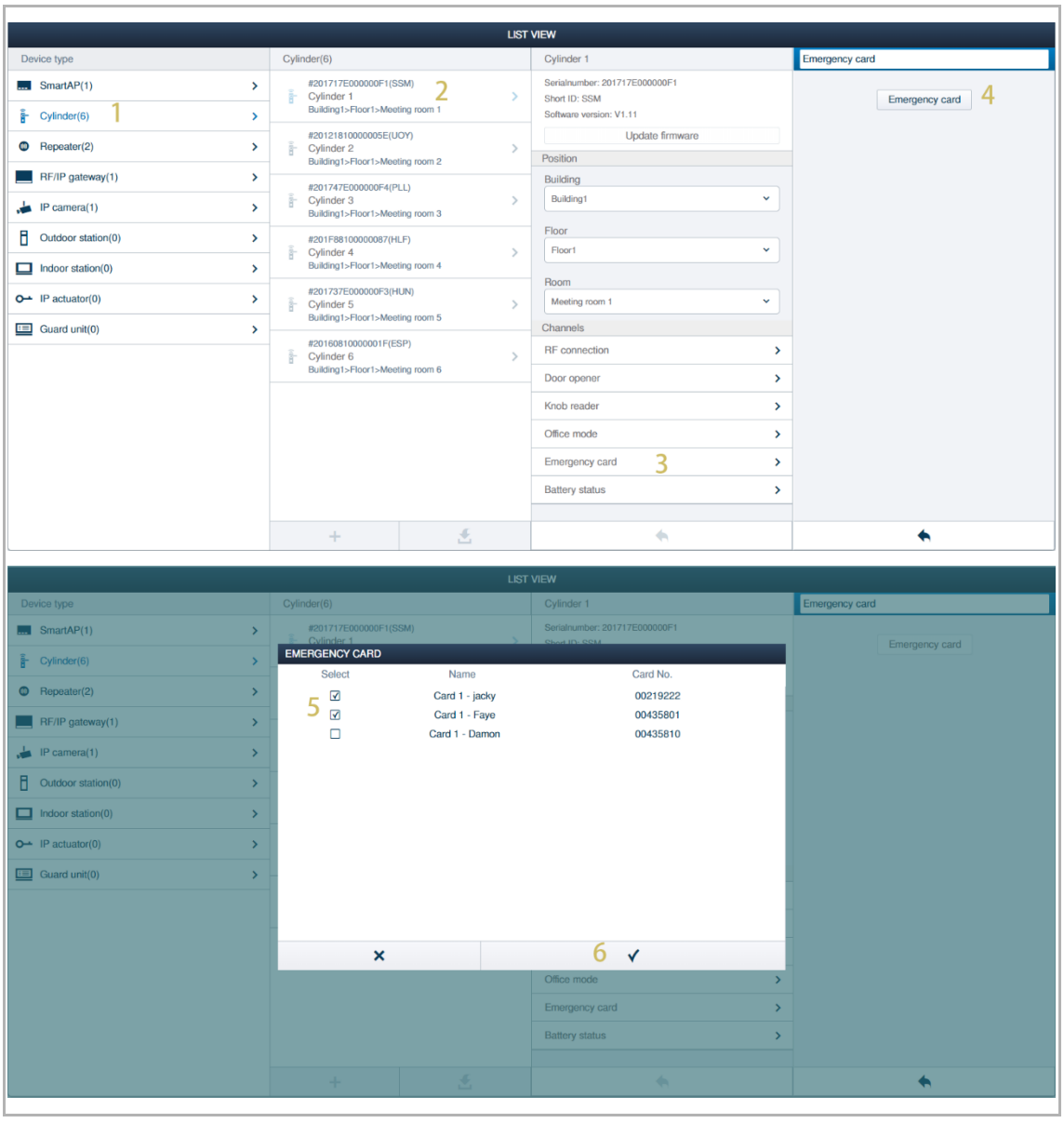
[2] Klik op de "Elektronische slotcilinder".

[3] Klik op "Kaart voor noodgevallen".

[4] Klik op "Kaart voor noodgevallen".

[5] Vink de keuzevakjes aan om noodkaarten toe te voegen.

[6] Klik op "√" om te bevestigen.



2. Noodkaarten verwijderen

Volg de onderstaande stappen:

[1] Klik in het configuratiescherm op "Apparaatconfiguratie" en vervolgens op "Cilinder".

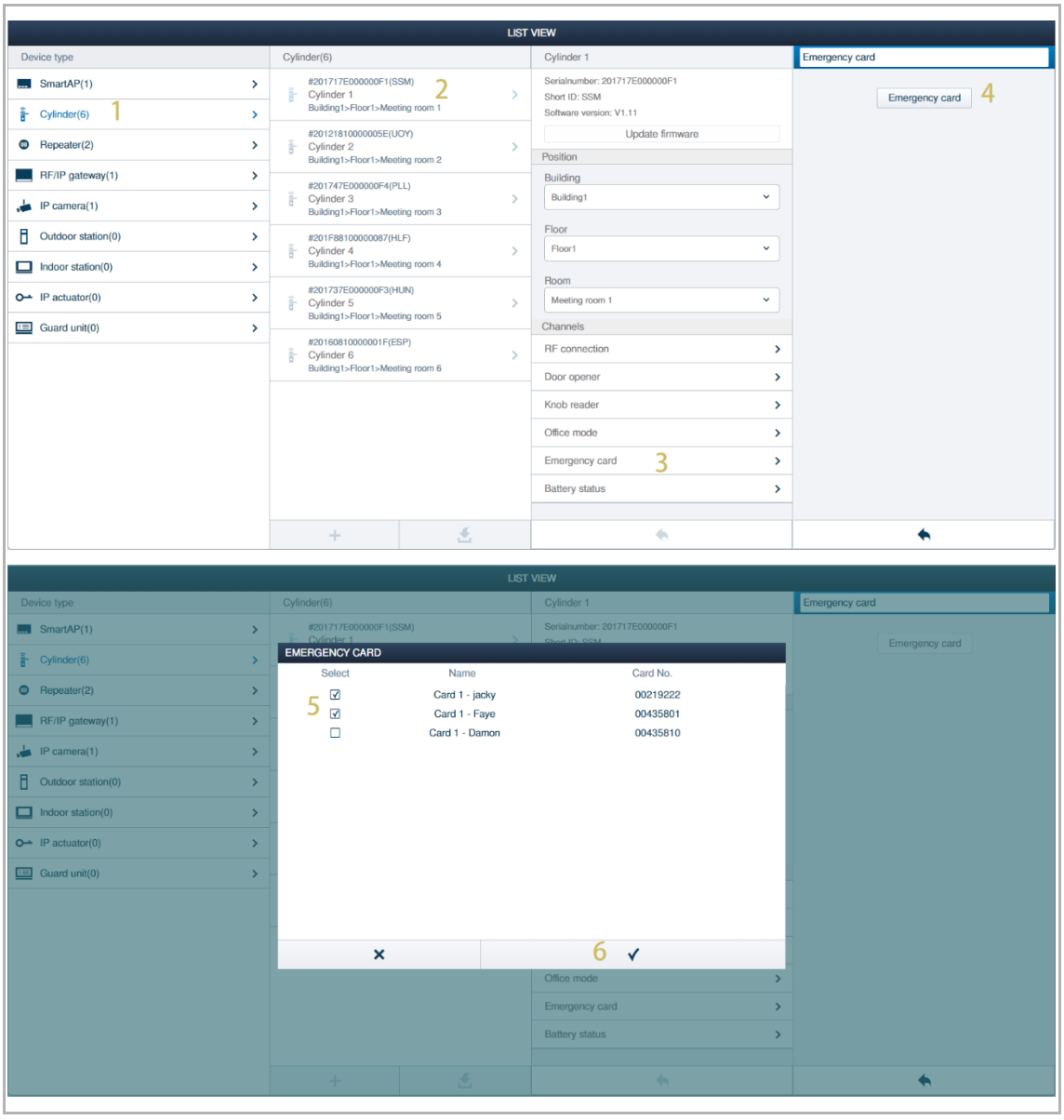
[2] Klik op de "Elektronische slotcilinder".

[3] Klik op "Kaart voor noodgevallen".

[4] Klik op "Kaart voor noodgevallen".

[5] Vink de keuzevakjes af om noodkaarten te verwijderen.

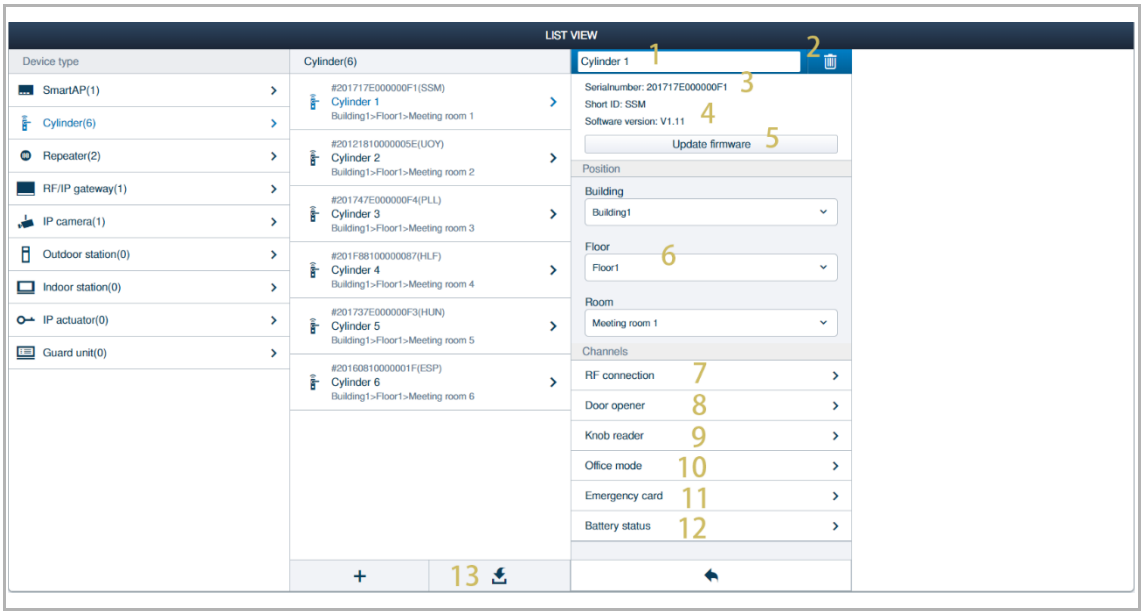
[6] Klik op "√" om te bevestigen.



10.6 Apparaten configureren

10.6.1 "Elektronische slotcilinder" configureren

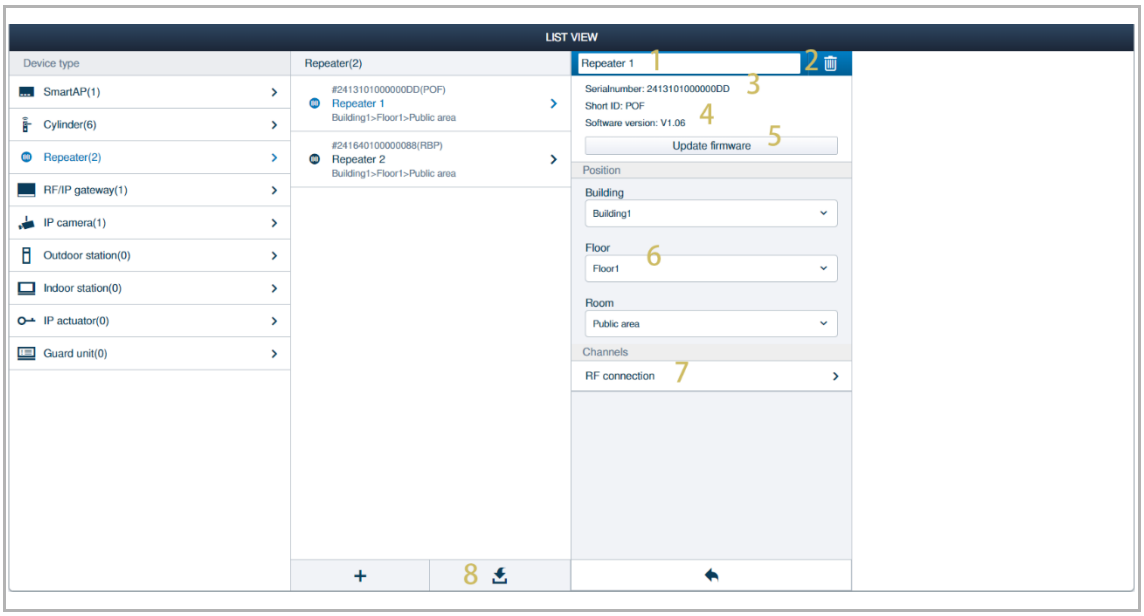
Klik in het configuratiescherm op "Apparaatconfiguratie", "Cilinder, "Cilinder 1" om het configuratiescherm te openen.



Nr.	Beschrijving
1	Geef het apparaat een andere naam.
2	**Apparaat verwijderen** De elektronische slotcilinder moet eerst worden ontkoppeld voordat deze wordt verwijderd.
3	Serienummer van het apparaat.
4	Firmwareversie van het apparaat.
5	Firmware-update via de website.
6	De locatie van het apparaat toewijzen.
7	RF-verbindingsstatus van het apparaat bekijken.
8	Stel de deblokkeringstijd voor de elektronische slotcilinder in.
9	**Stel de offline dag voor de cilinder in.** zie hoofdstuk 10.5.3 “Offline-dag instellen“ op pagina 175.
10	**De kantoormodus-functie activeren/deactiveren** zie hoofdstuk 10.6.4 “Kantoormodus“ op pagina 185.
11	**Noodkaarten beheren** zie hoofdstuk 10.5.4 “Noodkaarten beheren“ op pagina 176.
12	Controleer de batterijstatus van het apparaat.
13	Update de firmwareversie lokaal of op afstand voor meerdere apparaten in een batch.

10.6.2 "RF-repeater" configureren

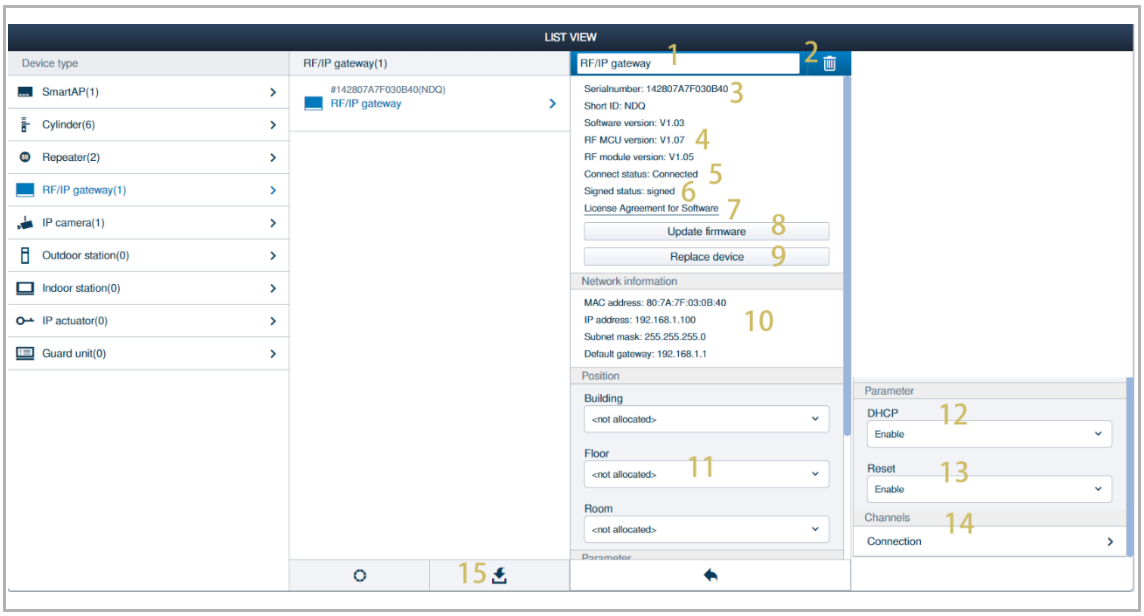
Klik in het configuratiescherm op "Apparaatconfiguratie", "Repeater, "Repeater 1" om het configuratiescherm te openen.



Nr.	Beschrijving
1	Geef het apparaat een andere naam.
2	**Apparaat verwijderen** Het apparaat moet eerst worden ontkoppeld voordat het wordt verwijderd.
3	Serienummer van het apparaat.
4	Firmwareversie van het apparaat.
5	Firmware-update via de website.
6	De locatie van het apparaat toewijzen.
7	RF-verbindingsstatus van het apparaat bekijken.
8	Update de firmwareversie lokaal of op afstand voor meerdere apparaten in batches.

10.6.3 "RF/IP-gateway" configureren

Klik in het configuratiescherm op "Apparaatconfiguratie", "BLE, "Cilinder 1" om het configuratiescherm te openen.



Nr.	Beschrijving
1	Geef het apparaat een andere naam.
2	**Apparaat verwijderen** Klik op " ", gevolgd door "√" om het apparaat te verwijderen.
3	Serienummer van het apparaat.
4	Firmwareversie van het apparaat.
5	"Verbonden" betekent dat de RF/IP-gateway via een LAN-verbinding verbonden met "Smart Access Point" is.
6	"Gesigneerd" betekent dat de RF/IP-gateway met succes gesigneerd is op het Smart Access Point.
7	Klik om de "Licentieovereenkomst voor software" te bekijken.
8	Firmware-update via de website.
9	Zie pagina 181.
10	De netwerkinformatie bekijken.
11	De locatie van het apparaat toewijzen
12	Als "DHCP" is ingesteld op "Deacitveren", moet u het statische IP-adres van het apparaat instellen.
13	Als "Reset" is ingesteld op "Deacitveren", kan de resetknop van de apparaten niet meer worden gebruikt.
14	RF-verbindingsstatus van het apparaat bekijken.
15	Update de firmwareversie lokaal of op afstand voor meerdere apparaten in een batch.

Een apparaat vervangen

U kunt een nieuwe RF/IP-gateway gebruiken om de oude te vervangen als deze kapot is. Alle gegevens (inclusief de positie en de verbinding) van de oude gateway worden naar de nieuwe gekopieerd.

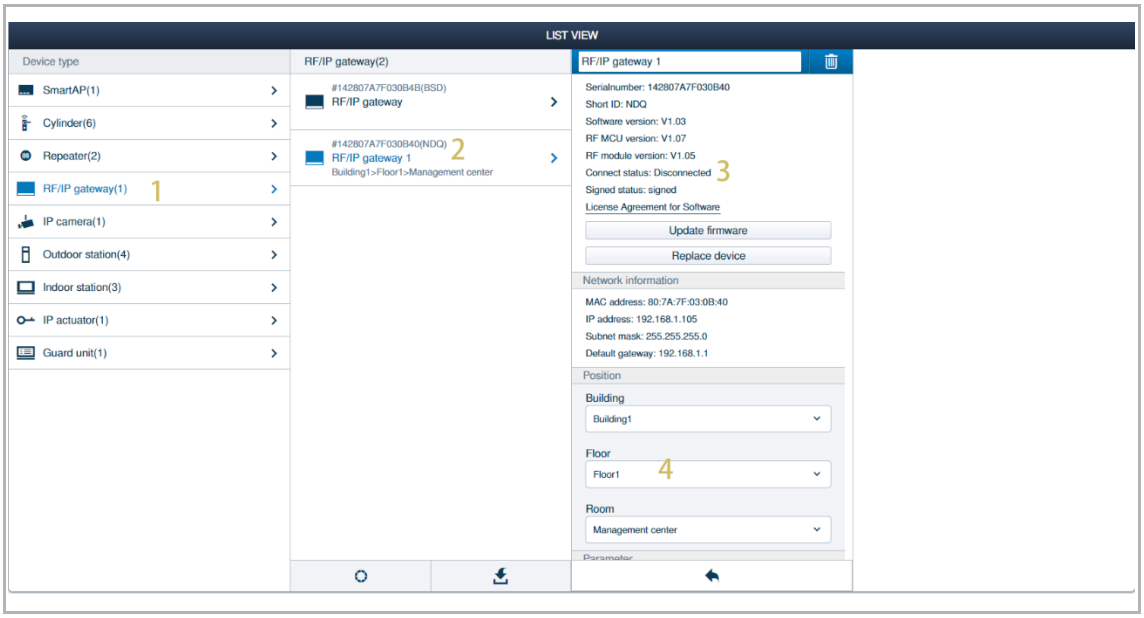
Volg de onderstaande stappen:

[1] Klik in het scherm "Apparaatconfiguratie" op "BLE".

[2] Klik op de "BLE 1".

[3] De verbindingsstatus moet "Ontkoppeld" zijn als de verbinding met de oude gateway is verbroken.

[4] De positie van de oude gateway wordt weergegeven op het scherm.



[5] Voeg de nieuwe gateway toe zonder een positie. zie hoofdstuk 10.3.4 “Toevoegen en lokaliseren van een "RF/IP-gateway".“ op pagina 158

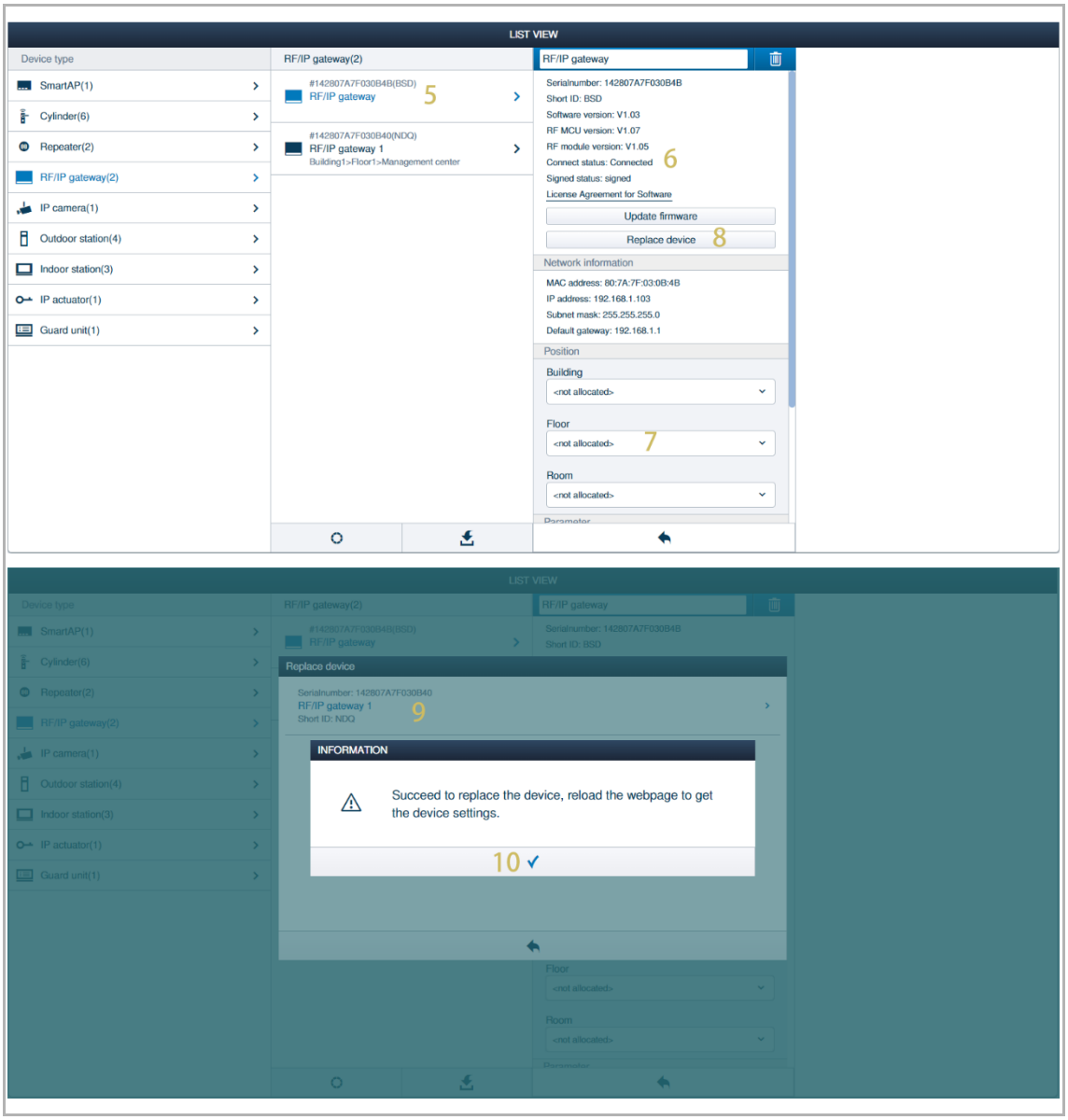
[6] De verbindingsstatus van de nieuwe gateway moet "Verbonden" zijn.

[7] De positie van de nieuwe gateway is momenteel leeg.

[8] Klik op "Apparaat vervangen" op de nieuwe gateway.

[9] Klik op de oude gateway in de lijst.

[10]Klik op "√" om door te gaan de vervanging van het apparaat gelukt is.

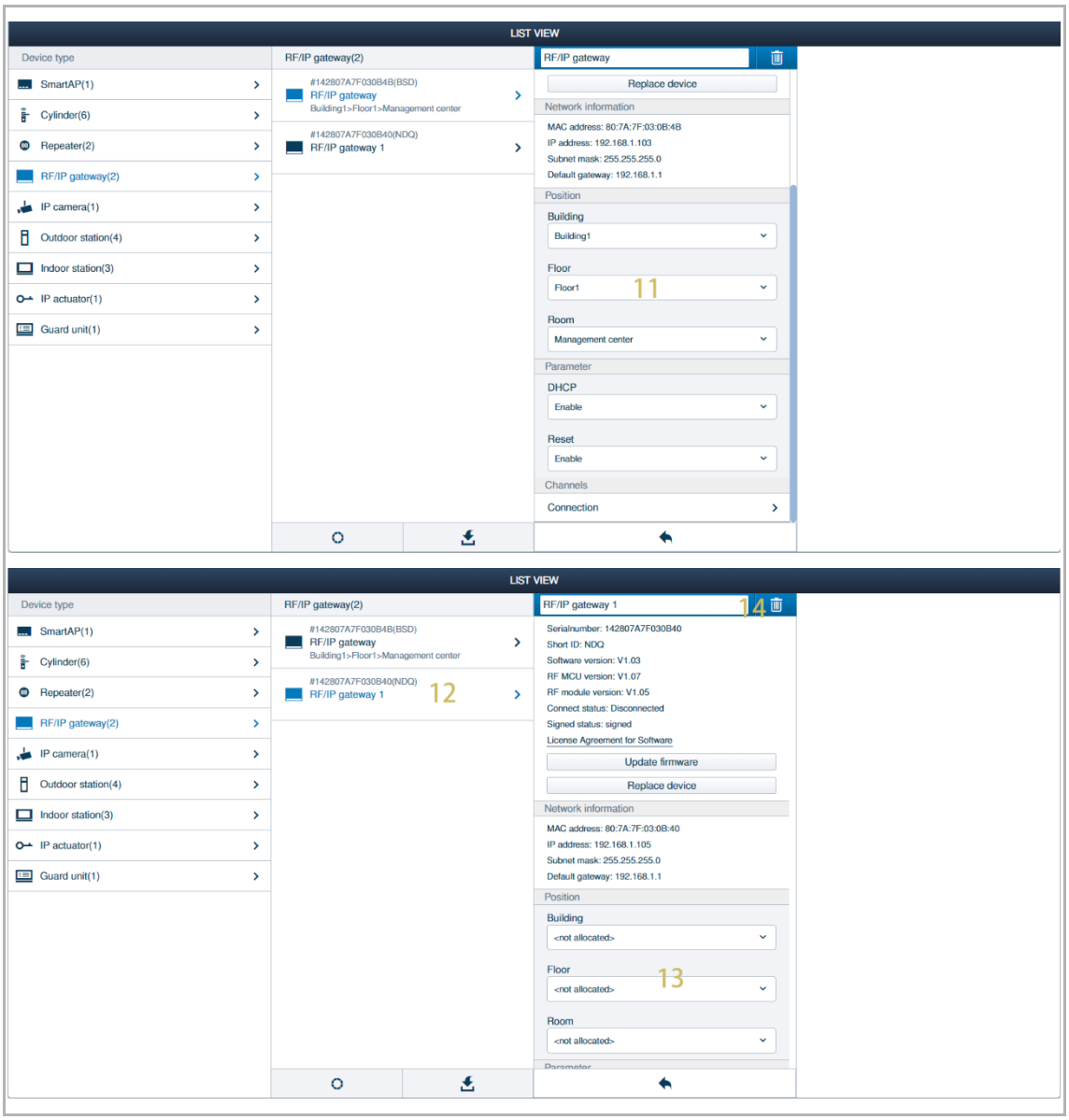


[11]De positie van de oude gateway wordt gekopieerd naar de nieuwe (de verbindingen op de oude worden ook gekopieerd naar de nieuwe).

[12]Klik op de oude gateway.

[13]De positie van de oude gateway is leeg. (De verbindingen van de oude gateway zijn ook gewist).

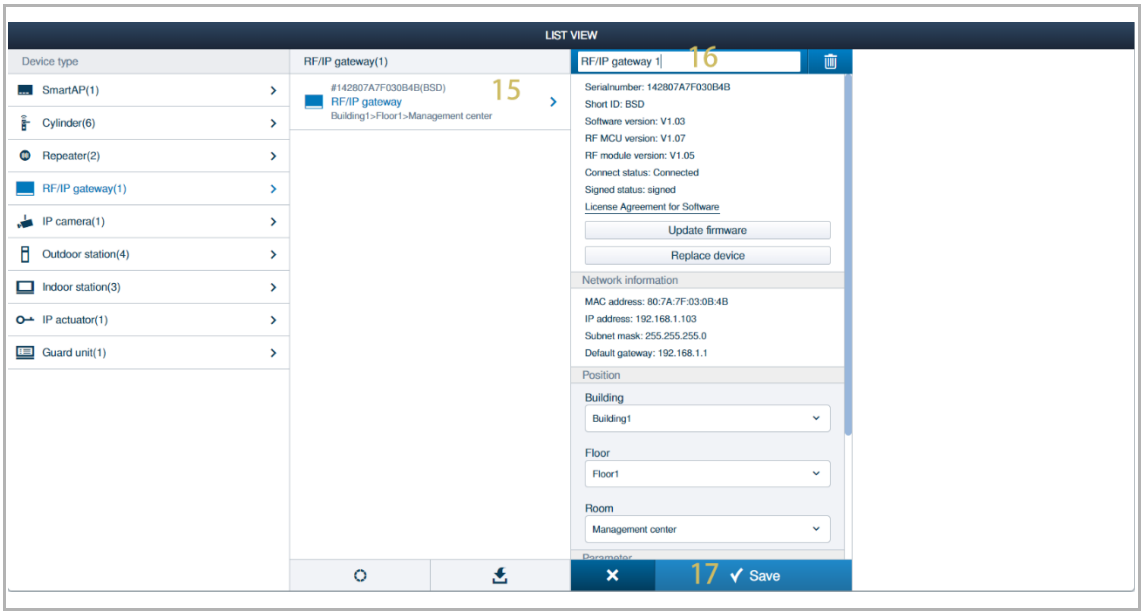
[14]Klik op " ", gevolgd door "√" om de oude gateway te verwijderen.



[15]Klik op de nieuwe gateway.

[16]Geef de nieuwe gateway een andere naam.

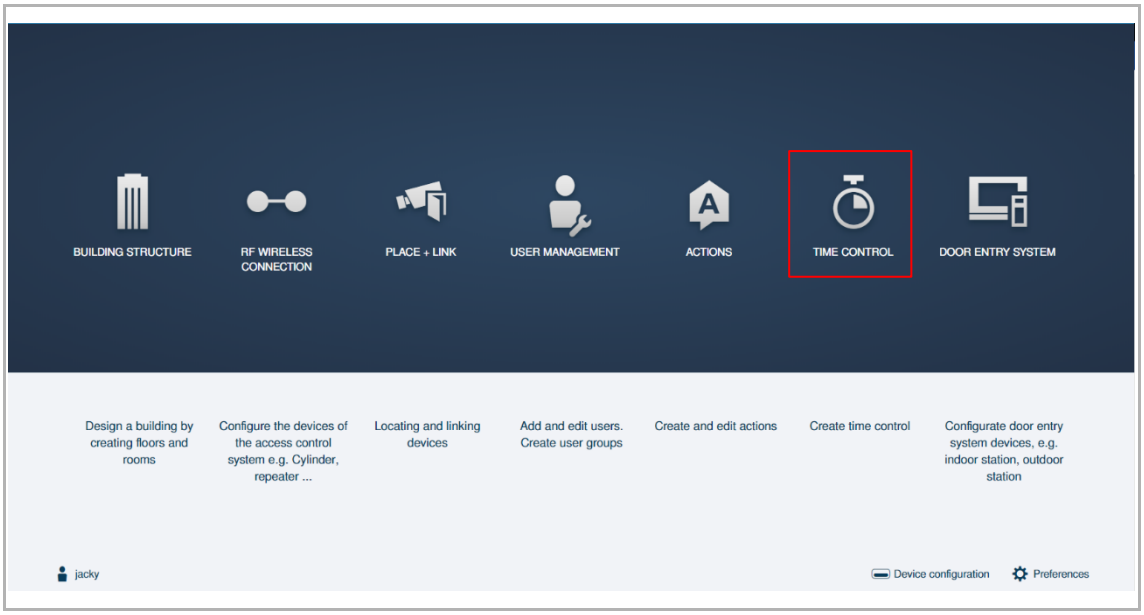
[17]Klik op "√" om op te slaan.



10.6.4 Kantoormodus

"Tijdscontrole"-scherm oproepen

Klik in het configuratiescherm op "Tijdscontrole" om het scherm "Tijdscontrole" te openen.



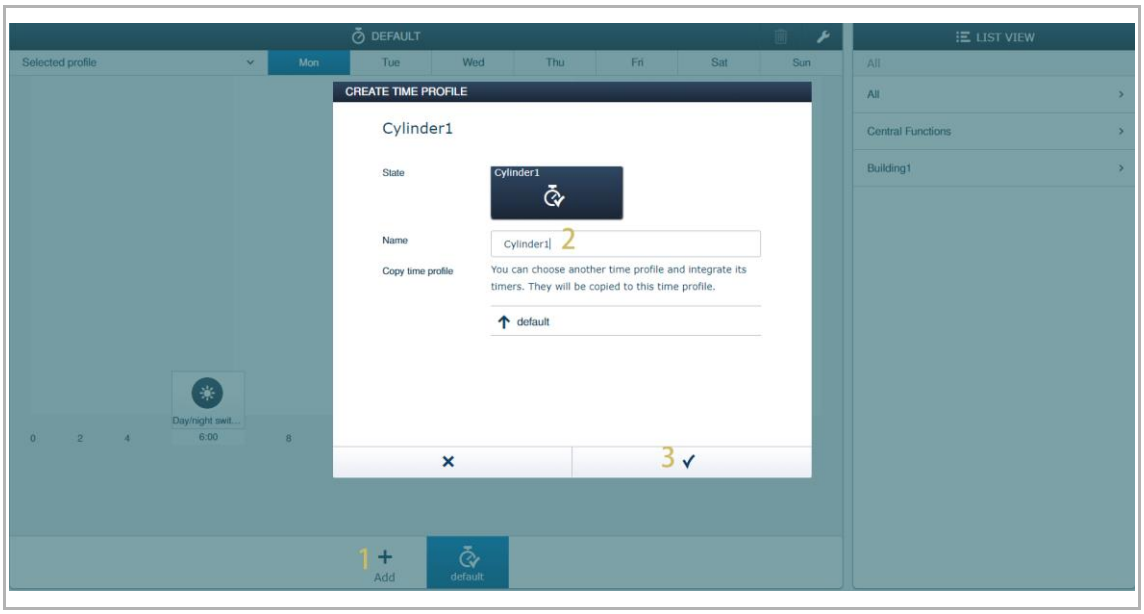
1. Kantoormodus-tijdsprofiel toevoegen voor de betreffende elektronische slotcilinder

Volg de onderstaande stappen:

[1] Op het scherm "Tijdscontrole" klikt u op "Toevoegen".

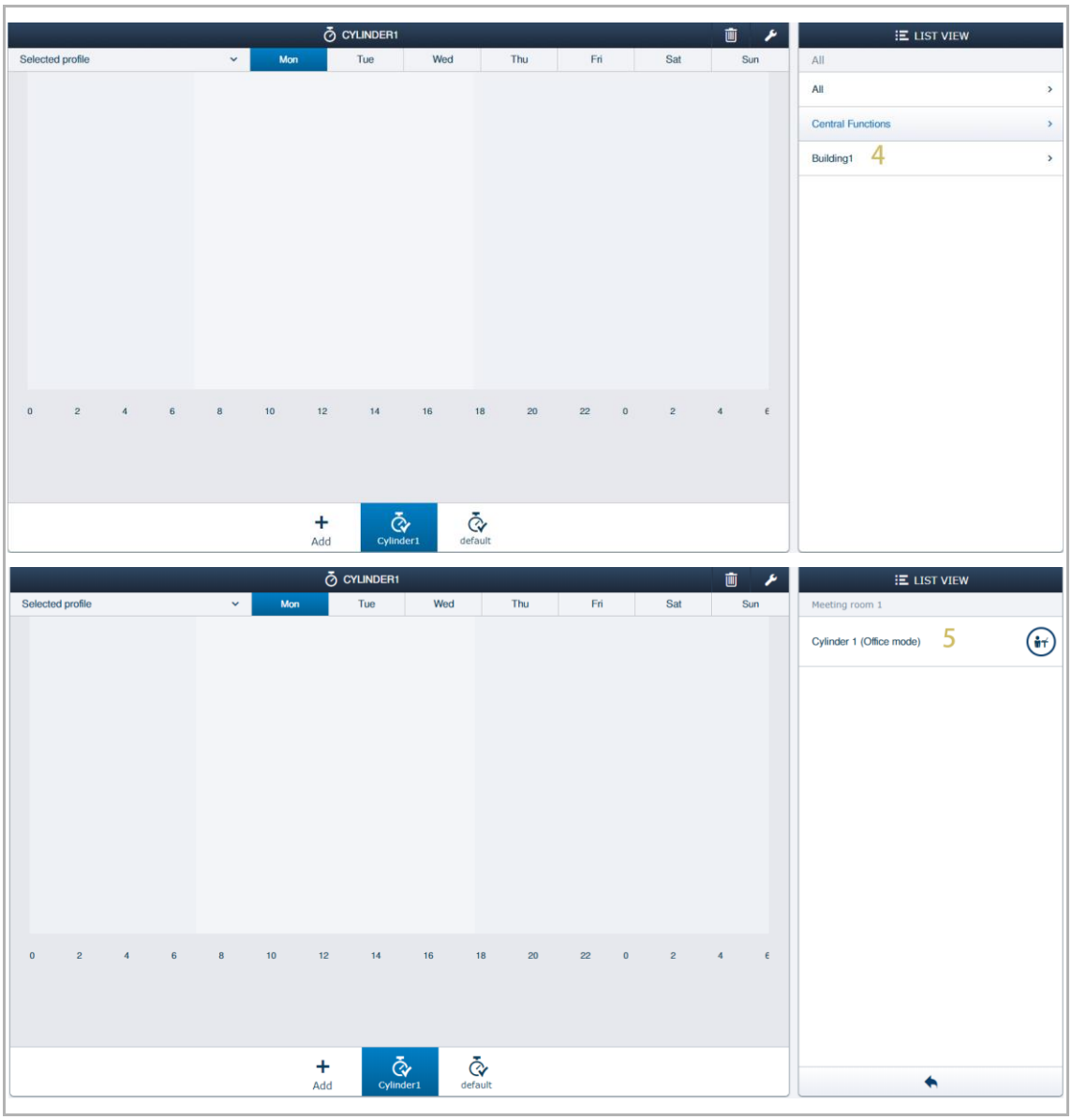
[2] Voer de naam in (bijv. "Cilinder1").

[3] Klik op "√" om op te slaan.



[4] Klik op "Gebouw1">>"Etage 1">>"Vergaderzaal 1" om naar de locatie van de betreffende elektronische slotcilinder te gaan.

[5] Klik op de "Elektronische slotcilinder" (bijv. "Cilinder 1").

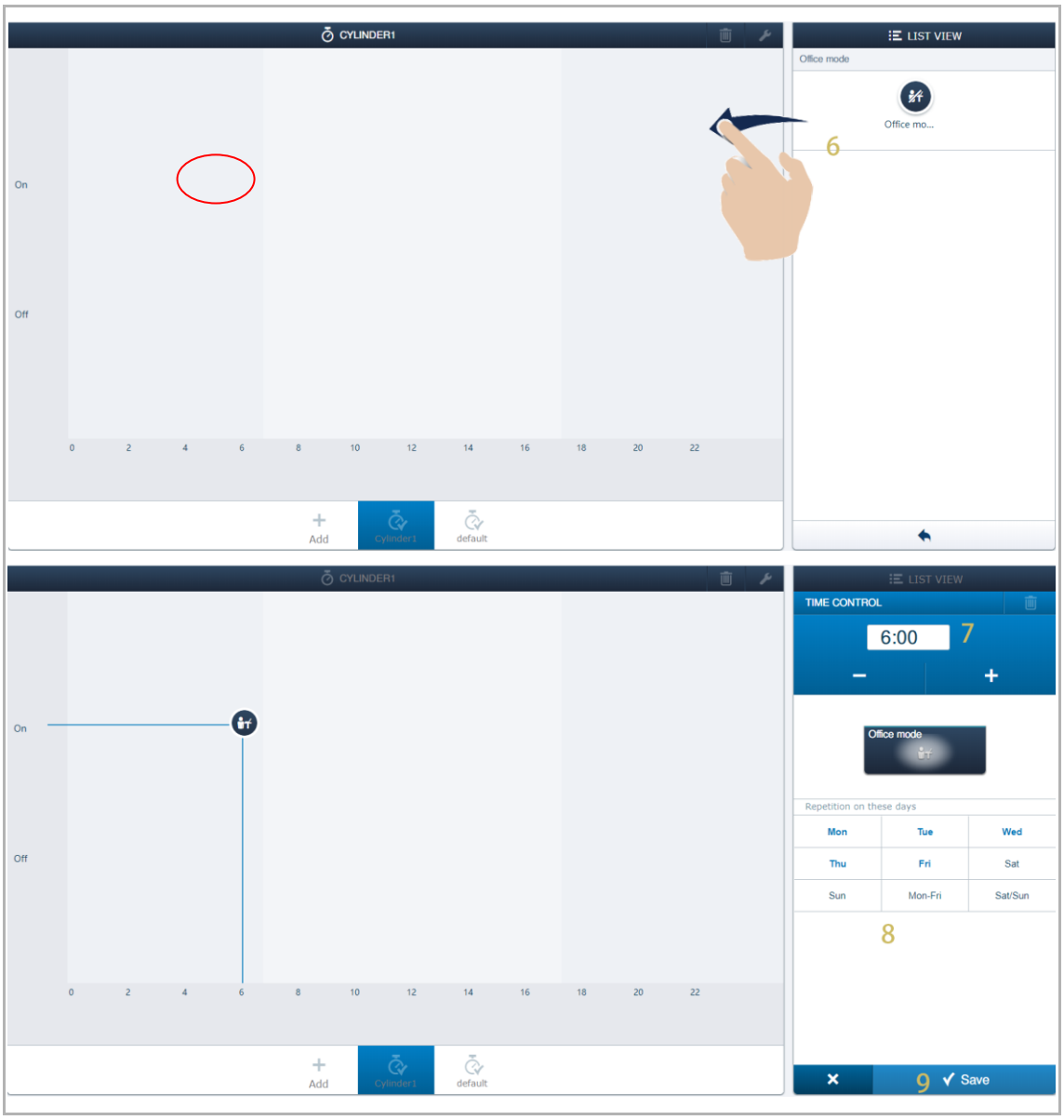


[6] Sleep het symbool voor de kantoormodus naar de "Aan"-positie op het scherm.

[7] Voer de precieze tijd in.

[8] Klik op de betreffende dag om de selectie te annuleren (optioneel).

[9] Klik op "√" om op te slaan.

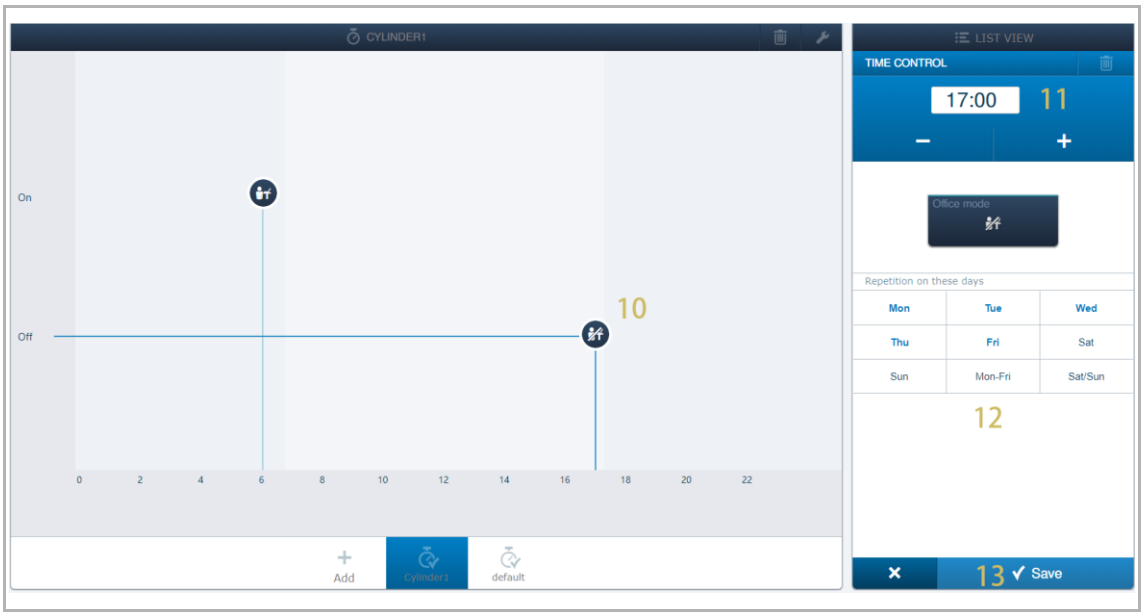


[10]Sleep het symbool voor de kantoormodus naar de "Uit"-positie op het scherm.

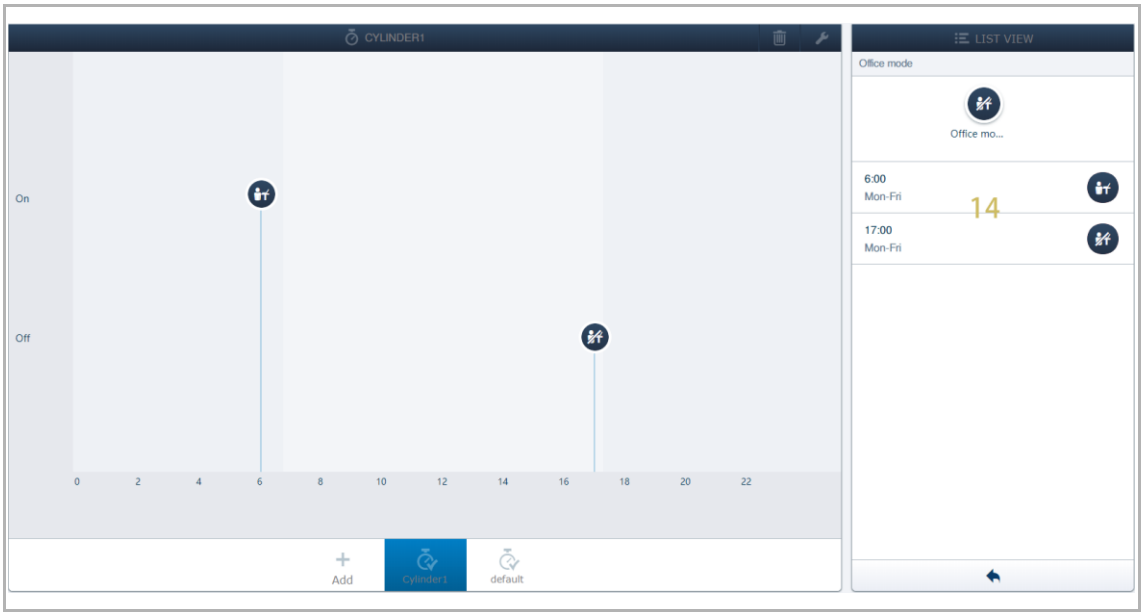
[11]Voer de precieze tijd in.

[12]Klik op de betreffende dag om de selectie te annuleren (optioneel).

[13]Klik op "√" om op te slaan.



[14]Het resultaat wordt weergegeven op het scherm.



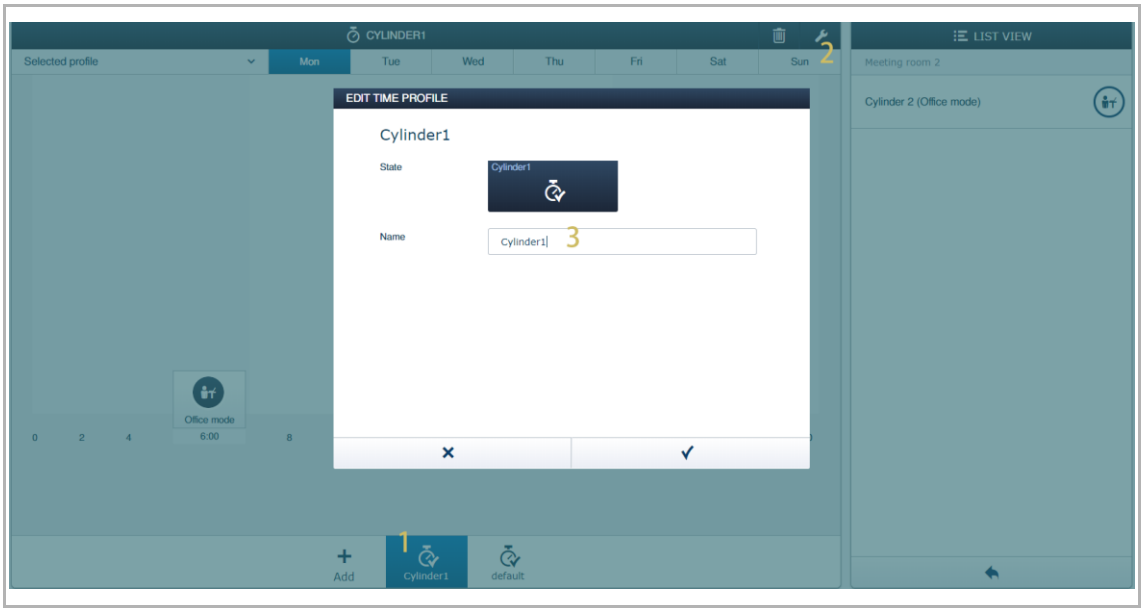
2. Kantoormodus-tijdsprofiel hernoemen voor de betreffende elektronische slotcilinder

Volg de onderstaande stappen:

[1] Klik op het scherm "Tijdscontrole op de betreffende "Elektronische slotcilinder" (bijv. "Cilinder 1").

[2] Klik op " ".

[3] Voer een nieuwe naam in.



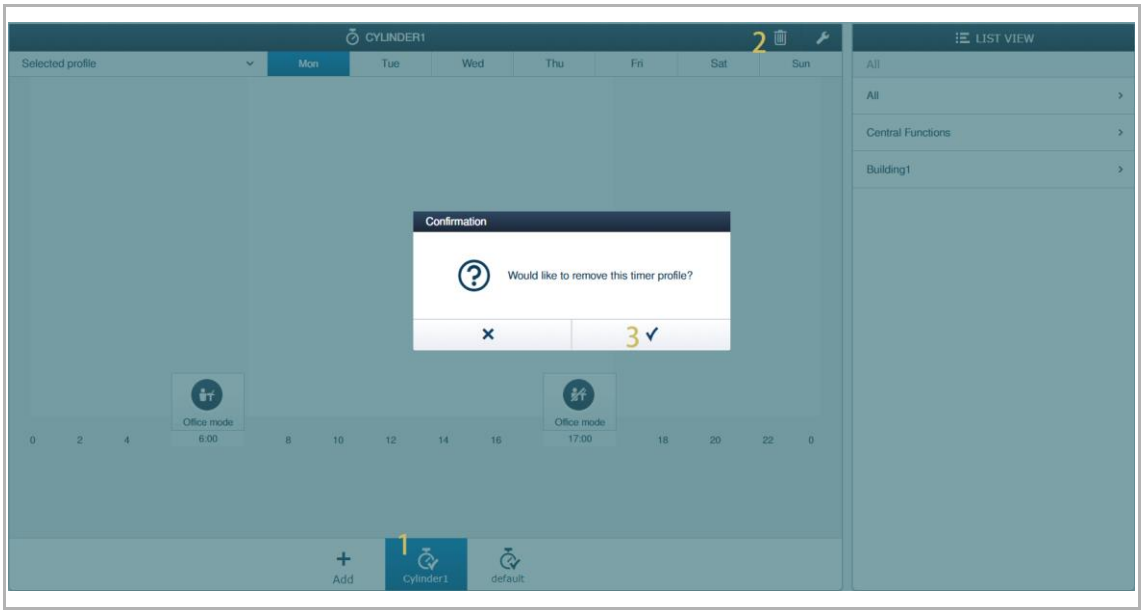
3. Kantoormodus-tijdsprofiel verwijderen voor de betreffende elektronische slotcilinder

Volg de onderstaande stappen:

[1] Klik op het scherm "Tijdscontrole op de betreffende "Elektronische slotcilinder" (bijv. "Cilinder 1").

[2] Klik op "".

[3] Klik op "√" om te bevestigen.

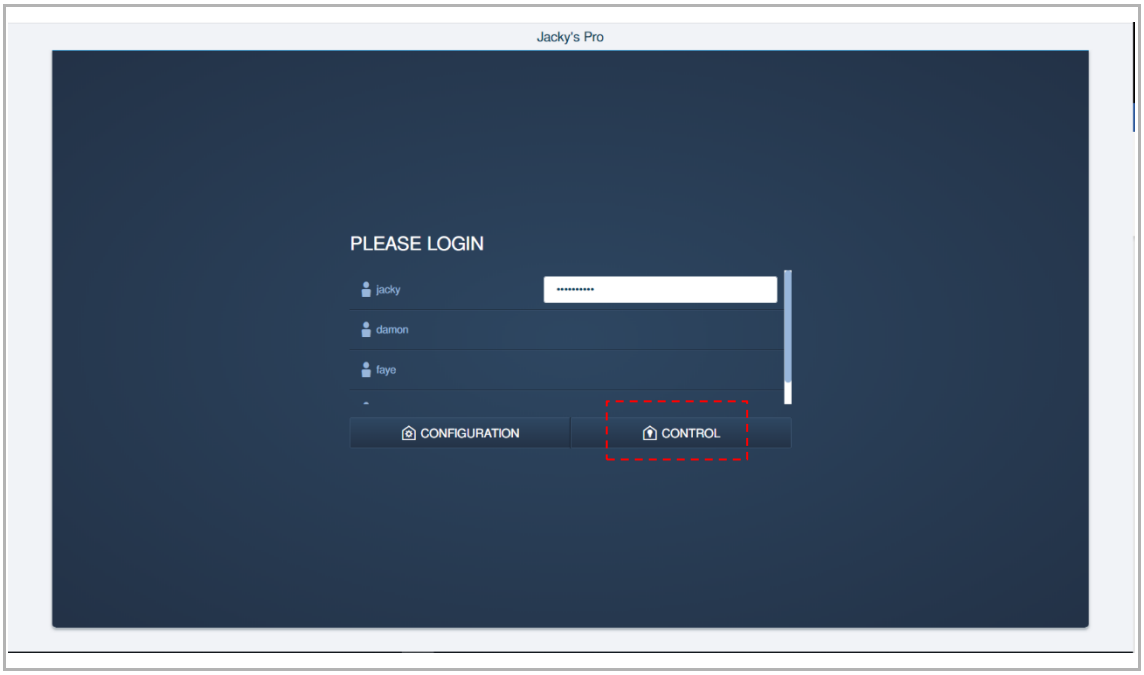


10.7 Apparaten besturen via het "Smart Access Point"

Besturingsscherm oproepen

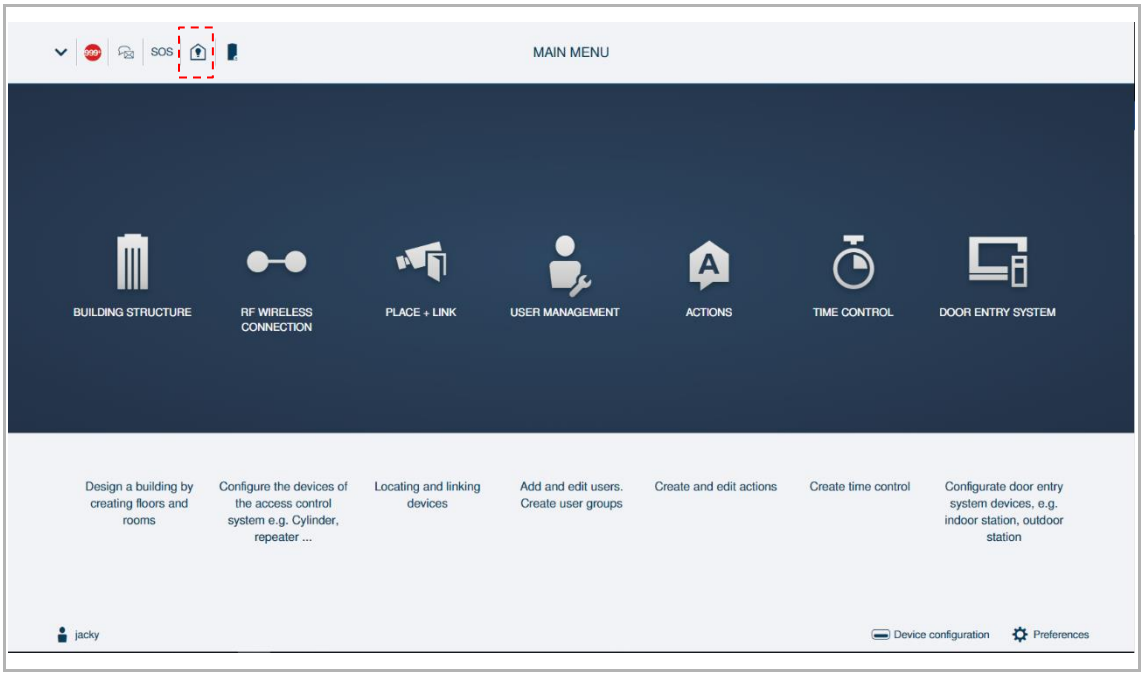
1. Alle gebruikers kunnen de onderstaande handeling uitvoeren:

Voer op het inlogscherm het wachtwoord in en klik op "Besturing" om toegang te krijgen tot het betreffende scherm.



2. Alleen admin-gebruikers kunnen de onderstaande handeling uitvoeren:

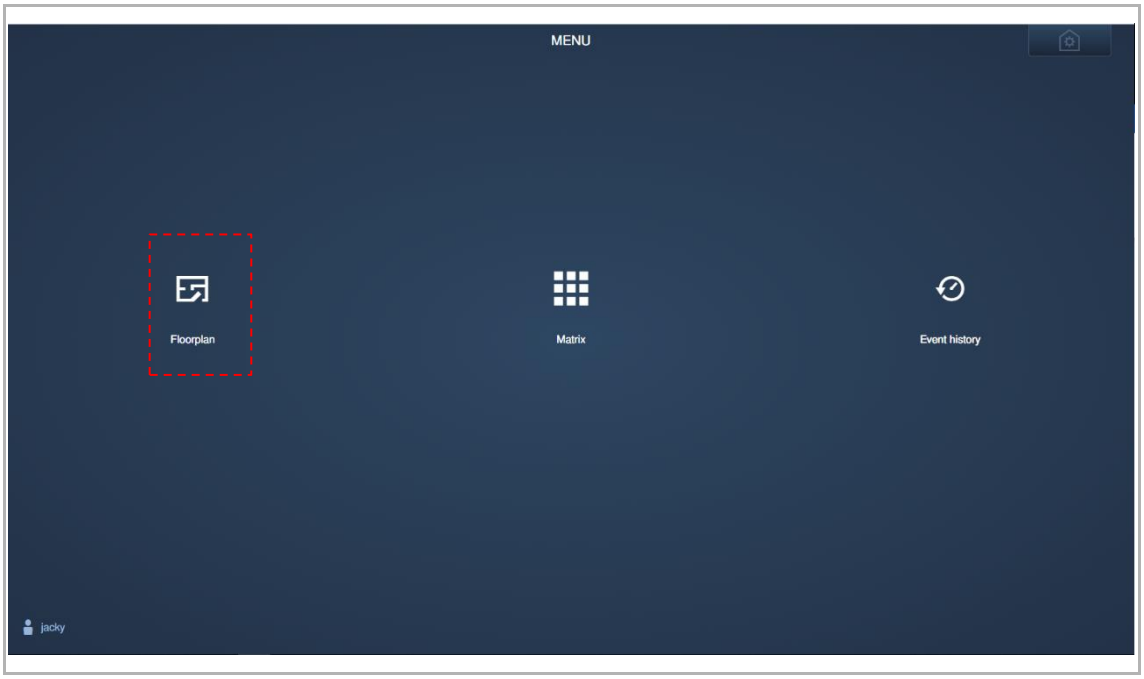
Klik in het configuratiescherm op " " om het besturingsscherm te openen.



10.7.1 Apparaten besturen via de plattegrond

Etagescherm oproepen

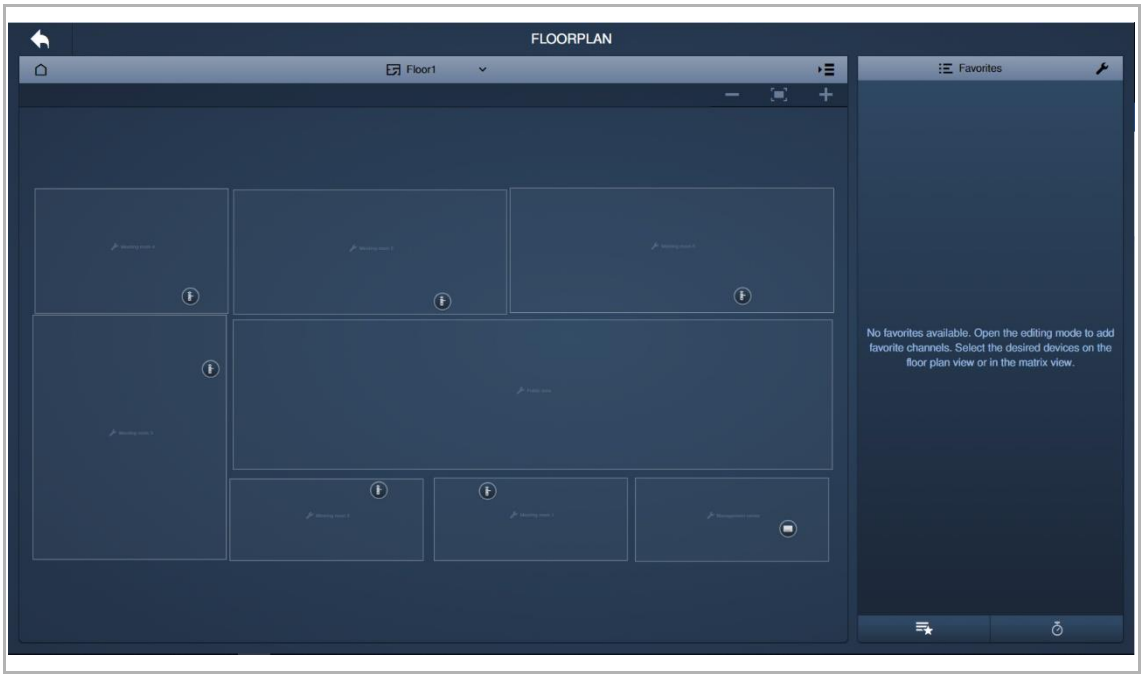
Klik in het besturingsscherm "Plattegrond" om het bijbehorende scherm te openen.



Opmerking

De volgende bewerkingen zijn gebaseerd op demonstratie 1. U moet uw bewerkingen aanpassen wanneer u aan een echt project werkt.

Klik op "Gebouw 1", "Etage 1" om toegang te krijgen tot het etagescherm.

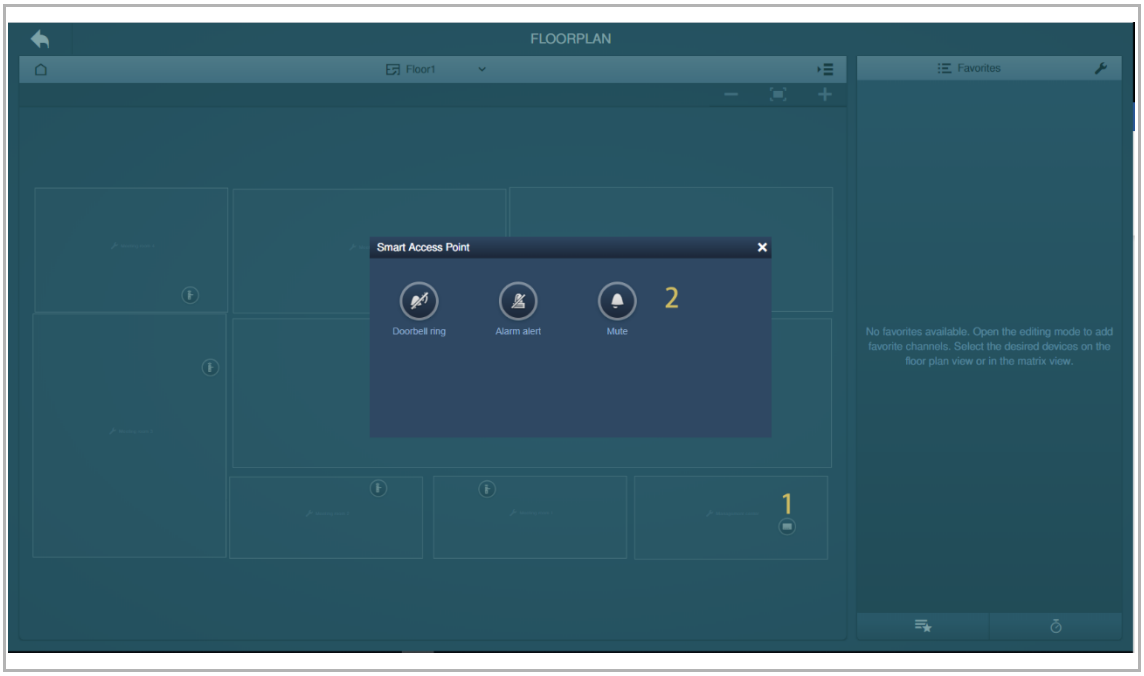


1. Functie van "Smart Access Point" besturen

Volg de onderstaande stappen:

[1] Klik op het etagescherm op "Smart Access Point".

[2] Klik op een functiesymbool om de functie uit te voeren.

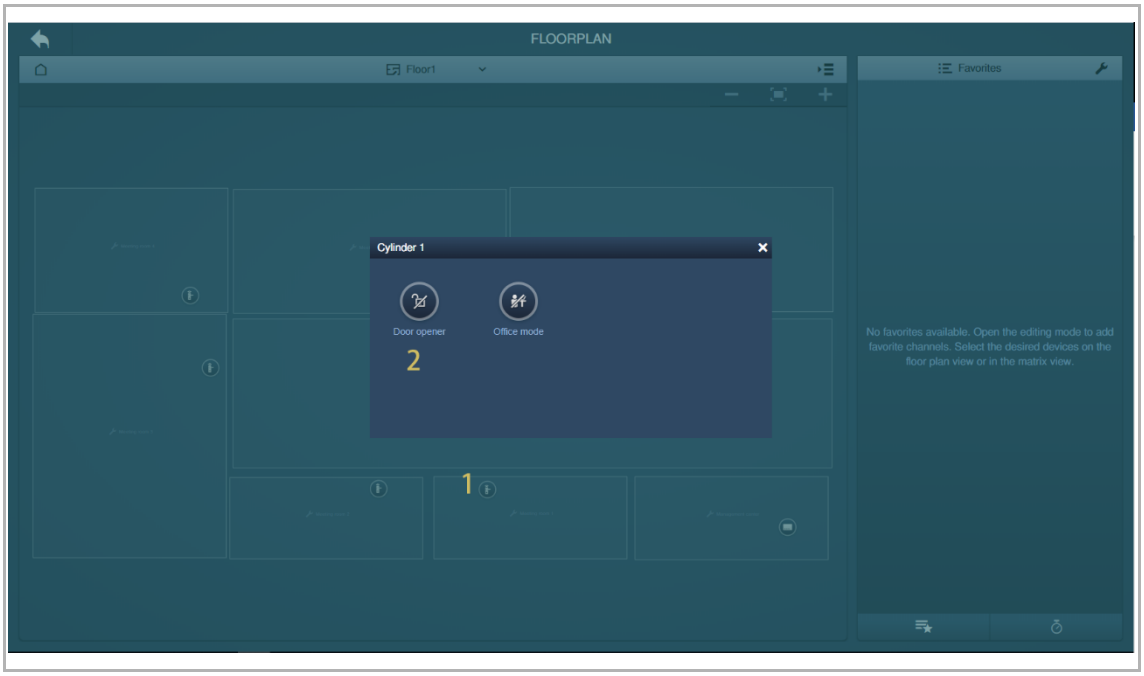


2. "Elektronische slotcilinder" deblokkeren.

Volg de onderstaande stappen:

[1] Klik op het etagescherm op de betreffende "Elektronische slotcilinder" (bijv. "Cilinder 1" voor demonstratie 1).

[2] Klik op "Deblokkeren"-symbool om de elektronische slotcilinder te deblokkeren.

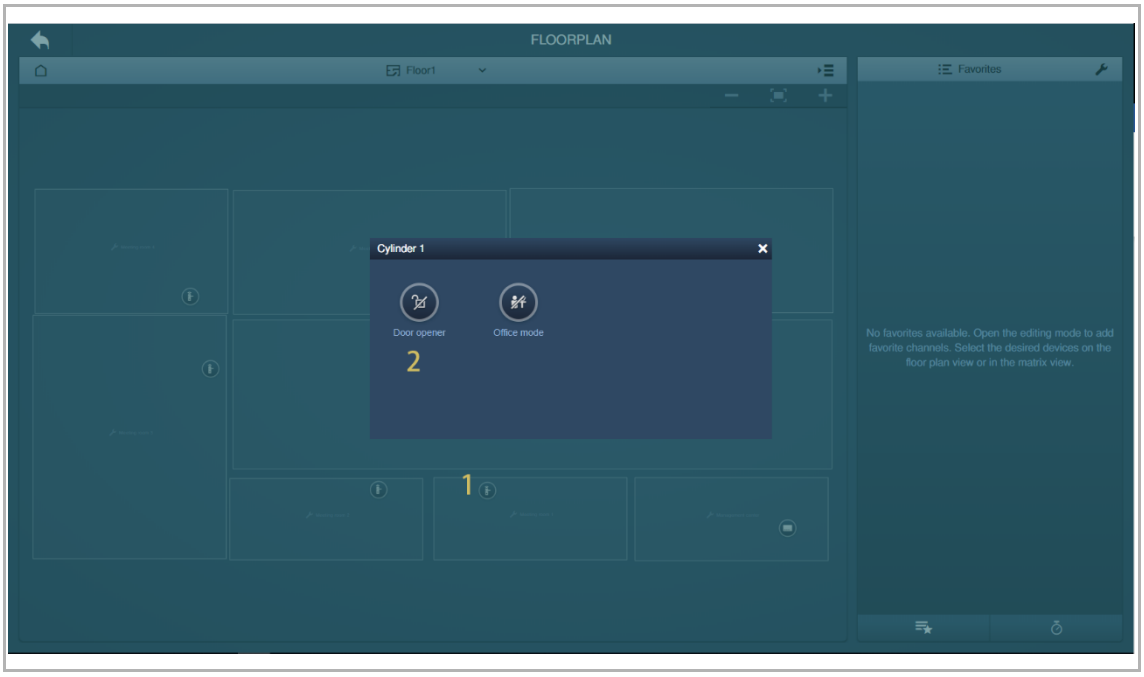


3. Kantoor een mooi activeren/deactiveren voor de betreffende elektronische slotcilinder

Volg de onderstaande stappen:

[1] Klik op het etagescherm op de betreffende "Elektronische slotcilinder" (bijv. "Cilinder 1" voor demonstratie 1).

[2] Klik op het "kantoormodus"-symbool om de kantoormodus-functie te activeren/deactiveren, zie hoofdstuk 10.6.4 “Kantoormodus“ op pagina 185.

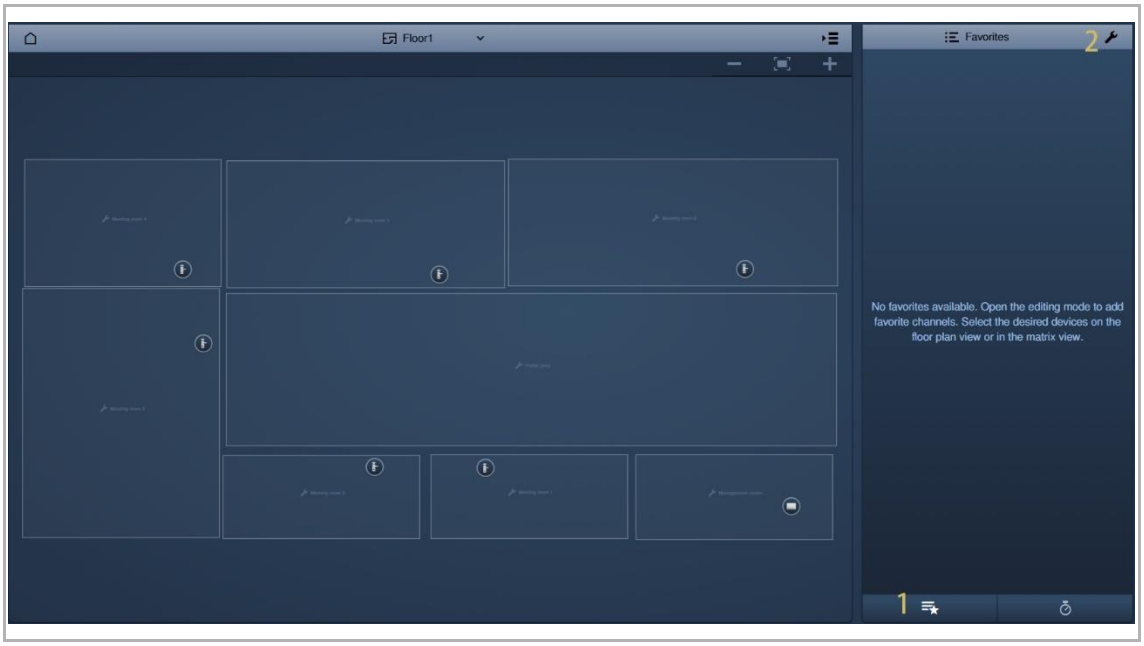


4. Handelingen toevoegen aan de favorietenlijst

Volg de onderstaande stappen:

[1] Klik op het etagescherm op "".

[2] Klik op "": een markering geeft de instellingsstatus aan.



[3] Op de intstellingsstatus klik u op een AccessControl-apparaat (bijv. "Cilinder1").

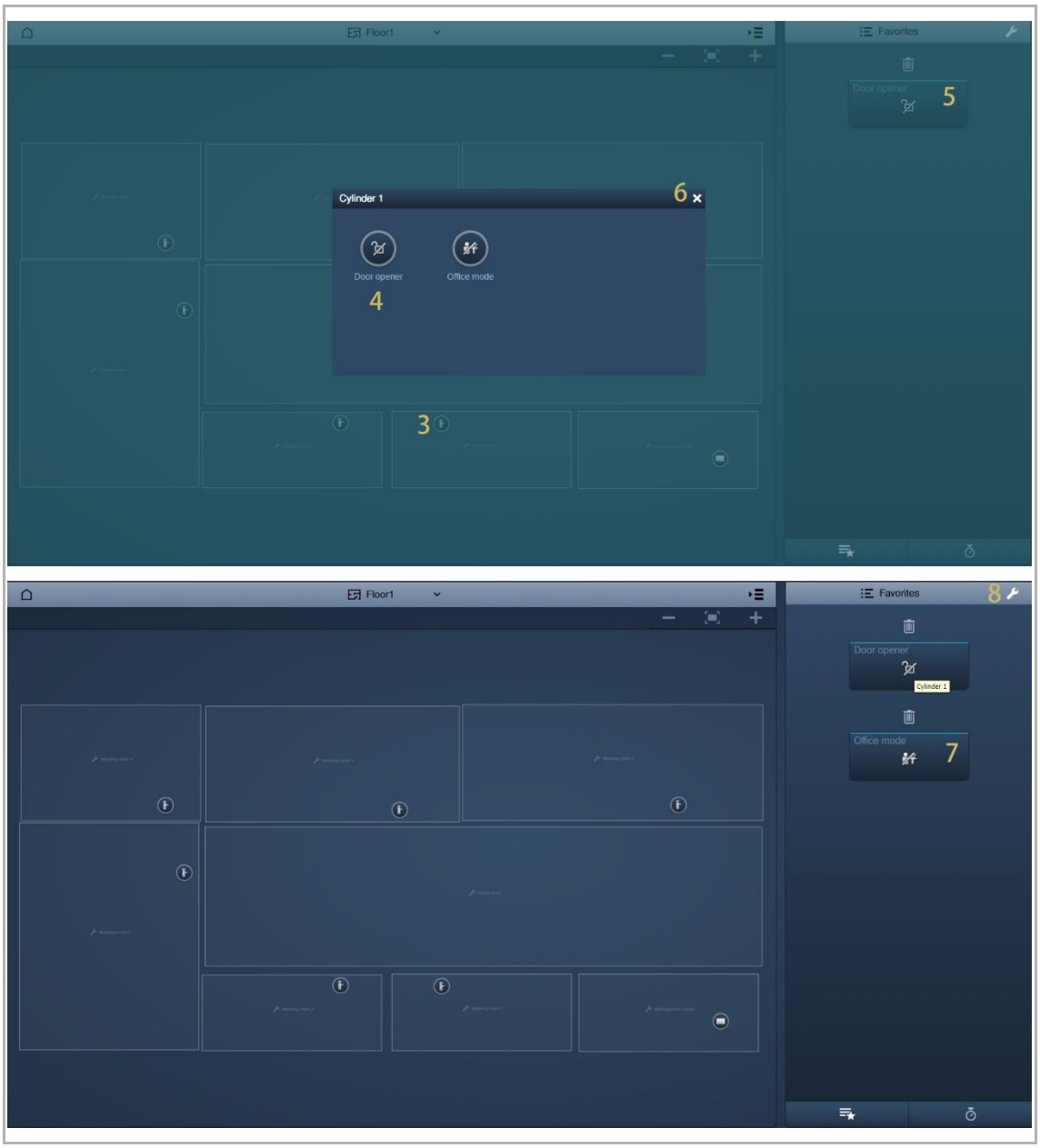
[4] Klik op een functiesymbool (bijv. "Deblokkeren").

[5] Het functiesymbool wordt toegevoegd aan de favorietenlijst.

[6] Klik op "x" om het pop-upvenster te sluiten.

[7] Herhaal stappen 3-6 om andere handelingen één voor één toe te voegen.

[8] Klik op " " om de instellingsstatus te verlaten.

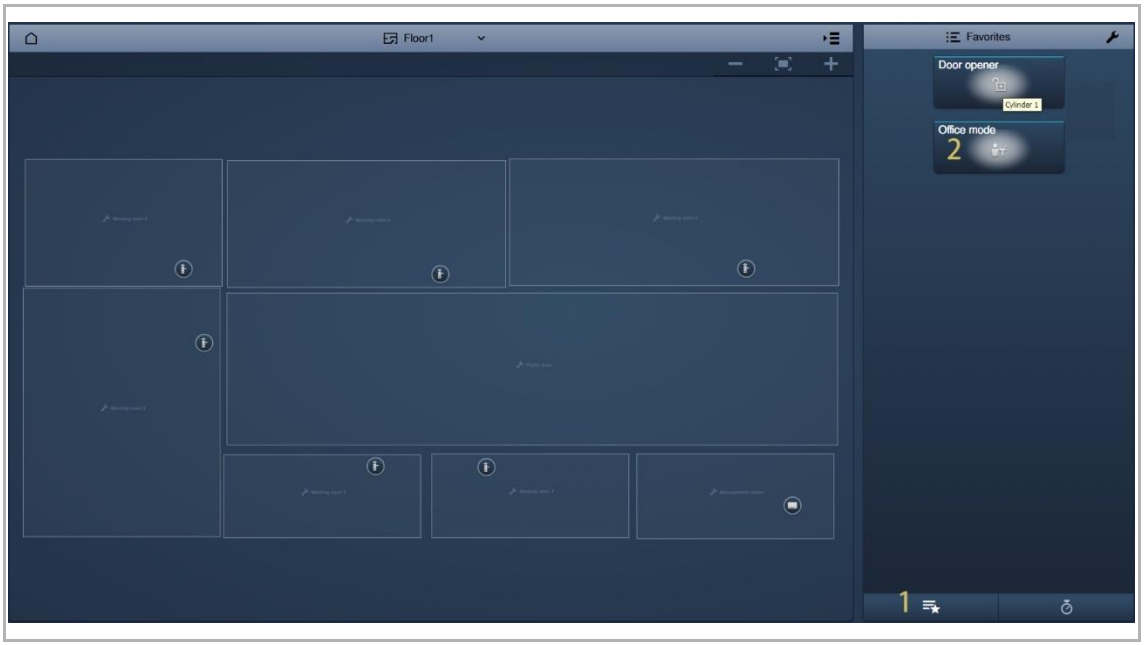


5. Functies in de favorietenlijst bedienen

Volg de onderstaande stappen:

[1] Klik op het etagescherm op "".

[2] Klik op het betreffende functiesymbool in de favorietenlijst om de functie te activeren/deactiveren, de markering geeft de geactiveerde status aan.



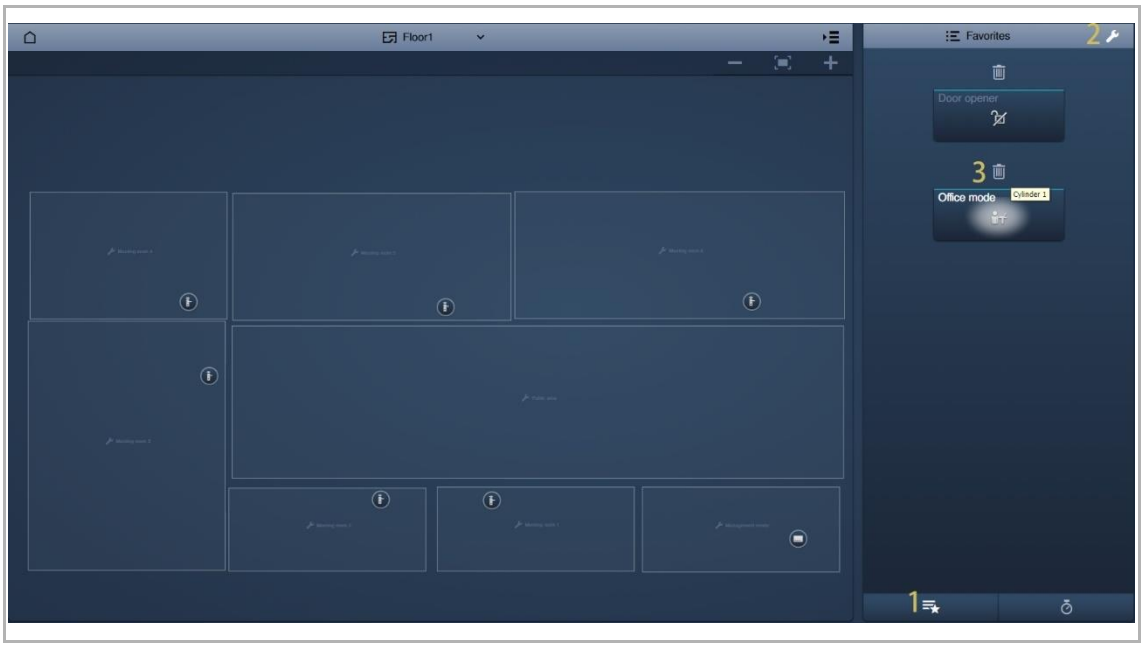
6. Functies uit de favorietenlijst verwijderen

Volg de onderstaande stappen:

[1] Klik op het etagescherm op " ".

[2] Klik op " ": een markering geeft de instellingsstatus aan.

[3] Klik op " " om deze direct te verwijderen.



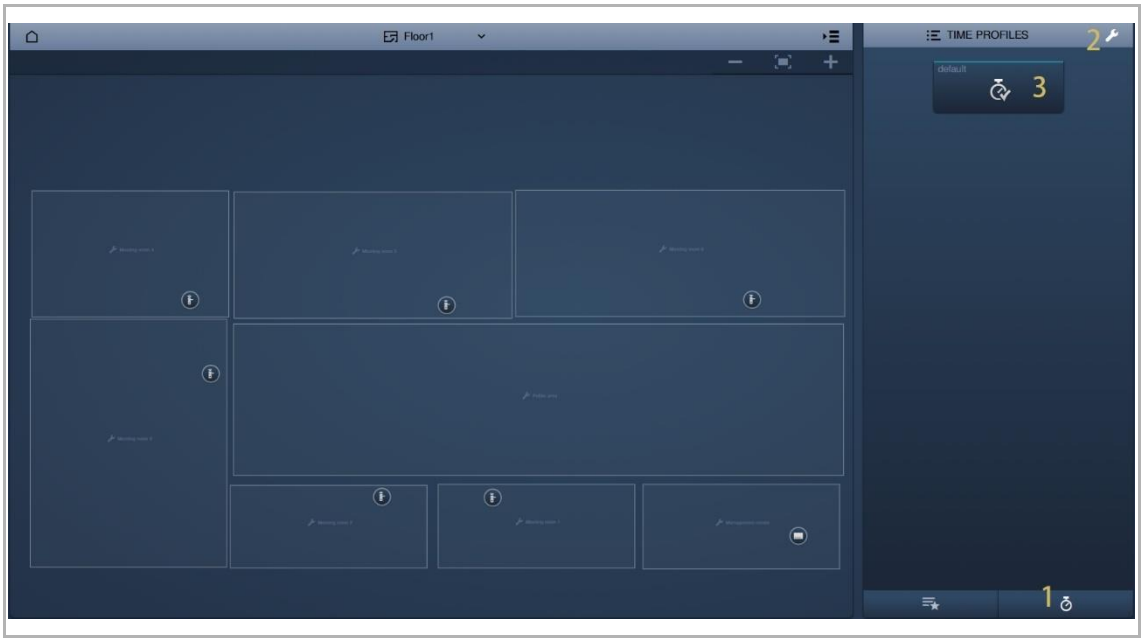
7. Tijdprofielen activeren/deactiveren

Volg de onderstaande stappen:

[1] Klik op het etagescherm op "".

[2] Klik op "": een markering geeft de instellingsstatus aan.

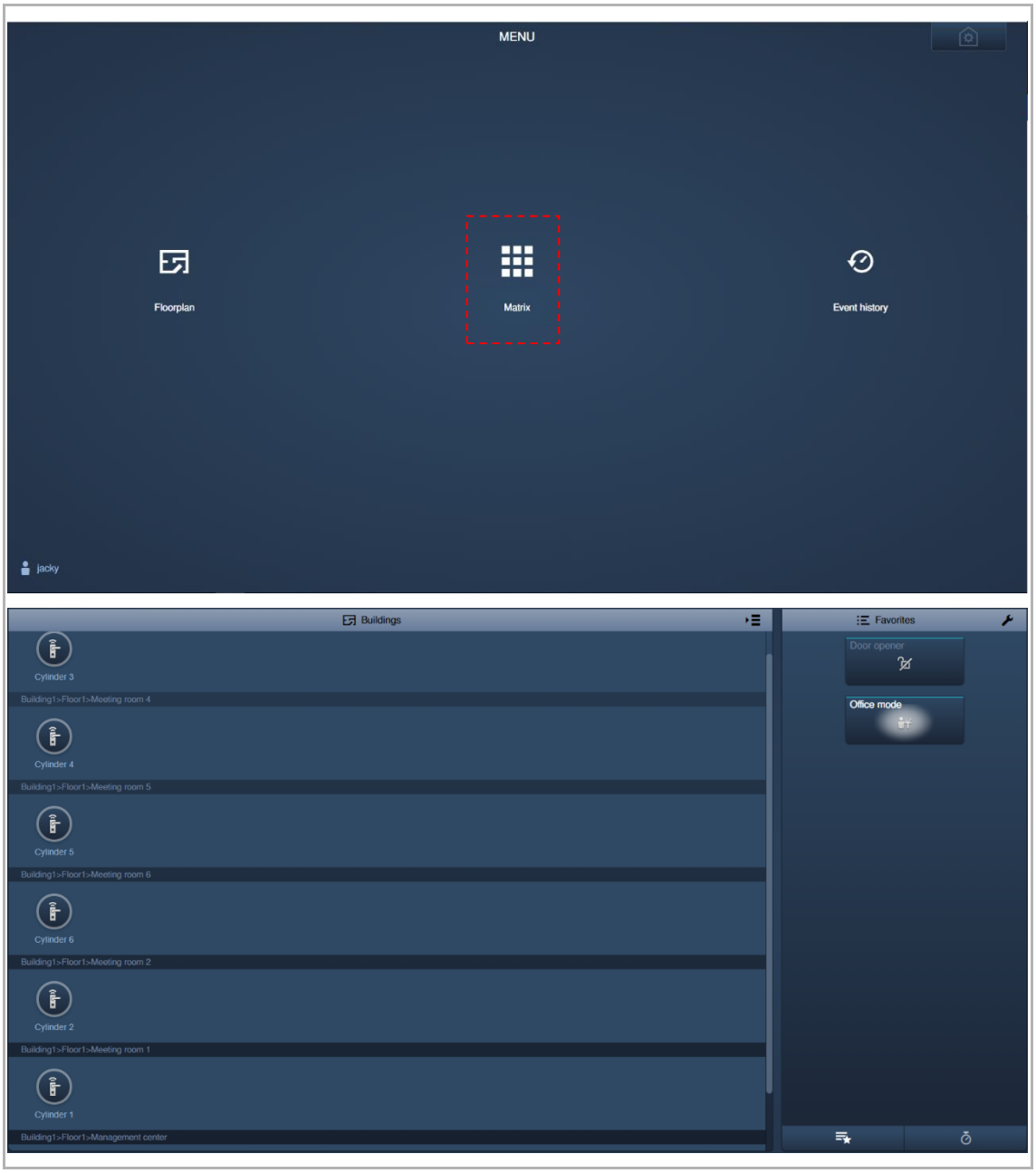
Klik op het "tijdprofiel"-symbool om de tijdprofielfunctie te activeren/deactiveren.



10.7.2 Apparaten besturen via matrix

Matrix-scherm oproepen

Klik in het besturingsscherm "Matrix" om het bijbehorende scherm te openen.



Opmerking

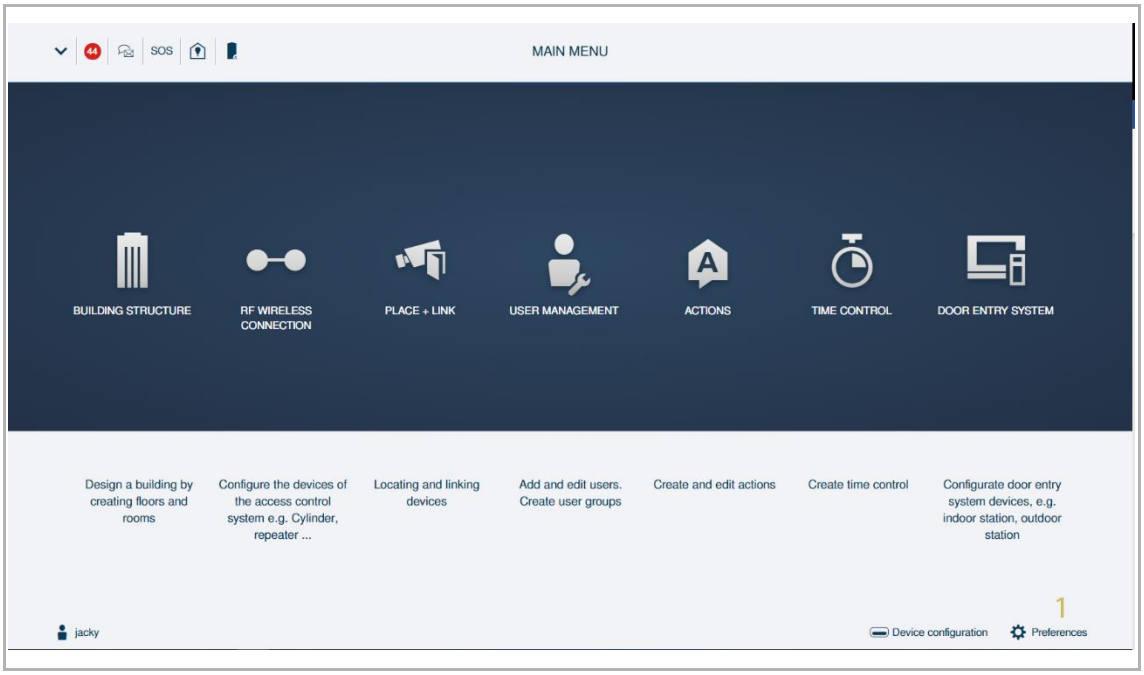
De bewerkingen op het matrixscherm zijn hetzelfde als op het etagescherm. zie hoofdstuk 10.7.1 “Apparaten besturen via de plattegrond“ op pagina 193.

10.8 Apparaten besturen via Welcome-app

10.8.1 "Smart Access Point" met Welcome-app koppelen

Volg de onderstaande stappen:

[1] Klik in het configuratiescherm op "Instellingen".



[2] Klik op "MyBuildings-account".

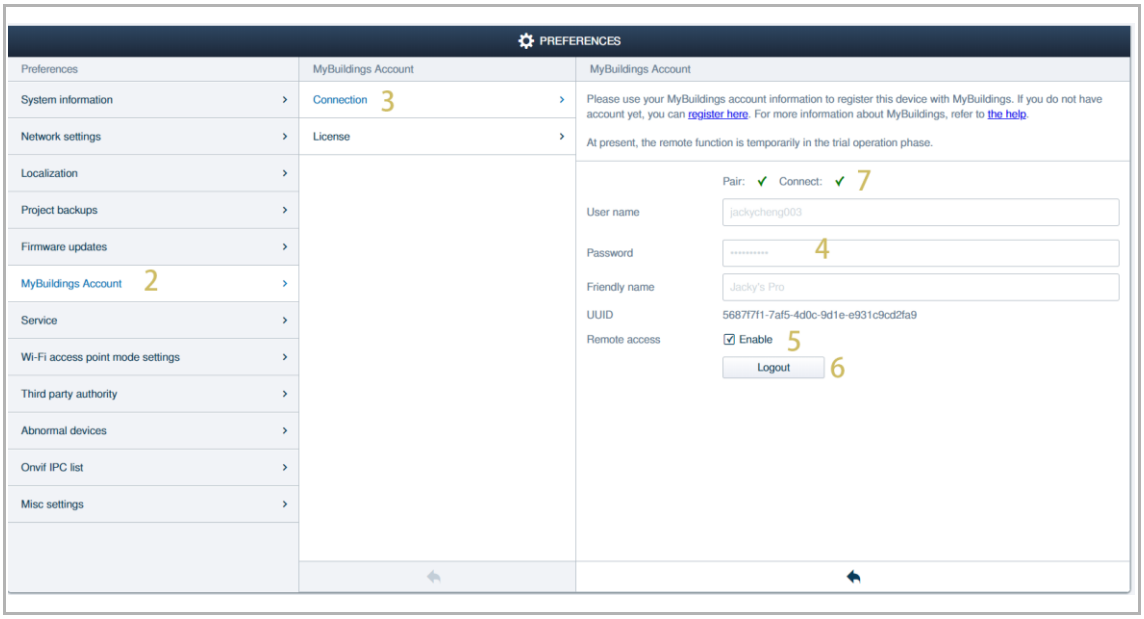
[3] Klik op "Connection".

[4] Voer het account, het wachtwoord en de bijnaam in.

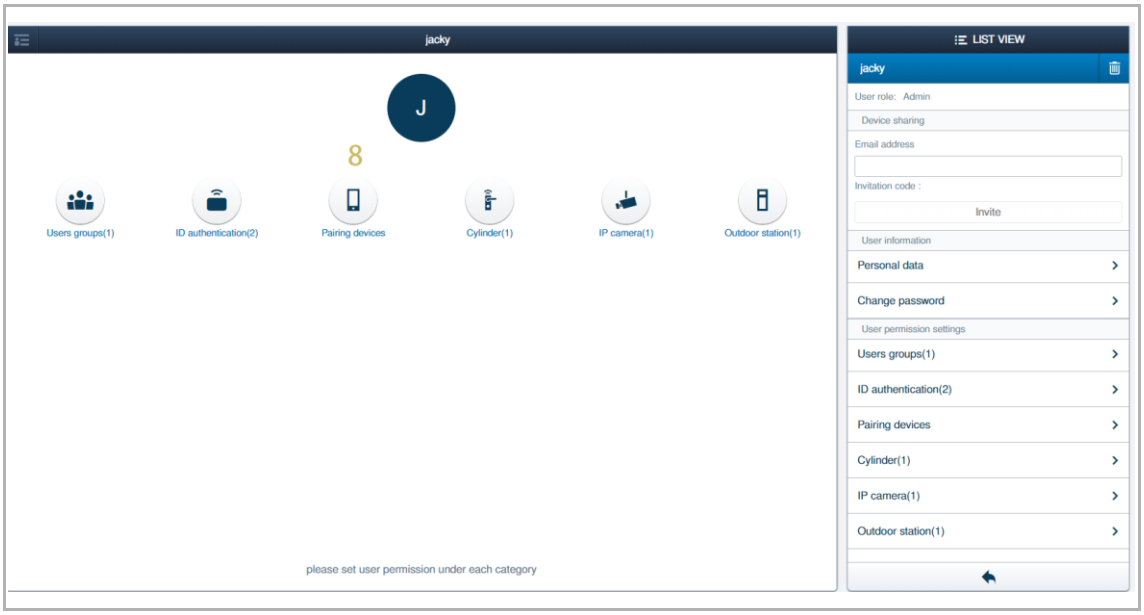
[5] Tik op "Activeren" om de functie"Toegang op afstand" te activeren (optioneel).

[6] Klik op "Login".

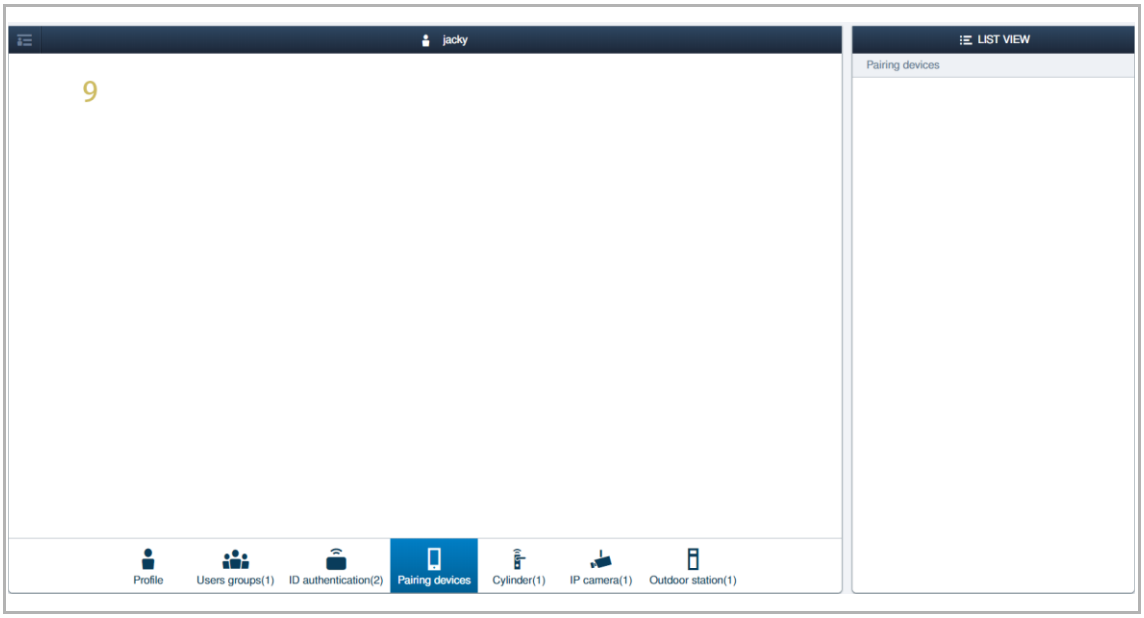
[7] Controleer de koppelingsstatus en de verbindingsstatus. Er wordt een groene "√" weergegeven als de verbinding gelukt is.



[8]Ret Ga terug naar het gebruikte scherm en klik op "Apparaten koppelen".



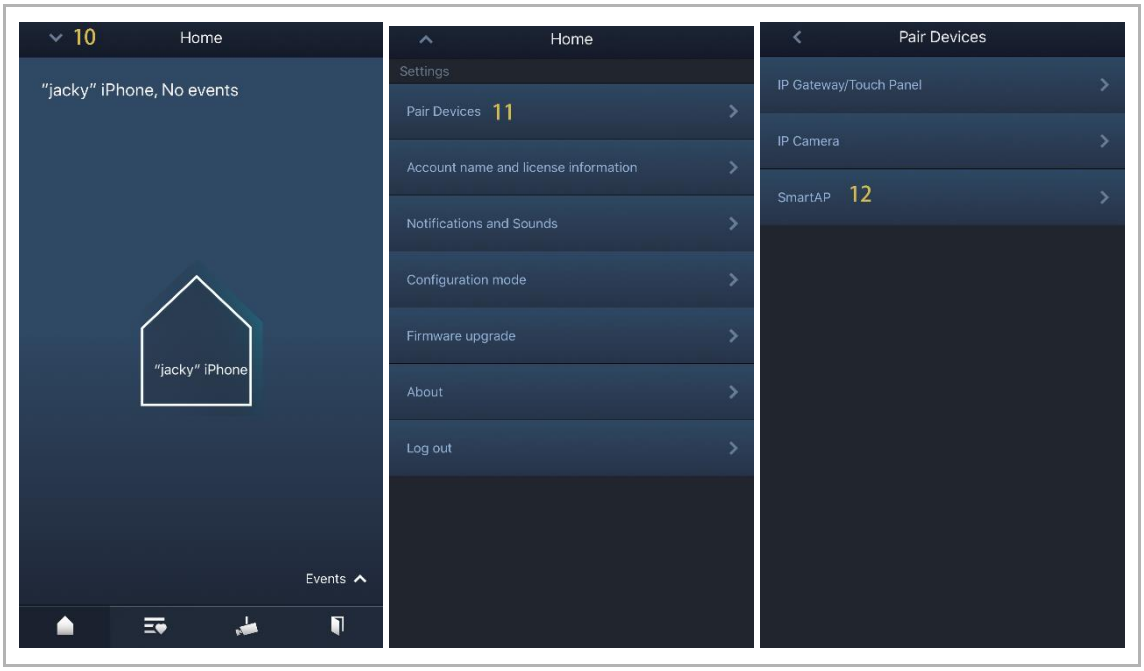
[9] Op dit moment wordt geen apparaat weergegeven. De volgende stap voert u uit in de Welcome-app.



[10]Op het startscherm van de Welcome-app tikt u op "v" (in de Welcome-app gebruikt u dezelfde inloggegevens als voor het MyBuildings-account met het "Smart Access Point").

[11]Tik op "Apparaten koppelen".

[12]Tik op "SmartAP".

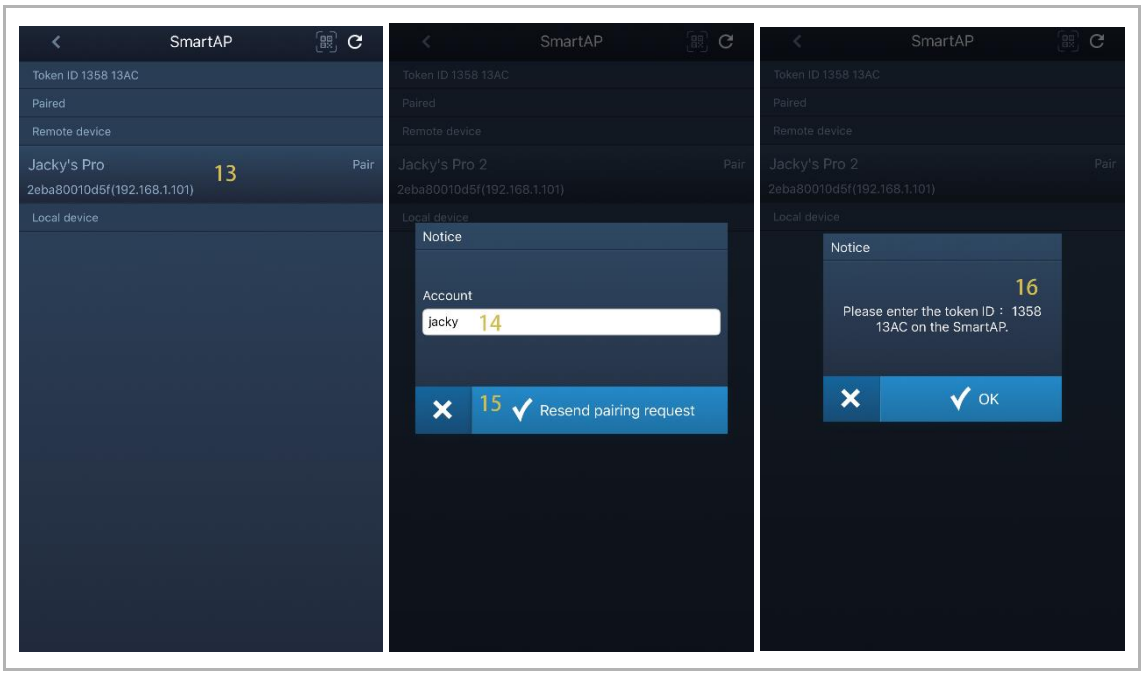


[13]Tik op het betreffende "Smart Access Point" in de sectie "Apparaat op afstand".

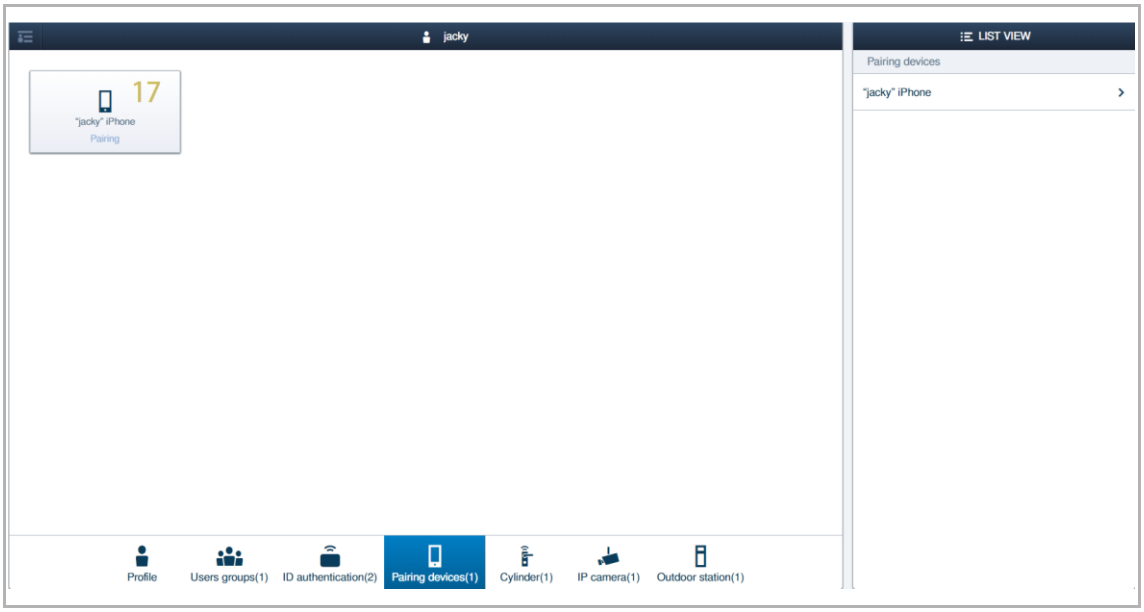
[14]Voer de gebruikersnaam in die u gebruikt op het "Smart Access Point".

[15]Tik op "√" om te bevestigen.

[16]Een token-ID wordt weergegeven in een pop-upvenster. Deze token-ID wordt gebruikt bij stap 18 op "Smart Access Point".



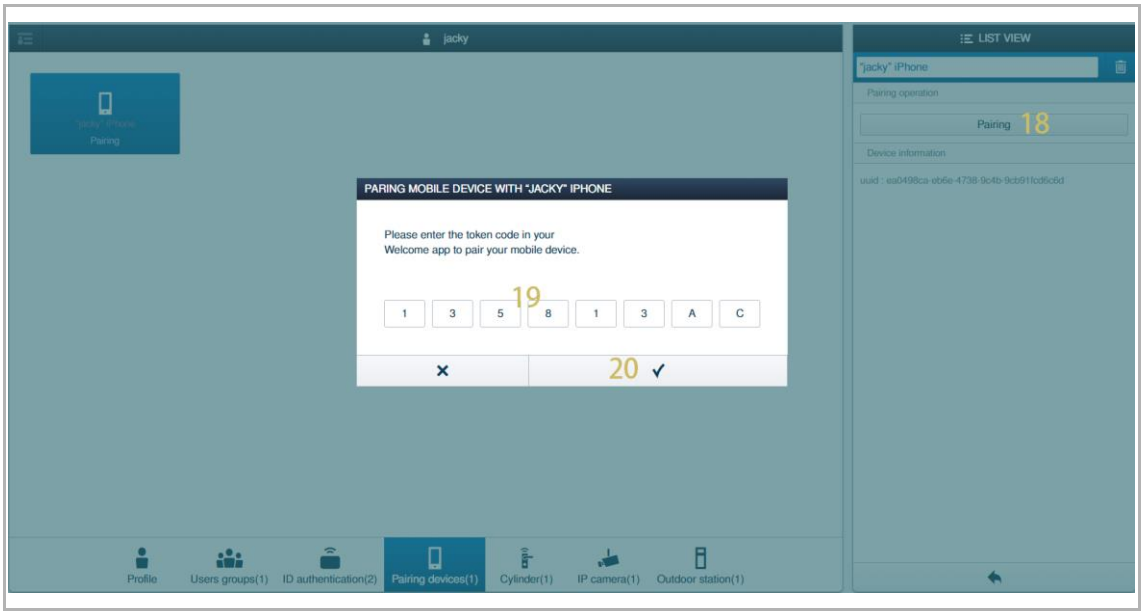
[17]Go Ga naar het "Smart Access Point ", op het scherm "Apparaten koppelen" (zie stap 9) verschijnt een vriendelijke naam op het scherm van het apparaat dat wordt gebruikt door Welcome-app. Klik op dit apparaat.



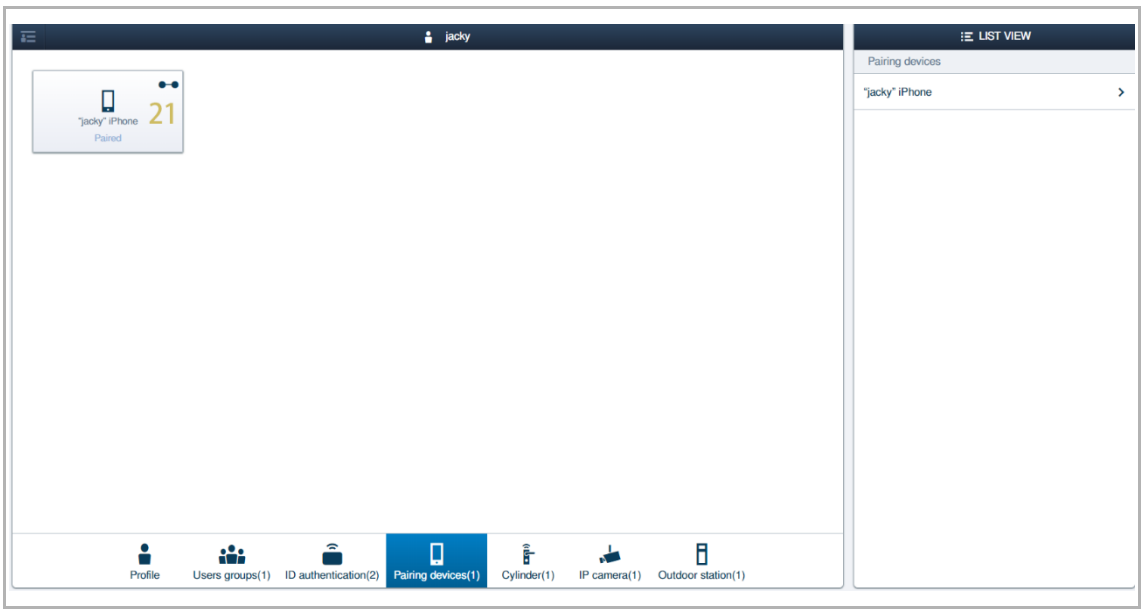
[18]Klik op "Verknoping".

[19]Voer de token-ID in (zie stap 16).

[20]Klik op "√" om te bevestigen.



[21]Indien succesvol wordt de status "Gepaard" op het scherm weergegeven.



10.8.2 Elektronische slotcilinder besturen via Welcome-app

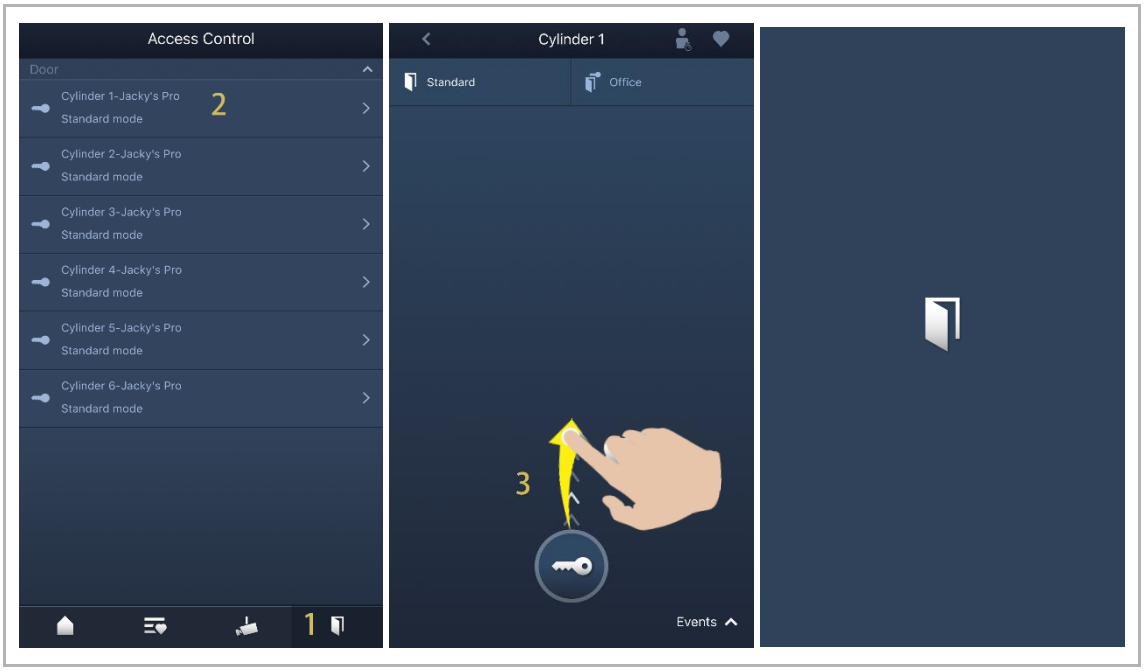
Elektronische slotcilinder deblokkeren

Volg de onderstaande stappen:

[1] Op het startscherm van de Welcome-app tikt u op "".

[2] Tik op het AccessControl-scherm op de aanduiding "Elektronische slotcilinder" om toegang te krijgen tot het betreffende scherm.

[3] Door het slotsymbool omhoog te vegen deblokkeert u de "elektronische slotcilinder".



Kantoormodus activeren/deactiveren

Volg de onderstaande stappen:

[1] Op het startscherm van de Welcome-app tikt u op "".

[2] Tik op het AccessControl-scherm op de aanduiding "Elektronische slotcilinder" om toegang te krijgen tot het betreffende scherm.

[3] Klik op "Kantoor".

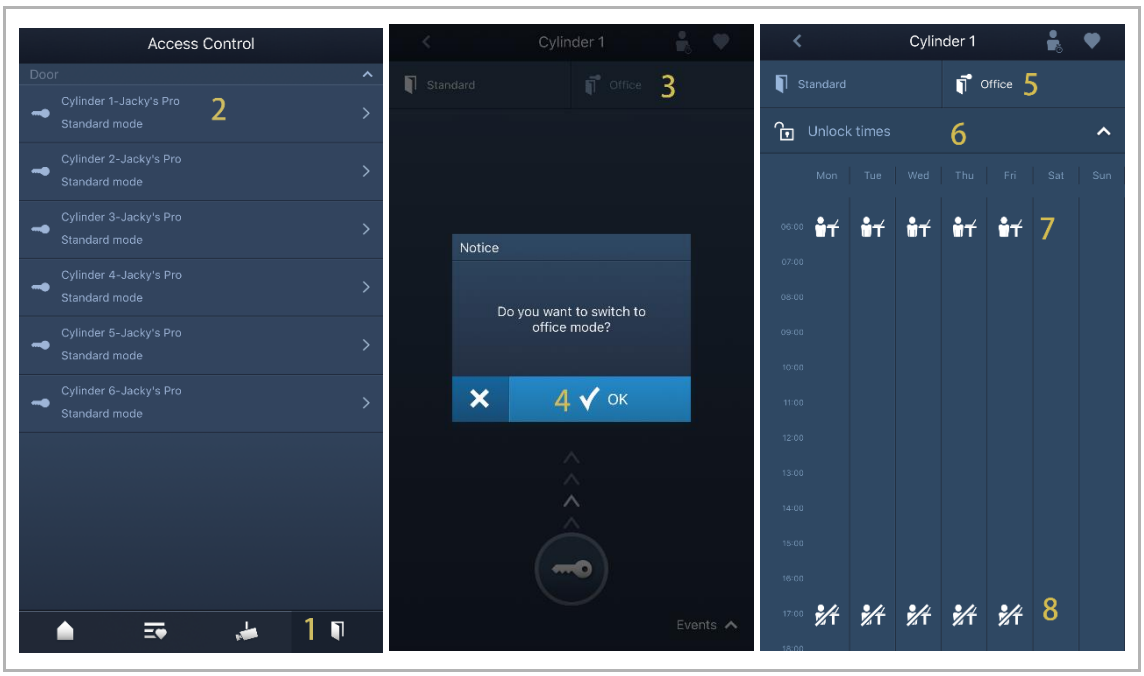
[4] Klik op "√" om te bevestigen.

[5] Klik op "Kantoor".

[6] Klik op "Deblokkeringstijden".

[7] Op dit moment is de kantoormodus geactiveerd.

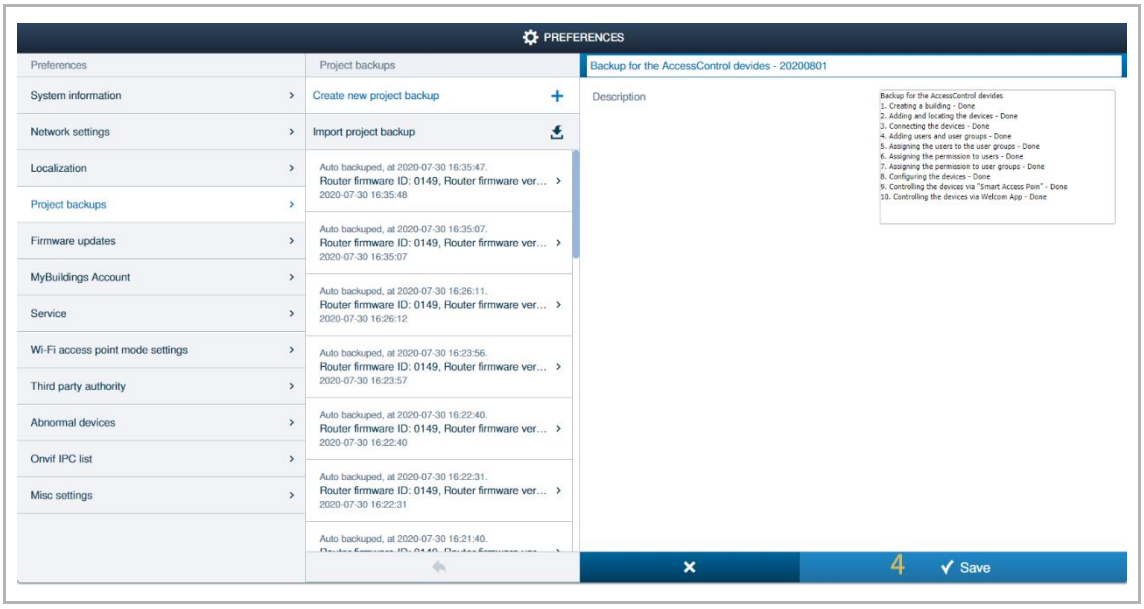
[8] Op dit moment is de kantoormodus gedeactiveerd.



10.9 Back-up beheren

Het is belangrijk om regelmatig een back-up te maken.

Zie voor meer informatie: zie hoofdstuk 13.5 “Back-up beheren“ op pagina 280.



10.10 Rechten verwijderen

10.10.1 Rechten van een gebruiker verwijderen

1. De "elektronische slotcilinder" van een gebruiker verwijderen

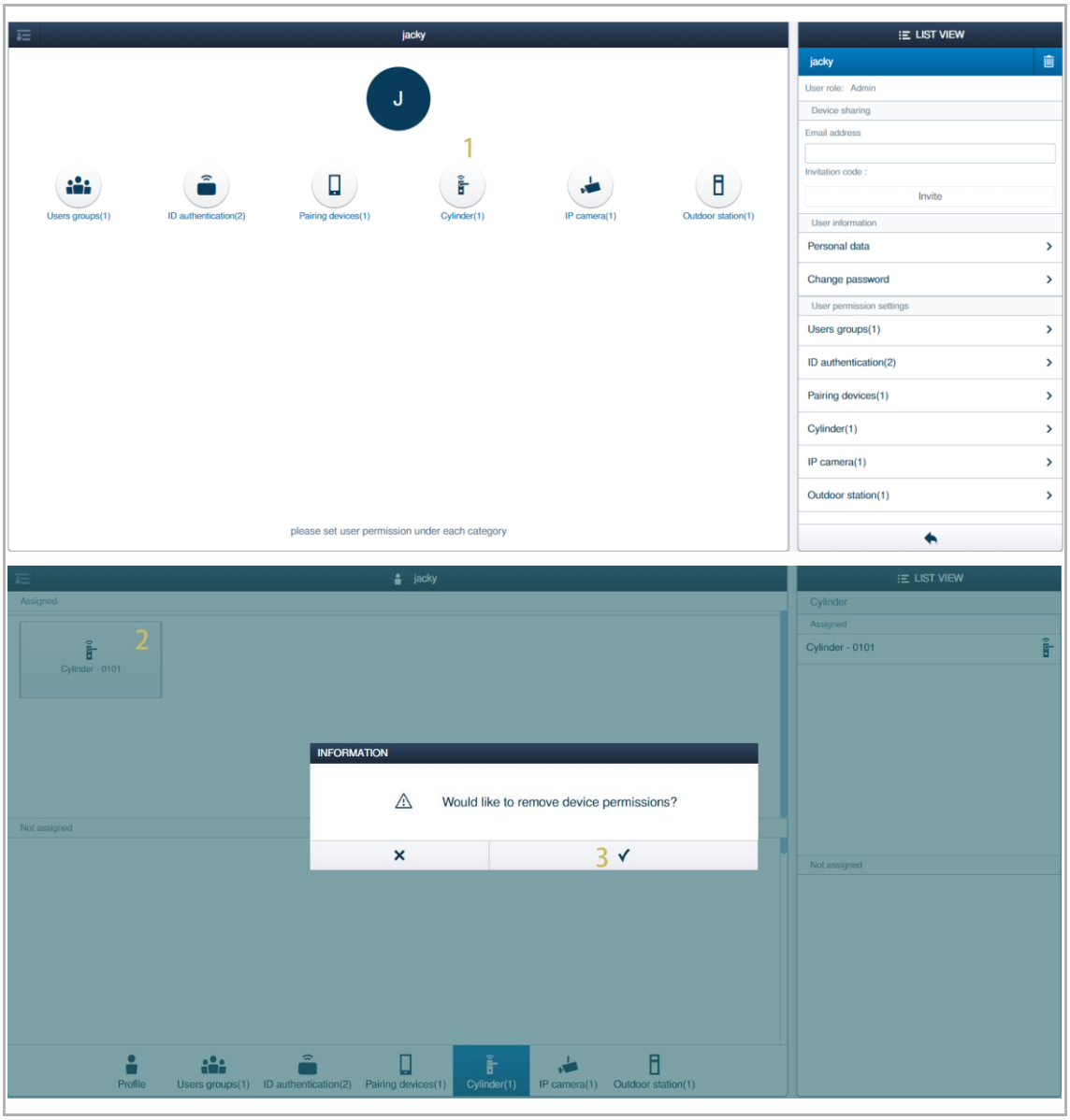
Als u de betreffende "elektronische slotcilinder" onbruikbaar wilt maken voor een gebruiker, volg dan de onderstaande stappen:

[1] Op het betreffende gebruikersscherm klikt u op "Cilinder".

[2] Klik op de "Elektronische slotcilinder" in de sectie "Toegewezen".

[3] Klik op "√" om te bevestigen.

Herhaal de stappen van 2-3 om de elektronische slotcilinders één voor één te verwijderen.



2. De ID-authenticaties van een gebruiker verwijderen

Als u de betreffende ID-authenticaties van een gebruiker onbruikbaar wilt maken, volg dan de onderstaande stappen:

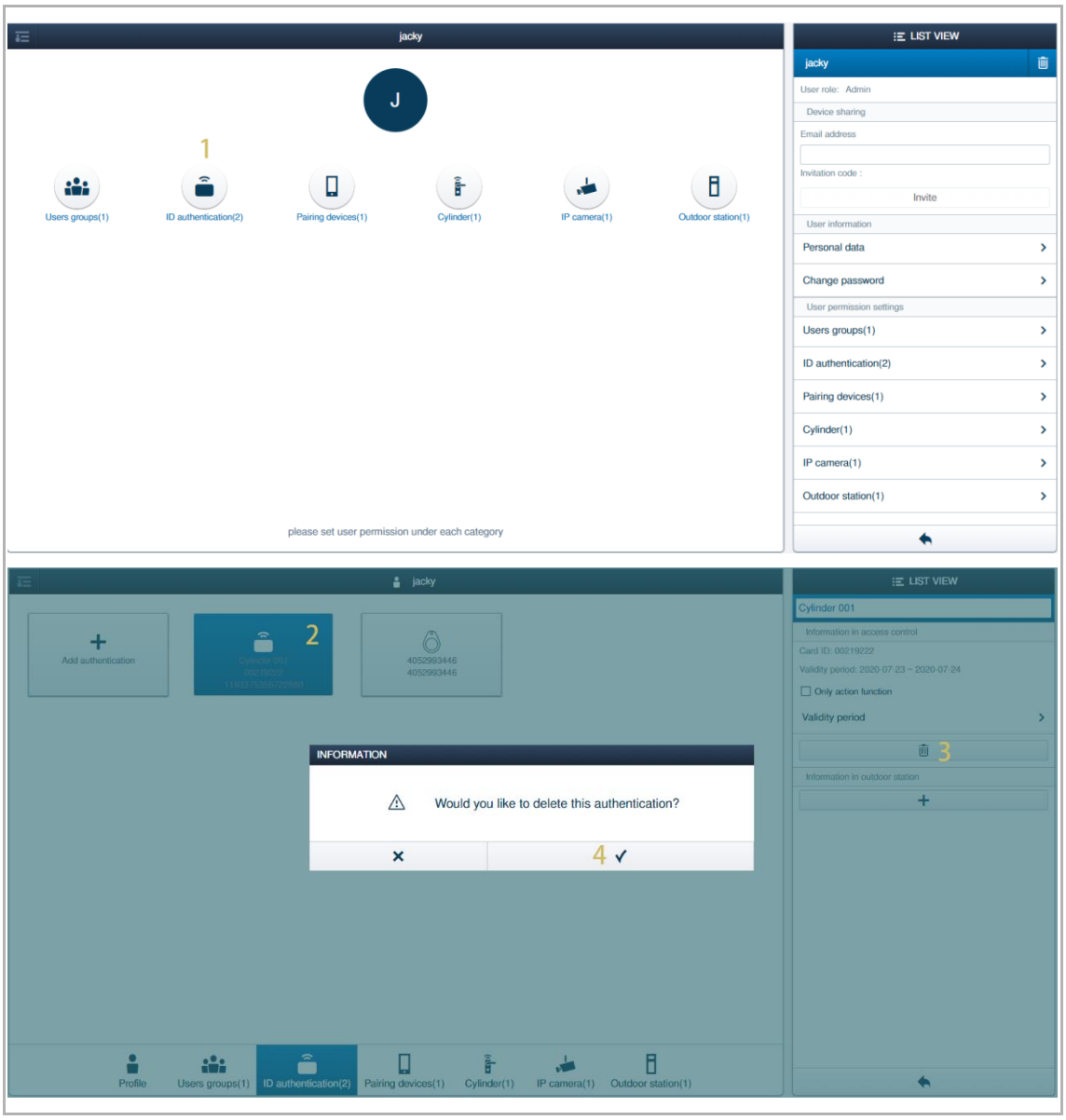
[1] Op het betreffende gebruikersscherm klikt u op "ID-authenticatie" om het bijbehorende scherm te openen.

[2] Klik op betreffende "ID-authenticatie".

[3] Klik op " "; als de kaart tot een "noodkaart" behoort dient u eerst de noodkaart te verwijderen. zie hoofdstuk 10.5.4 “Noodkaarten beheren“ op pagina 176.

[4] Klik op "√" om te bevestigen.

Herhaal de stappen van 2-4 om de ID-authenticaties één voor één te verwijderen.



10.10.2 Rechten van de gebruikers in een groep verwijderen

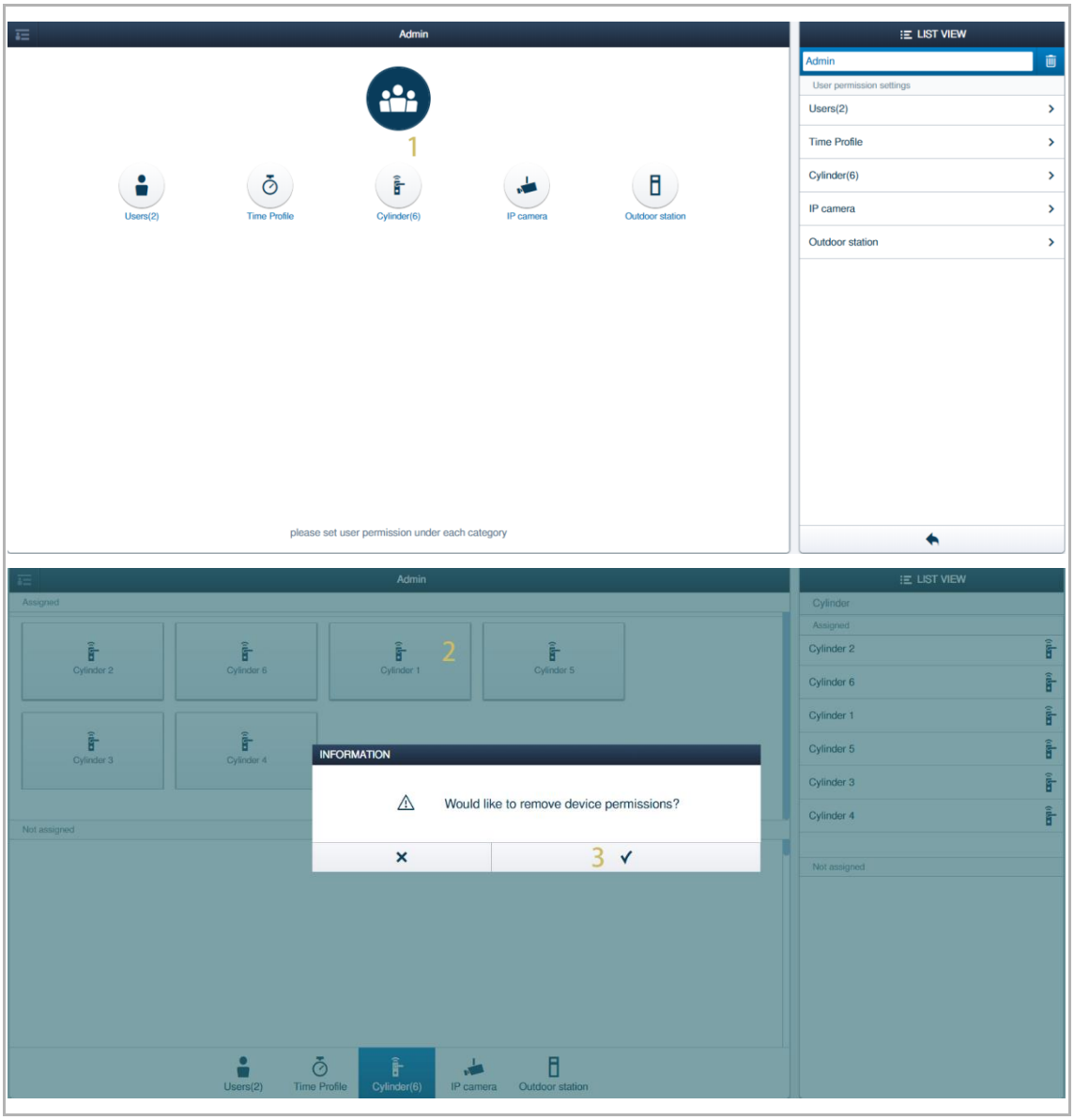
1. De "elektronische slotcilinder" van een groep verwijderen

Als u de betreffende "elektronische slotcilinder" onbruikbaar wilt maken voor alle gebruikers in de groep, volg dan de onderstaande stappen:

[1] Op het betreffende groepsscherm klikt u op "Cilinder".

[2] Klik op de "Elektronische slotcilinder" in de sectie "Toegewezen".

[3] Klik op "√" om te bevestigen.



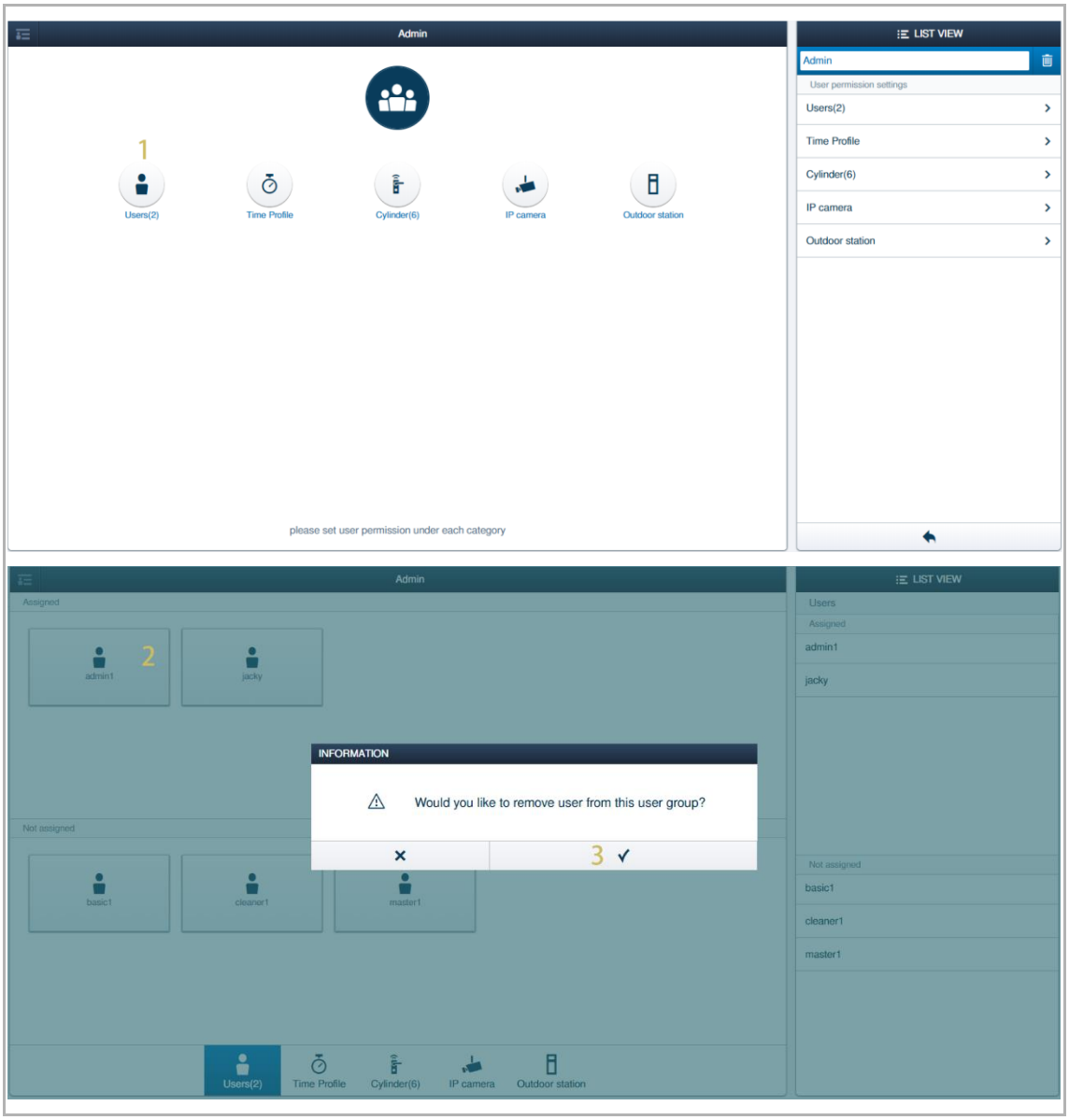
2. Gebruikers uit een gebruikersgroep verwijderen

Als u de betreffende "elektronische slotcilinder" onbruikbaar wilt maken voor enkele gebruikers in de groep, volg dan de onderstaande stappen:

[1] Op het betreffende groepsscherm klikt u op "Gebruiker".

[2] Klik op de gebruiker in de sectie "Toegewezen".

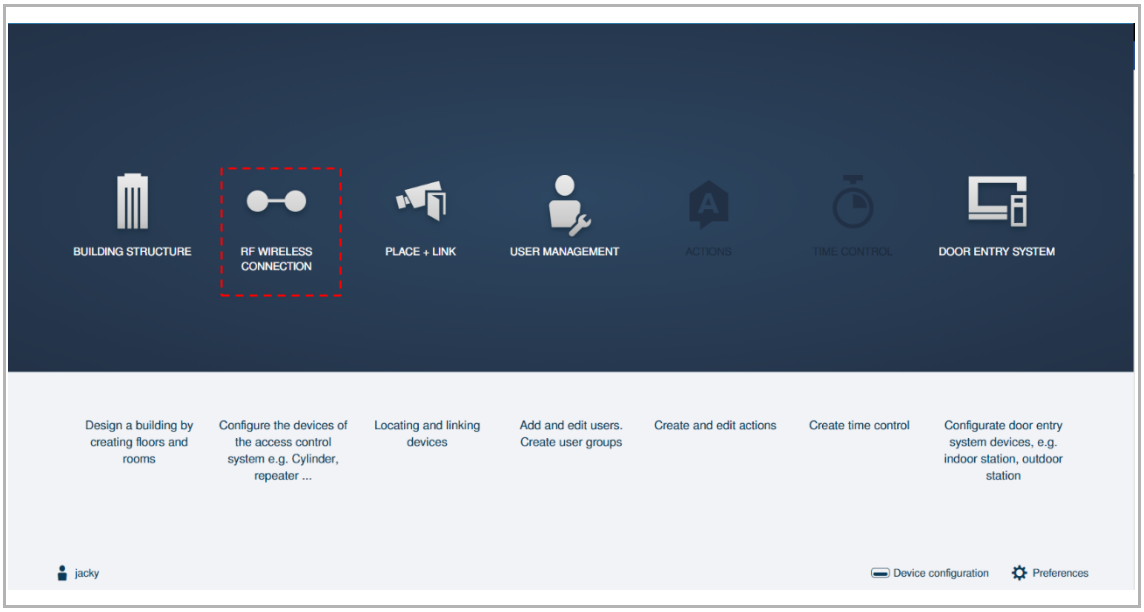
[3] Klik op "√" om te bevestigen.



10.11 Apparaten loskoppelen

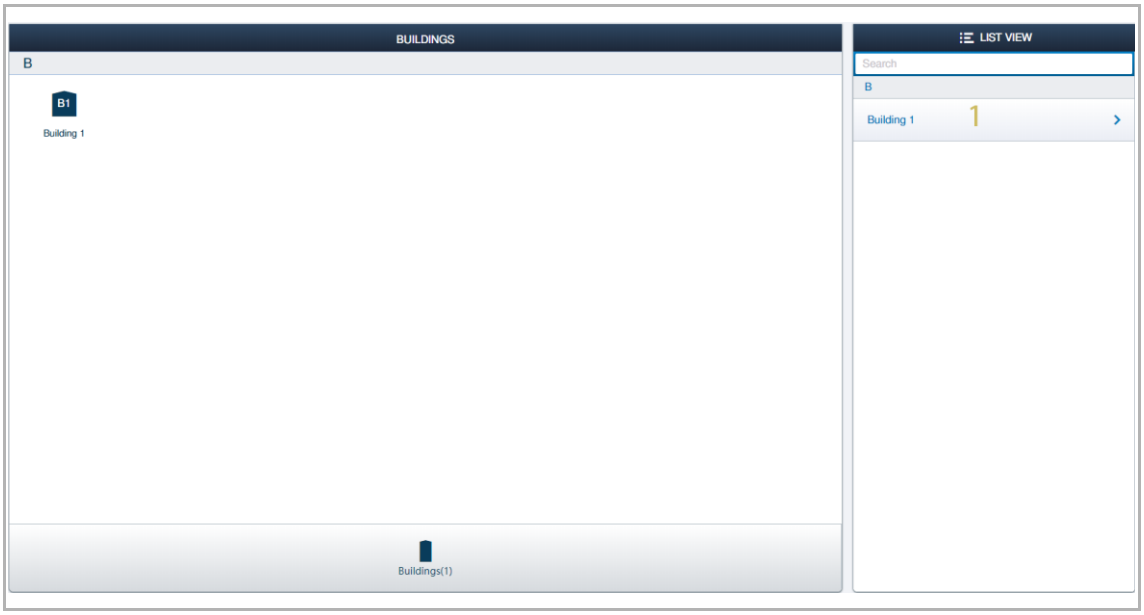
Scherm RF-verbindingen oproepen

Klik in het configuratiescherm op "Toegangscontrole" om het bijbehorende scherm te openen.

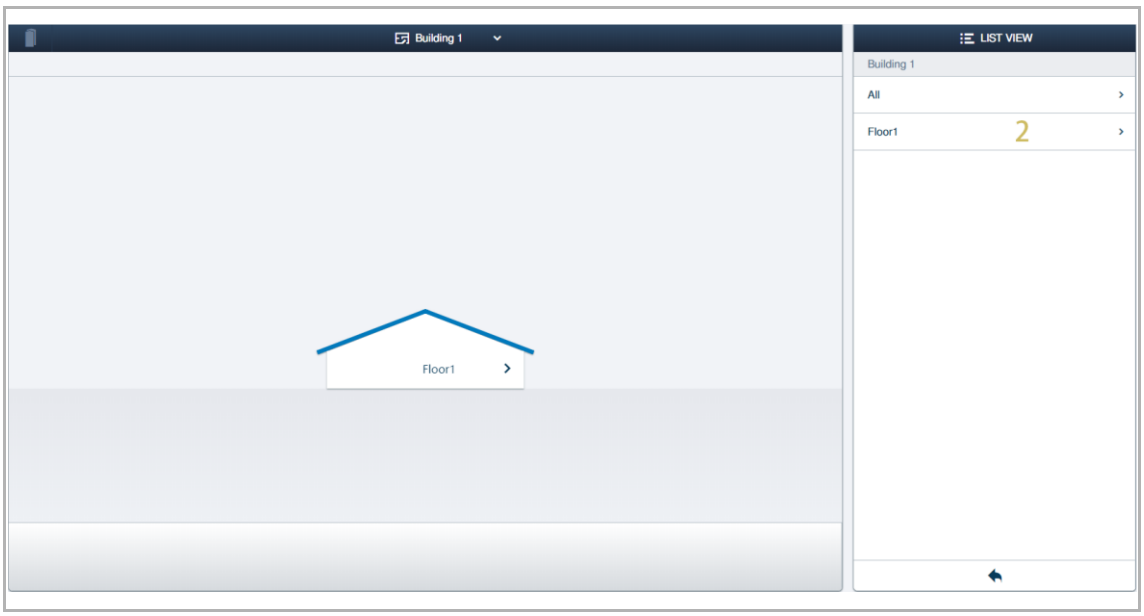


Volg de onderstaande stappen:

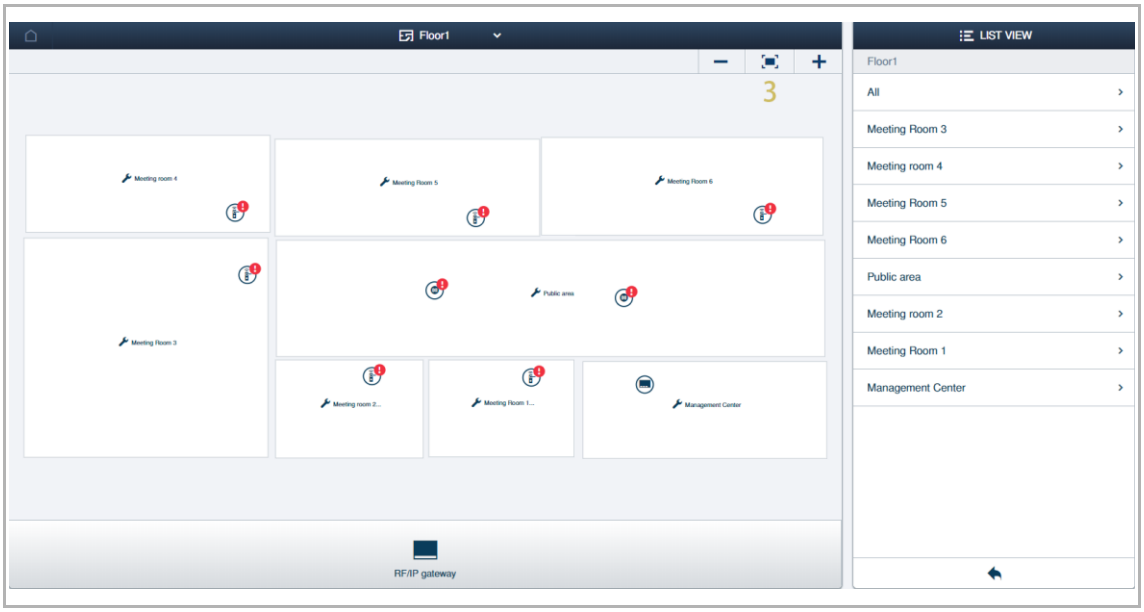
[1] Op het scherm "Gebouw" klikt u op het benodigde gebouw (bijv. "Gebouw 1" voor demonstratie 1).



[2] Klik op de benodigde etage (bijv. "Etage 1" voor demonstratie 1).



[3] Klik op " " om alle apparaten op het etagescherm te bekijken, u kunt de symbolen naar een geschikte positie slepen.



AccessControl-apparaten in een sequentie loskoppelen

Koppel de AccessControl-apparaten in een radiolijn los volgens de onderstaande volgorde:

[1] Koppel de "elektronische slotcilinder" los van de hogere apparaten.

[2] Koppel de "RF-repeater" los van de hogere apparaten.

10.11.1 "Elektronische slotcilinder" loskoppelen

Let op!

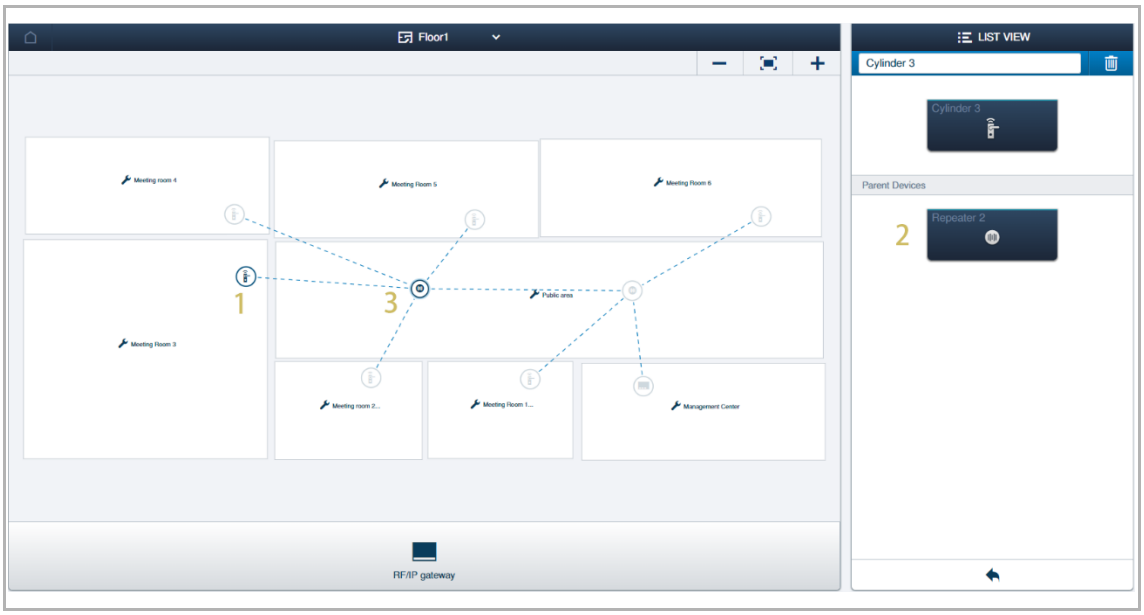
Het wordt ten zeerste aanbevolen om de "Elektronische Sluitcilinder" in online modus altijd te ontkoppelen. Als de "elektronische sluitcilinder" in de onlinetoestand wordt ontkoppeld, kan hij in andere systemen weer worden gebruikt. Indien zij in de offline-toestand geforceerd is ontkoppeld, kan zij alleen in het huidige systeem opnieuw worden ontkoppeld. zie hoofdstuk 10.4.3 “AccessControl-apparaat is offline“ op pagina 167

Volg de onderstaande stappen:

[1] Klik op het etagescherm op een "elektronische slotcilinder" (bijv. "Cilinder 3" voor demonstratie 1).

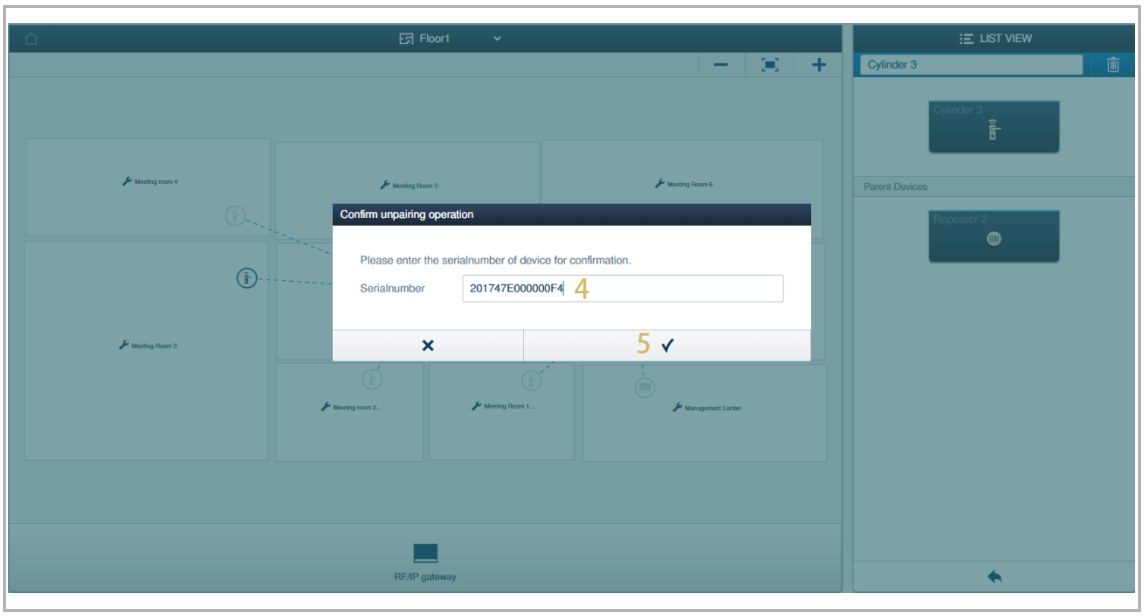
[2] Het hogere apparaat wordt weergegeven in de lijst.

[3] Klik op het hogere apparaat op de etageplattegrond (bijv. "Repeater 2" voor demonstratie 1).

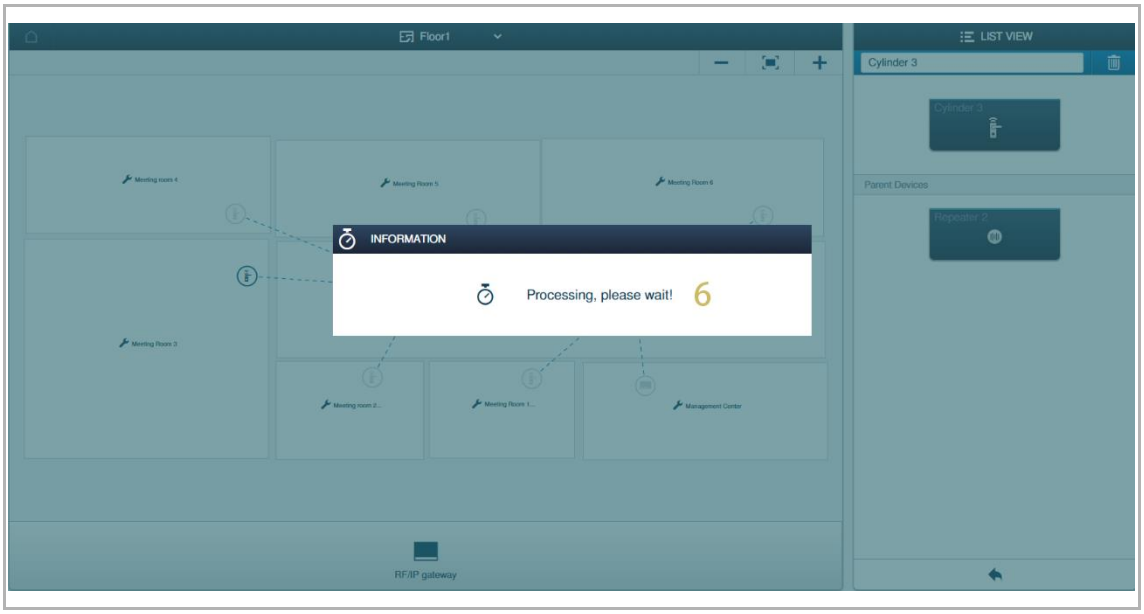


[4] Voer het serienummer van de elektronische slotcilinder in.

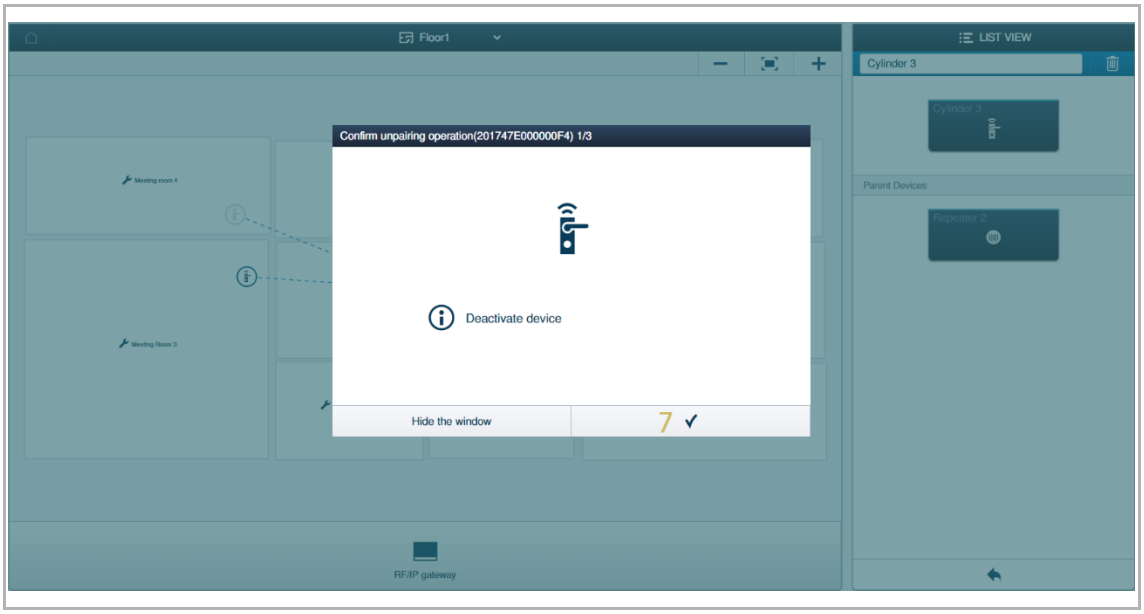
[5] Klik op "√" om te bevestigen.



[6] Wacht op de koppeling.

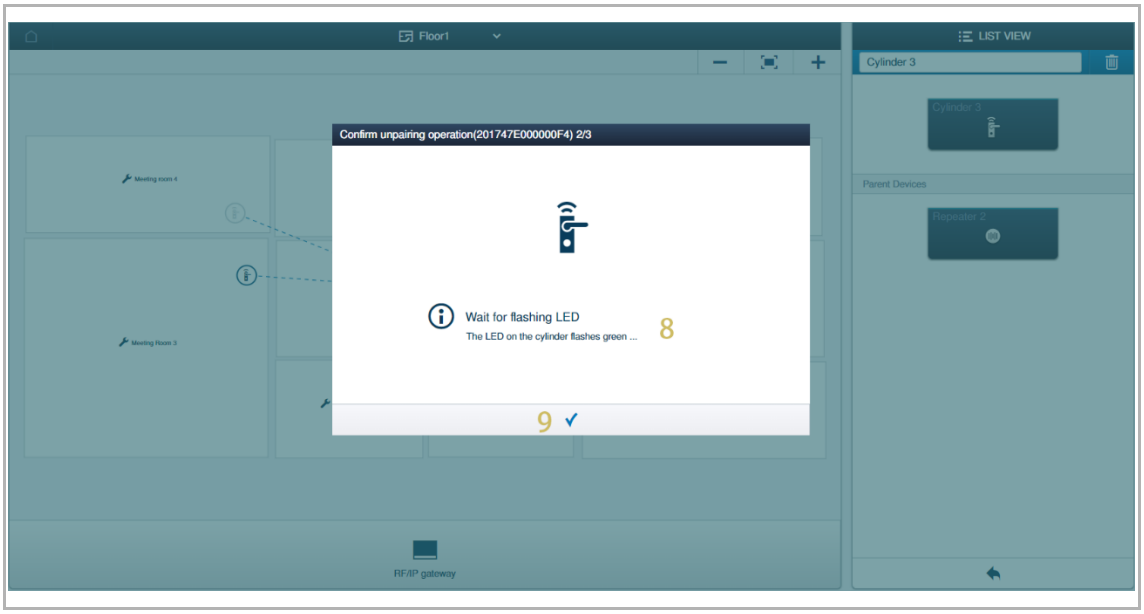


[7] Klik op "√" om door te gaan.



[8] Wacht totdat de LED op de "elektronische slotcilinder" groen knippert of totdat er een pieptoon klinkt.

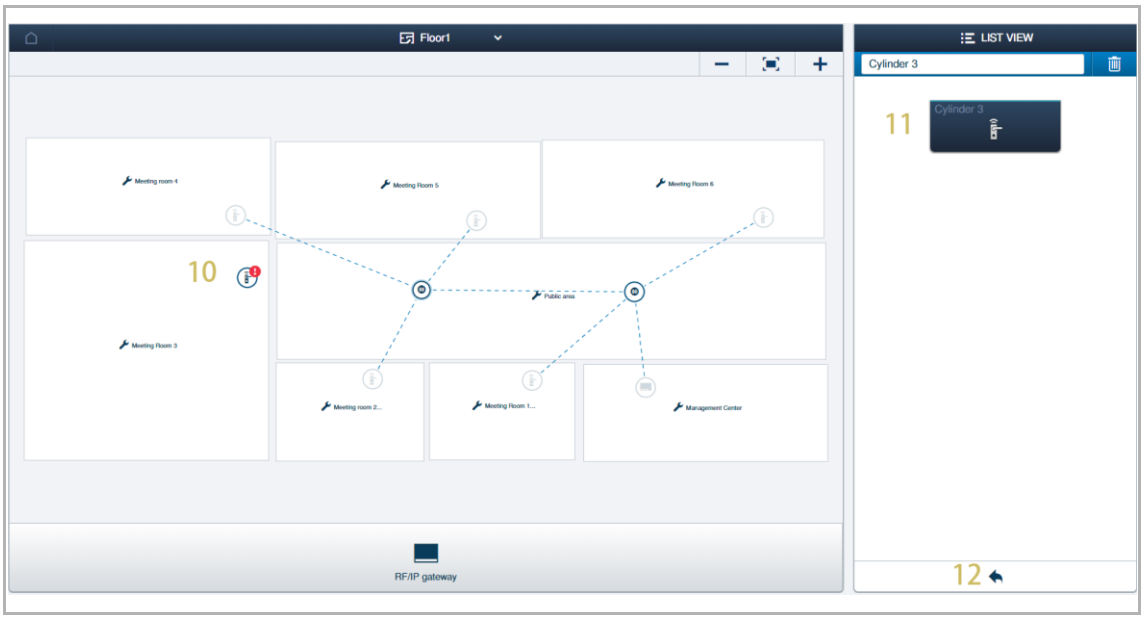
[9] Klik op "√" om door te gaan.



[10]Er wordt geen stippellijn weergegeven tussen de twee apparaten.

[11]In de lijst wordt geen hoger apparaat weergegeven.

[12]Klik op " " om terug te gaan naar het etagescherm.



10.11.2 "RF-repeater" loskoppelen

Let op!

Voordat een "RF Repeater" in een ander systeem kan worden gebruikt, moet hij worden gereset naar de fabrieksinstellingen (houd de reset-knop 3 seconden ingedrukt). zie hoofdstuk 10.4.3 “AccessControl-apparaat is offline“ op pagina 167

Let op!

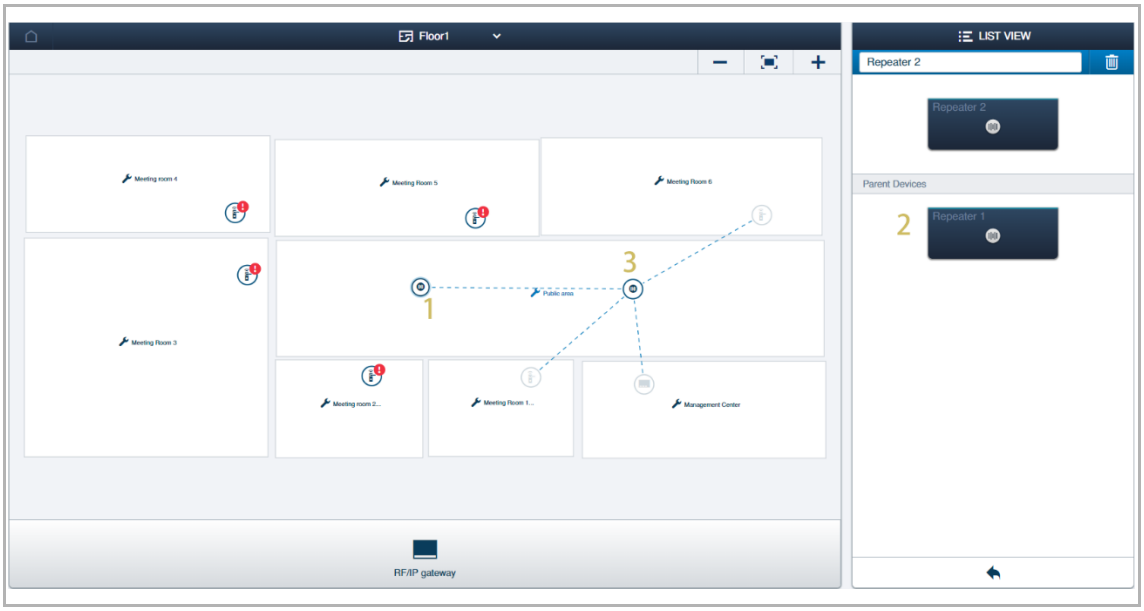
De RF-repeater die ontkoppeld moet worden kan geen slave-apparaten hebben!

Volg de onderstaande stappen:

[1] Klik op het etagescherm op een "RF-repeater" (bijv. "Repeater 2" voor demonstratie 1).

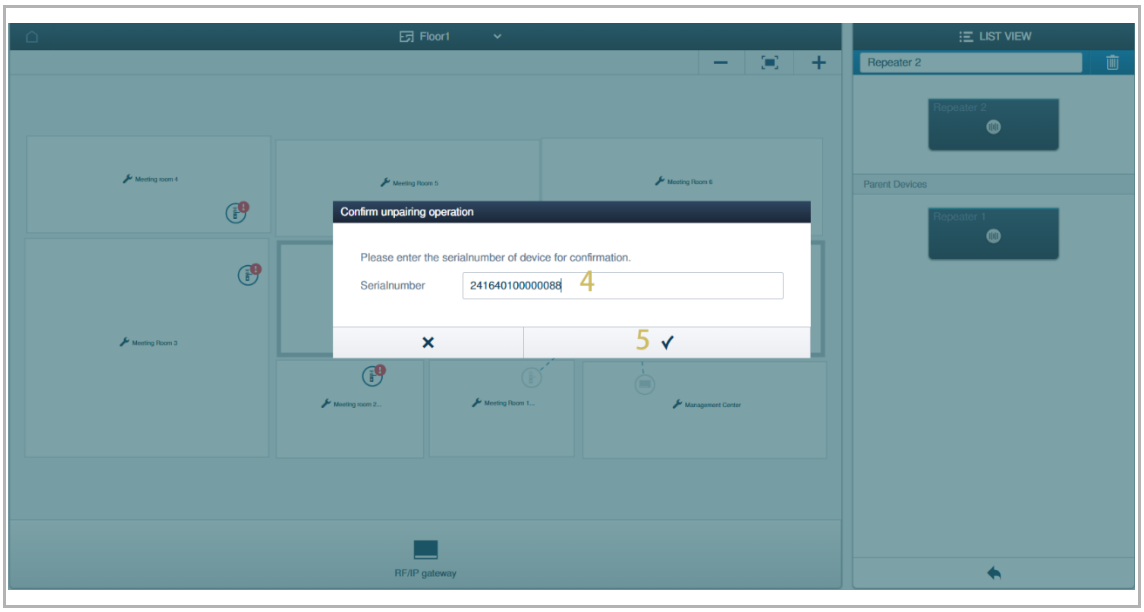
[2] Het hogere apparaat wordt weergegeven in de lijst.

[3] Klik op het hogere apparaat op de etageplattegrond (bijv. "Repeater 1" voor demonstratie 1).

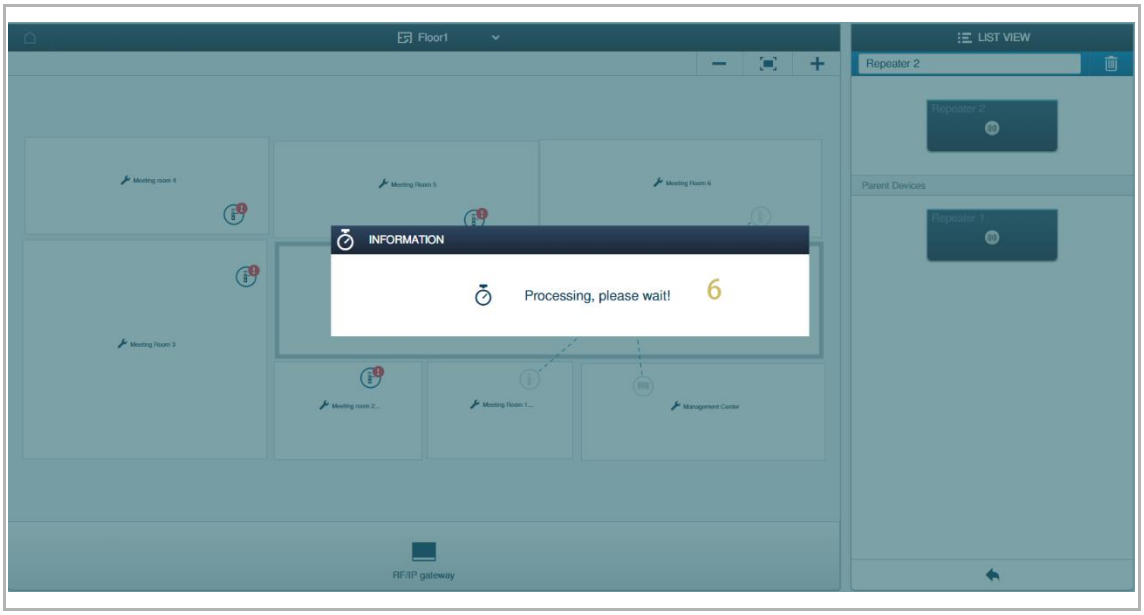


[4] Voer het serienummer van de "RF-repeater" in (bijv. "Repeater 2" voor demonstratie 1).

[5] Klik op "√" om te bevestigen.



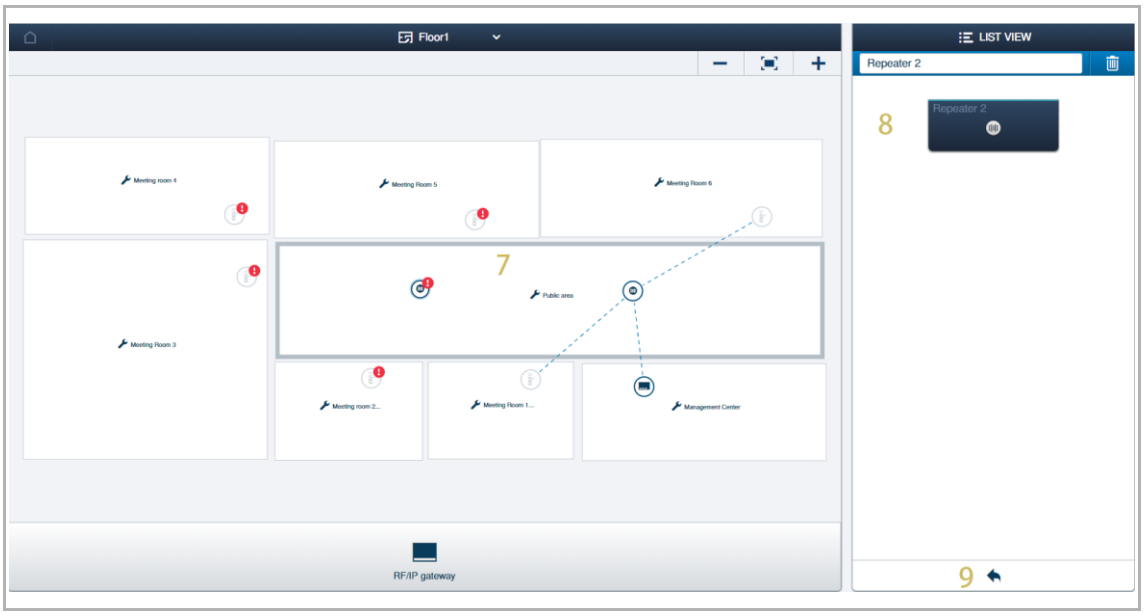
[6] Wacht op de koppeling.



[7] Er wordt geen stippellijn weergegeven tussen de twee apparaten.

[8] In de lijst wordt geen hoger apparaat weergegeven.

[9] Klik op " " om terug te gaan naar het etagescherm.



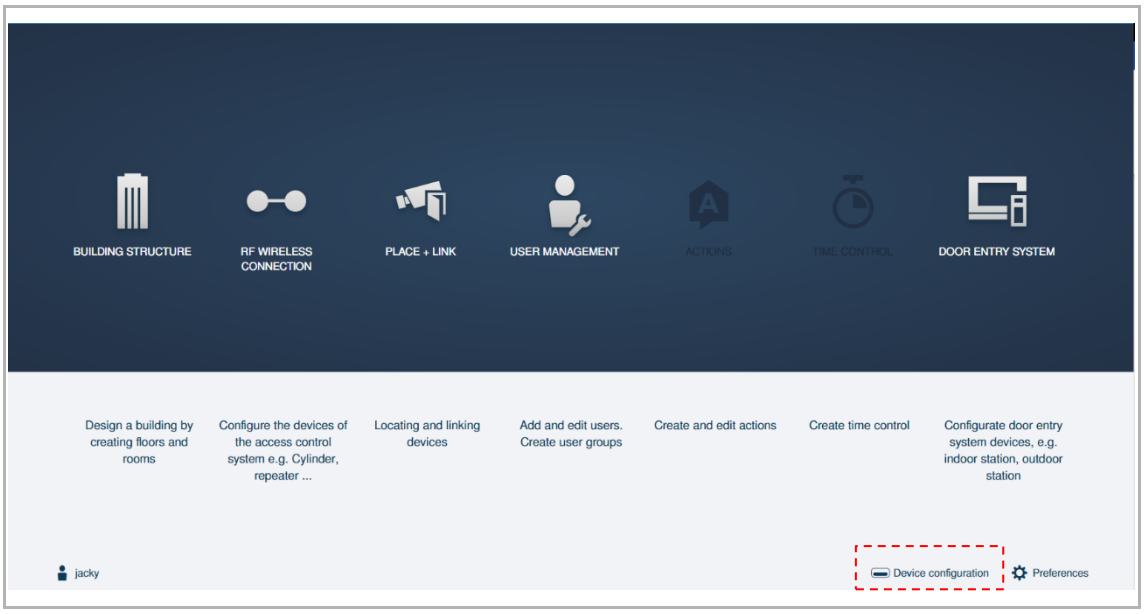
10.12 Apparaten verwijderen

Opmerking

Het AccessControl-apparaat kan niet worden verwijderd als het is gekoppeld. Ontkoppel het apparaat eerst. zie hoofdstuk 10.11 “Apparaten loskoppelen“ op pagina 215.

Scherm "Apparaatconfiguratie" oproepen

Klik in het configuratiescherm op "Apparaatconfiguratie" om het bijbehorende scherm te openen.



10.12.1 "Elektronische slotcilinder" verwijderen

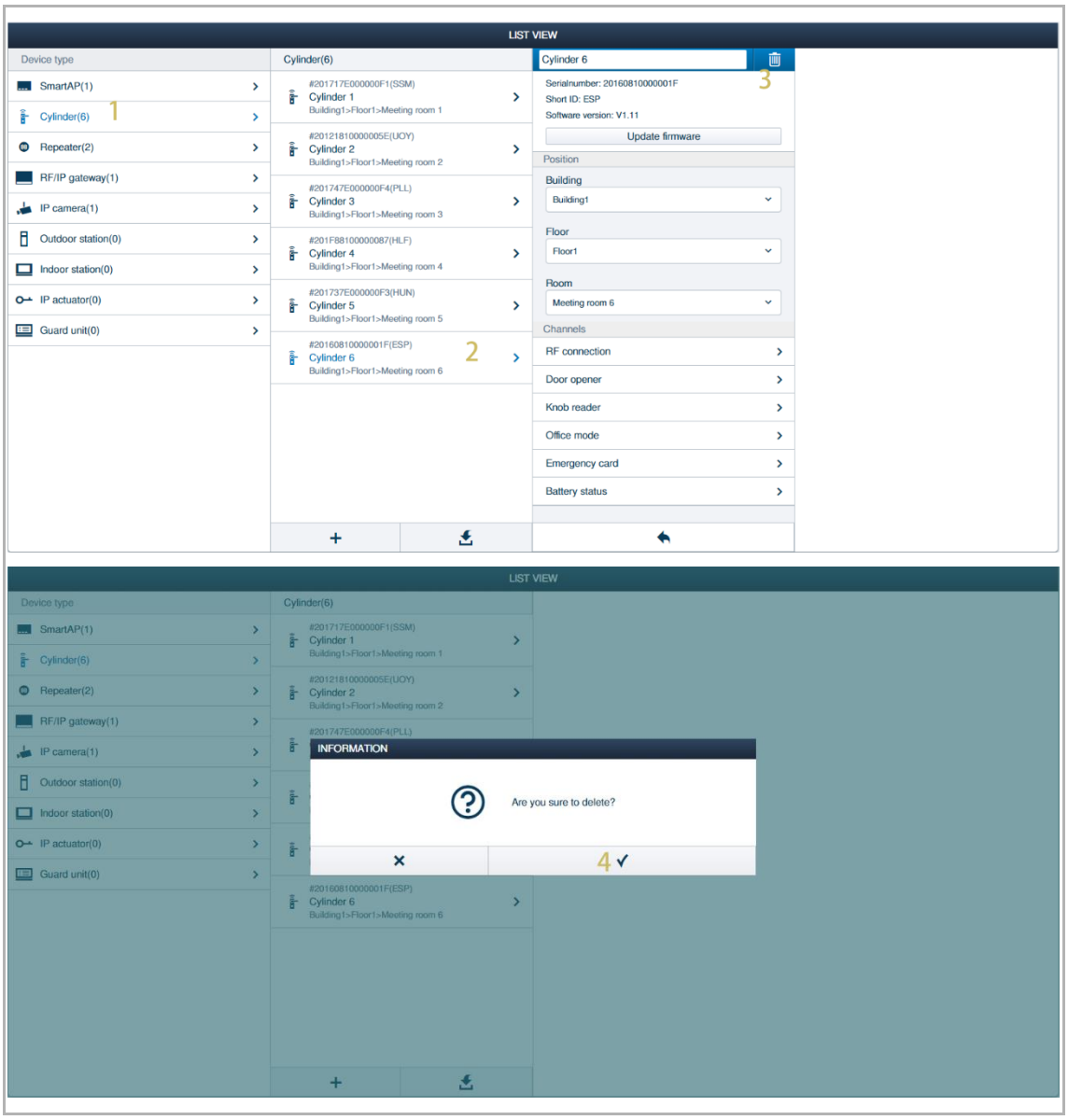
Volg de onderstaande stappen:

[1] Klik in het scherm "Apparaatconfiguratie" op "Cilinder".

[2] Klik op de "Elektronische slotcilinder" (bijv. "Cilinder 6").

[3] Klik op "".

[4] Klik op "√" om te bevestigen.



10.12.2 RF-repeater verwijderen

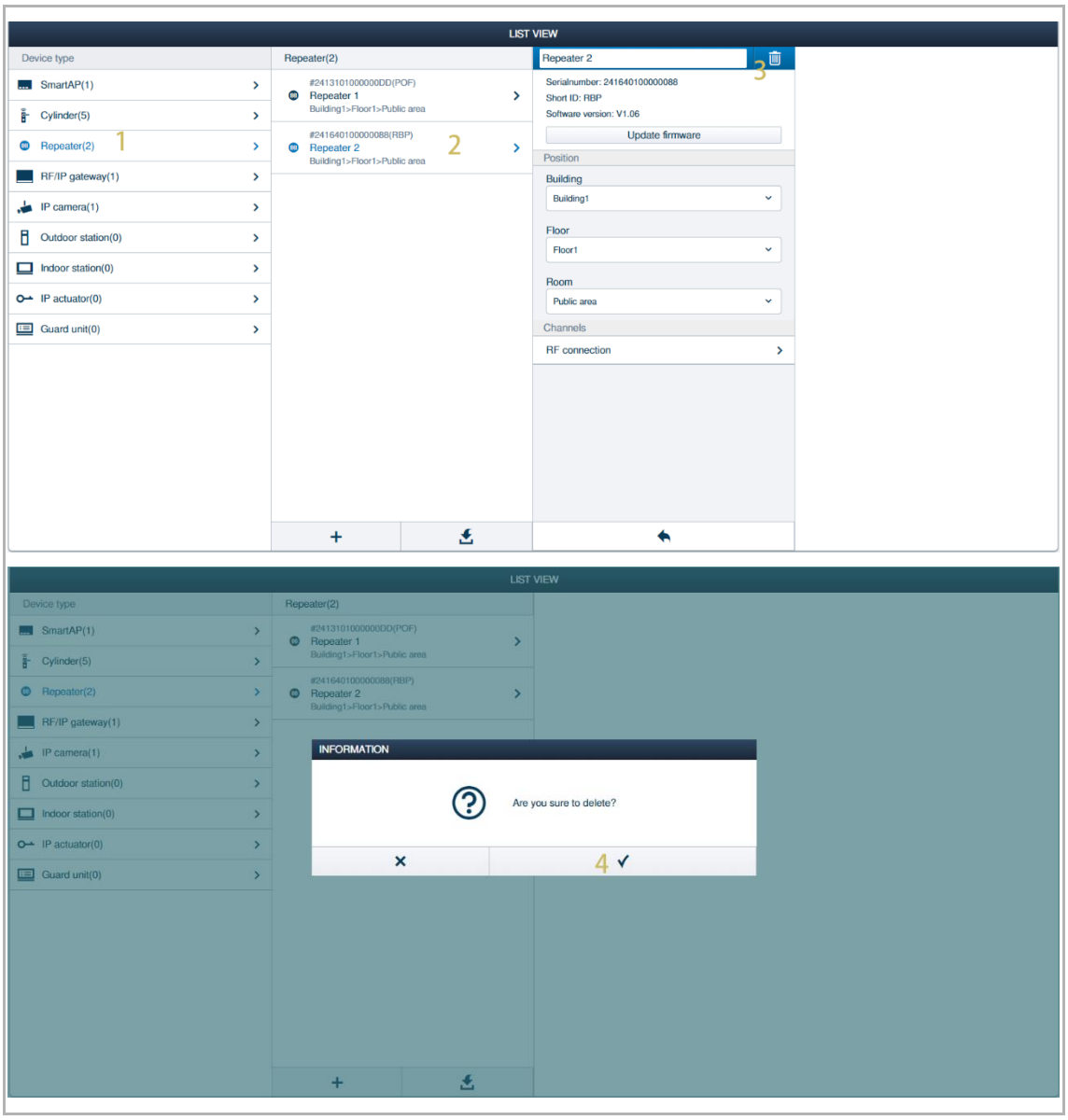
Volg de onderstaande stappen:

[1] Klik in het scherm "Apparaatconfiguratie" op "Repeater".

[2] Klik op de betreffende RF-repeater (bijv. "Repeater 2").

[3] Klik op "".

[4] Klik op "√" om te bevestigen.



10.12.3 RF/IP-gateway verwijderen

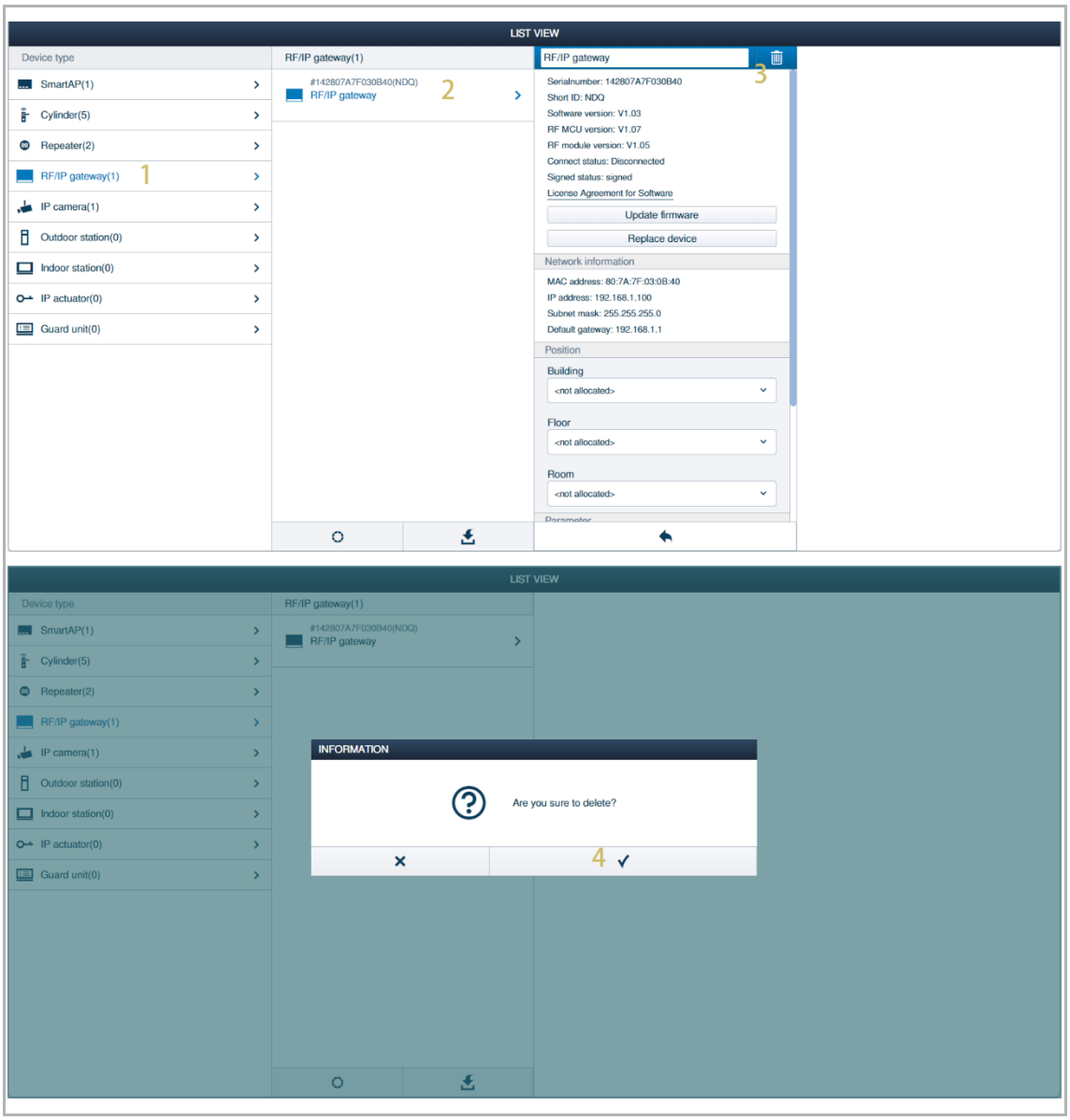
Volg de onderstaande stappen:

[1] Klik in het scherm "Apparaatconfiguratie" op "BLE".

[2] Klik op de betreffende RF/IP-gateway.

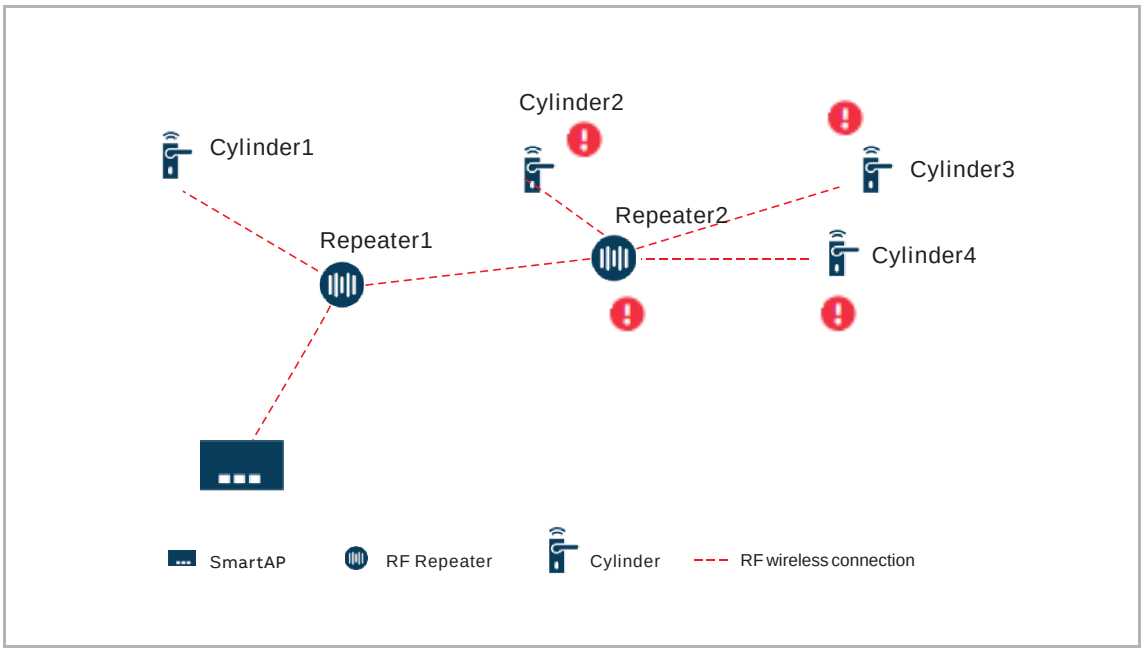
[3] Klik op "".

[4] Klik op "√" om te bevestigen.



10.13 Een defecte "RF Repeater" vervangen

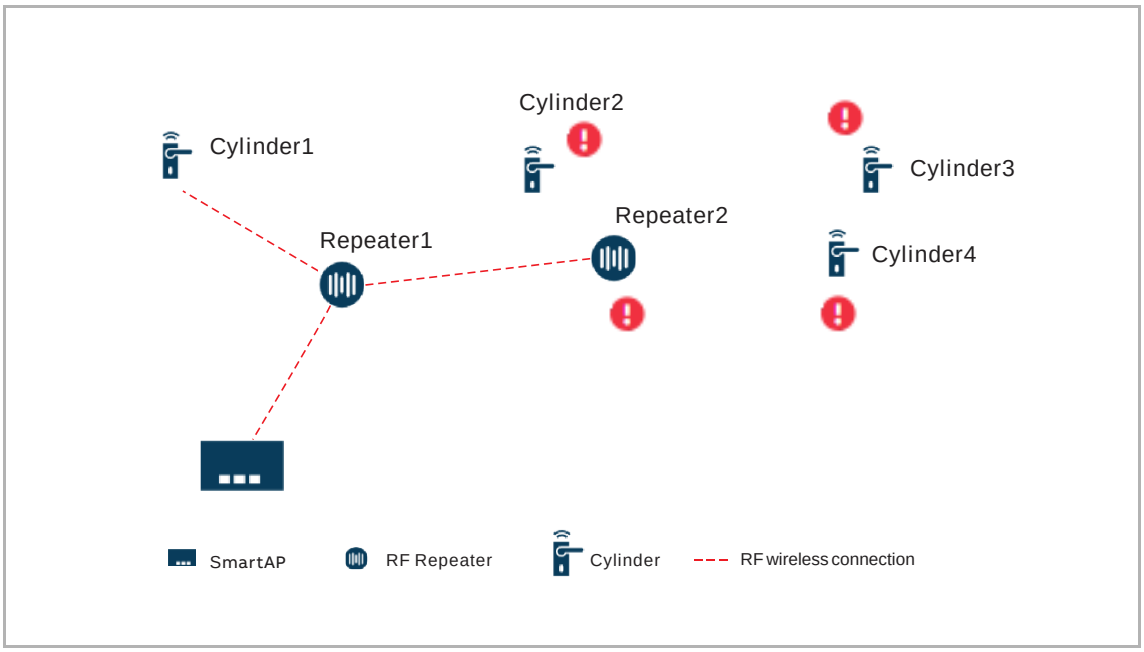
Als een "RF Repeater" beschadigd is (bijvoorbeeld "Repeater2" in de onderstaande figuur is defect), zijn alle "RF Repeaters" en alle daarmee gekoppelde "Electronic Locking Cylinders" offline. Een nieuwe "RF Repeater" (b.v. "Repeater3") wordt ingesteld ter vervanging van de beschadigde "RF Repeater" ("Repeater2").



Gelieve de onderstaande stappen te volgen:

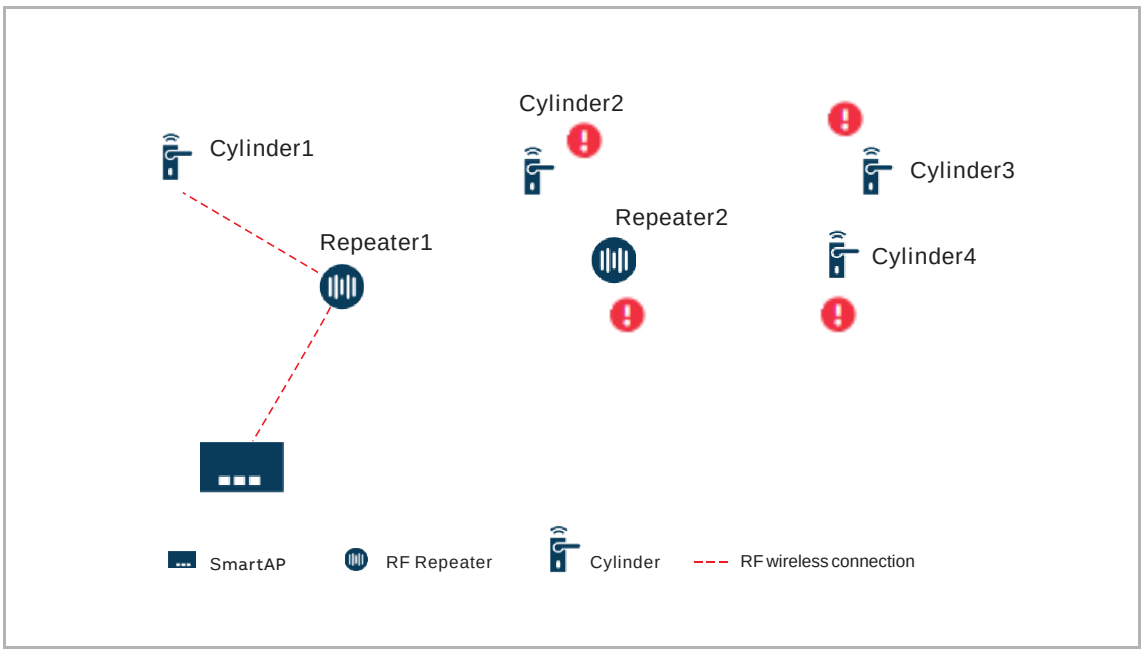
[1] Ontkoppel de cilinders van de defecte "RF Repeater".

zie hoofdstuk 10.11.1 “"Elektronische slotcilinder" loskoppelen“ op pagina 217



[2] Koppel de defecte "RF Repeater" los van het bovenliggende apparaat.

zie hoofdstuk 10.11.2 “"RF-repeater" loskoppelen“ op pagina 221



[3] Verwijder de defecte "RF Repeater" uit de lijst met apparaten.

zie hoofdstuk 10.12.2 “RF-repeater verwijderen“ op pagina 226

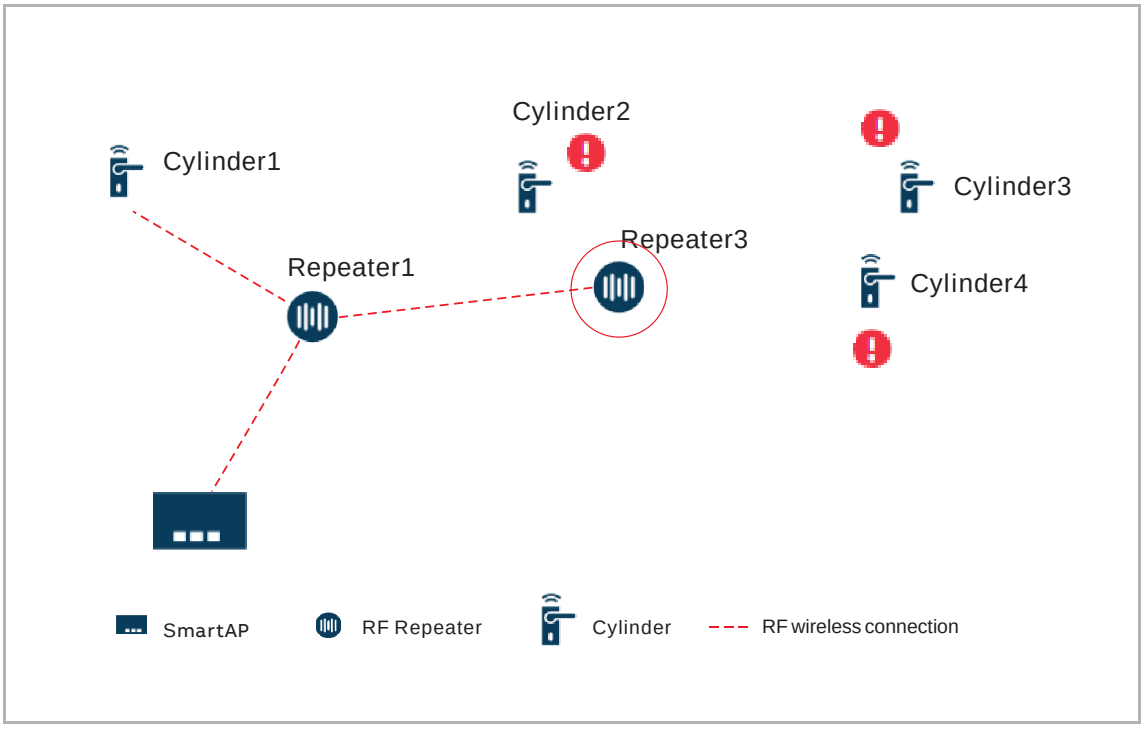
[4] Voeg een nieuwe "RF Repeater" toe.

zie hoofdstuk 10.3.3 “Toevoegen en lokaliseren van een "RF-repeater"“ op pagina 157

[5] Verbind de nieuwe "RF Repeater" met het bovenliggende apparaat.

De nieuwe "RF Repeater" moet worden gereset naar de fabrieksinstellingen voordat hij wordt aangesloten. Om dit te doen, houdt u de reset-knop 3 seconden ingedrukt tot de LED (wanneer het resetten is geslaagd) rood oplicht.

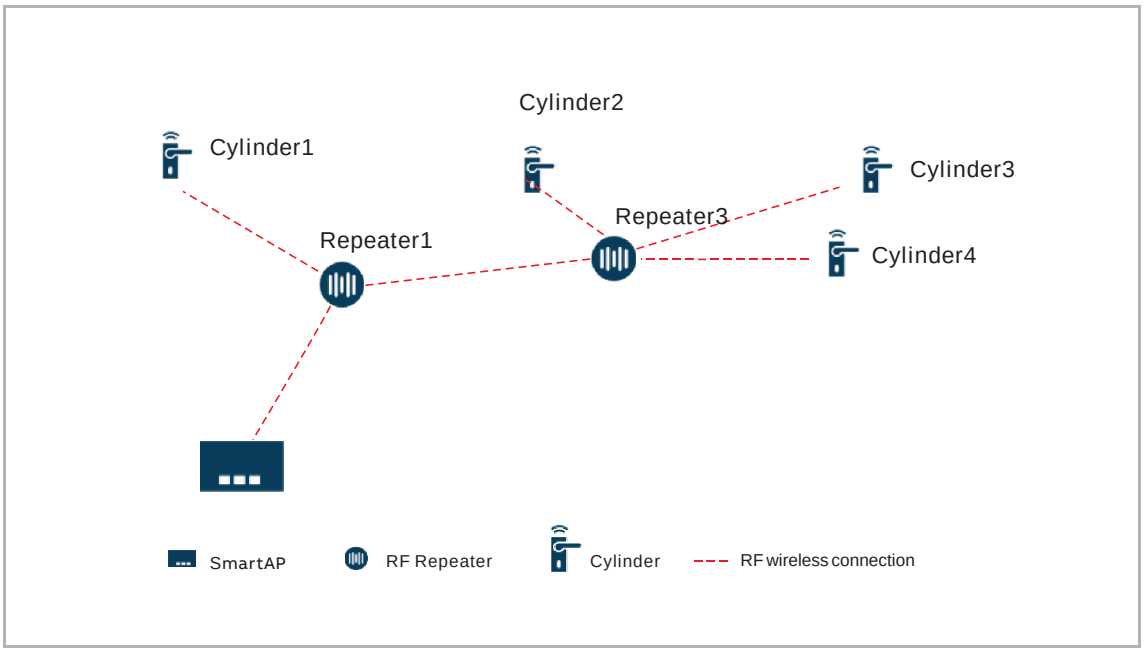
zie hoofdstuk 10.4.1 “"RF-repeater aansluiten"“ op pagina 161



[6] Koppel de "Elektronische Cilinders" aan de nieuwe "RF Repeater".

Tijdens het koppelingsproces moeten de "elektronische sluitcilinders" met behulp van de onderhoudskaart in de teach-in-modus worden gezet, zodat zij met hun apparaat van een hoger niveau kunnen worden gekoppeld.

zie hoofdstuk 10.4.2 ""Elektronische slotcilinder" verbinden“ op pagina 163



10.14 Verknoping tussen apparaten beheren

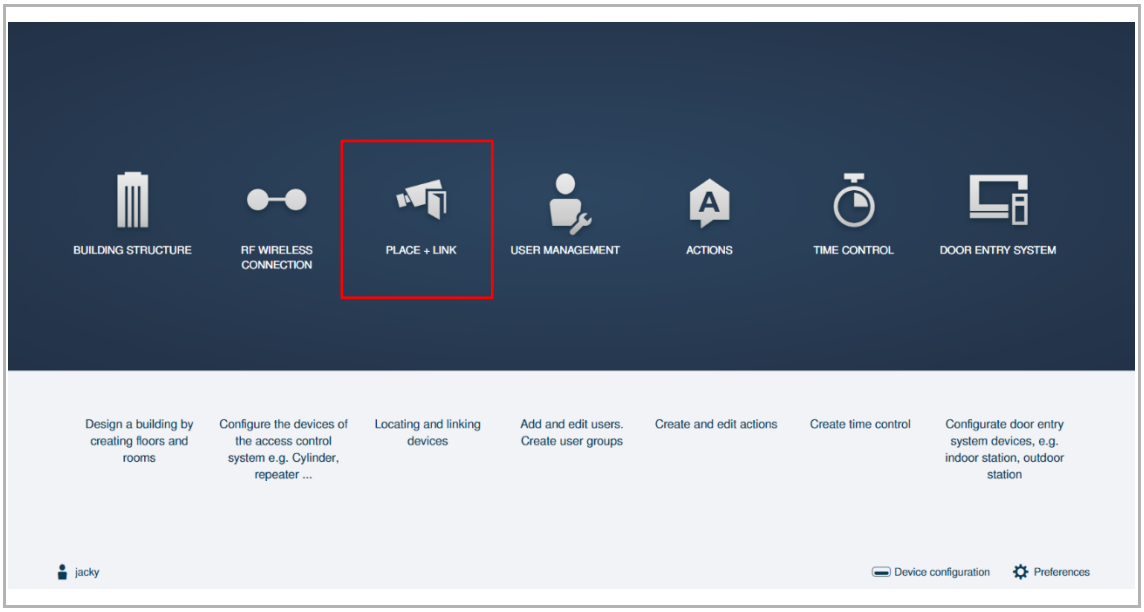
Op het "Smart Access Point" kunnen 2 AccessControl-apparaten aan elkaar worden gekoppeld. Wanneer het ene apparaat wordt getriggerd, kan de andere een actie uitvoeren.

Demonstratie

In deze demonstratie gaat de deurbel van het "Smart Access Point" over als de "kantoormodus" van de betreffende "elektronische slotcilinder" wordt geactiveerd.

Scherm Etageschema oproepen

Klik in het configuratiescherm op "Plaats + Link", "Gebouw 1", "Etage 1" om toegang te krijgen tot het etagescherm.



10.14.1 Verknoping toevoegen

De volgende handelingen zijn gebaseerd op de demonstratie. zie hoofdstuk 10.1 “AccessControl-topologie“ op pagina 139

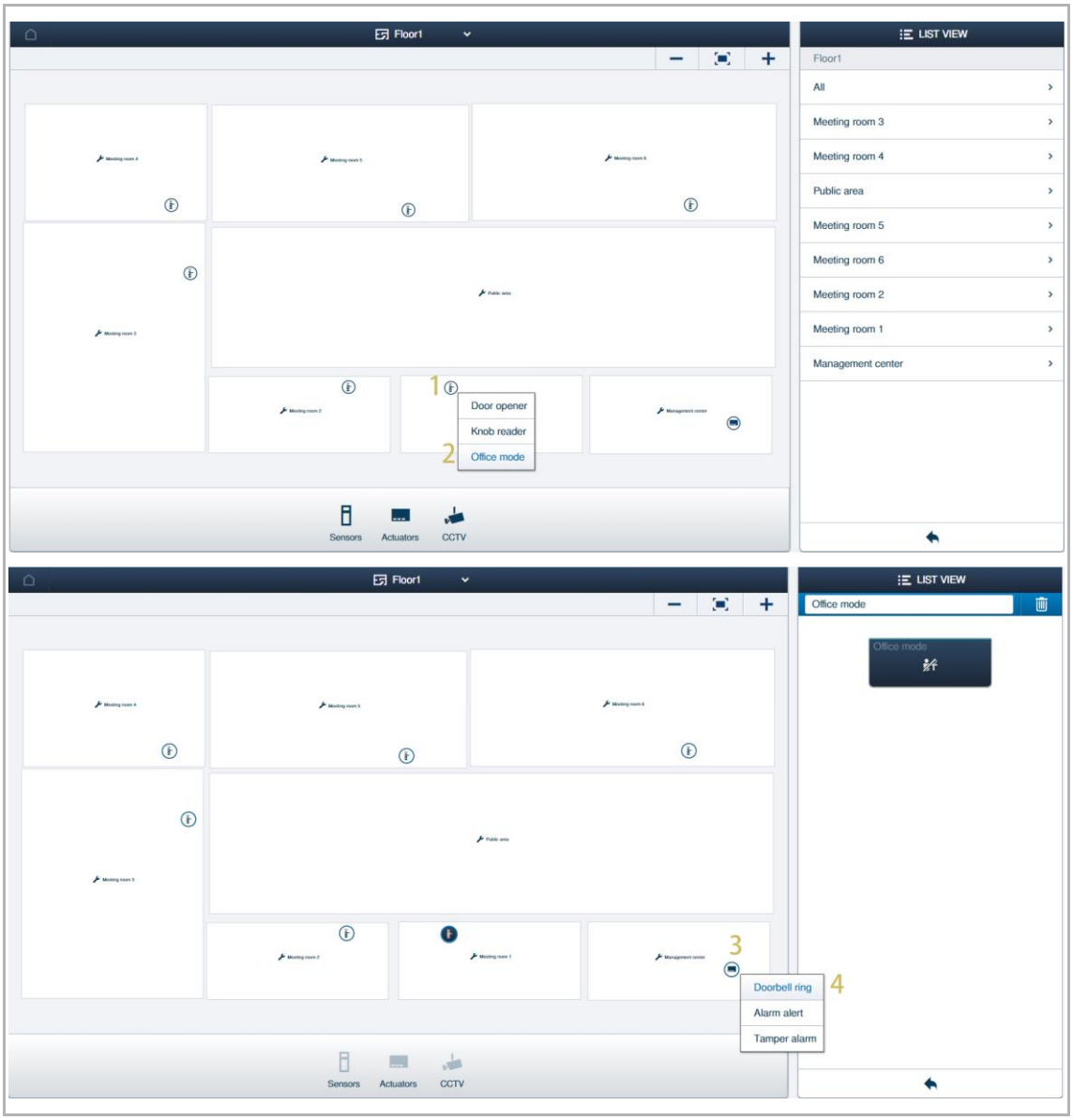
Volg de onderstaande stappen:

[1] Klik op het etagescherm op de betreffende "elektronische slotcilinder".

[2] Klik op "Kantoormodus".

[3] Klik op "Smart Access Point".

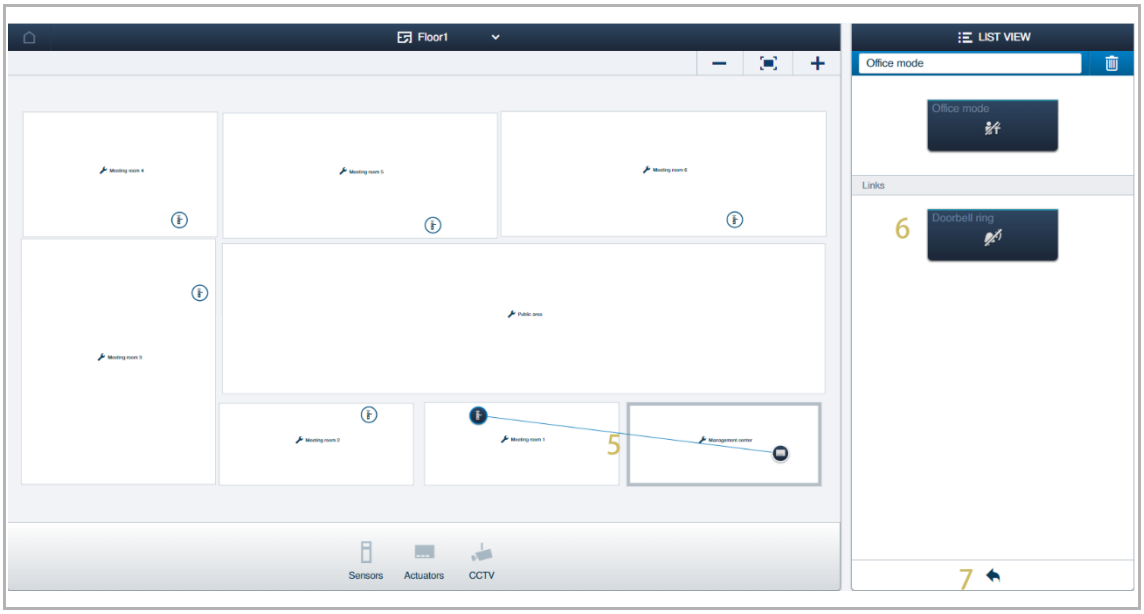
[4] Klik op "Deurbeloproep".



[5]Pairin Een geslaagde koppeling tussen de twee apparaten wordt aangegeven met een stippellijn.

[6] Gekoppeld apparaat wordt weergegeven in de lijst.

[7] Klik op " " om terug te gaan naar het etagescherm.



10.14.2 Verknopingen beheren

Volg de onderstaande stappen:

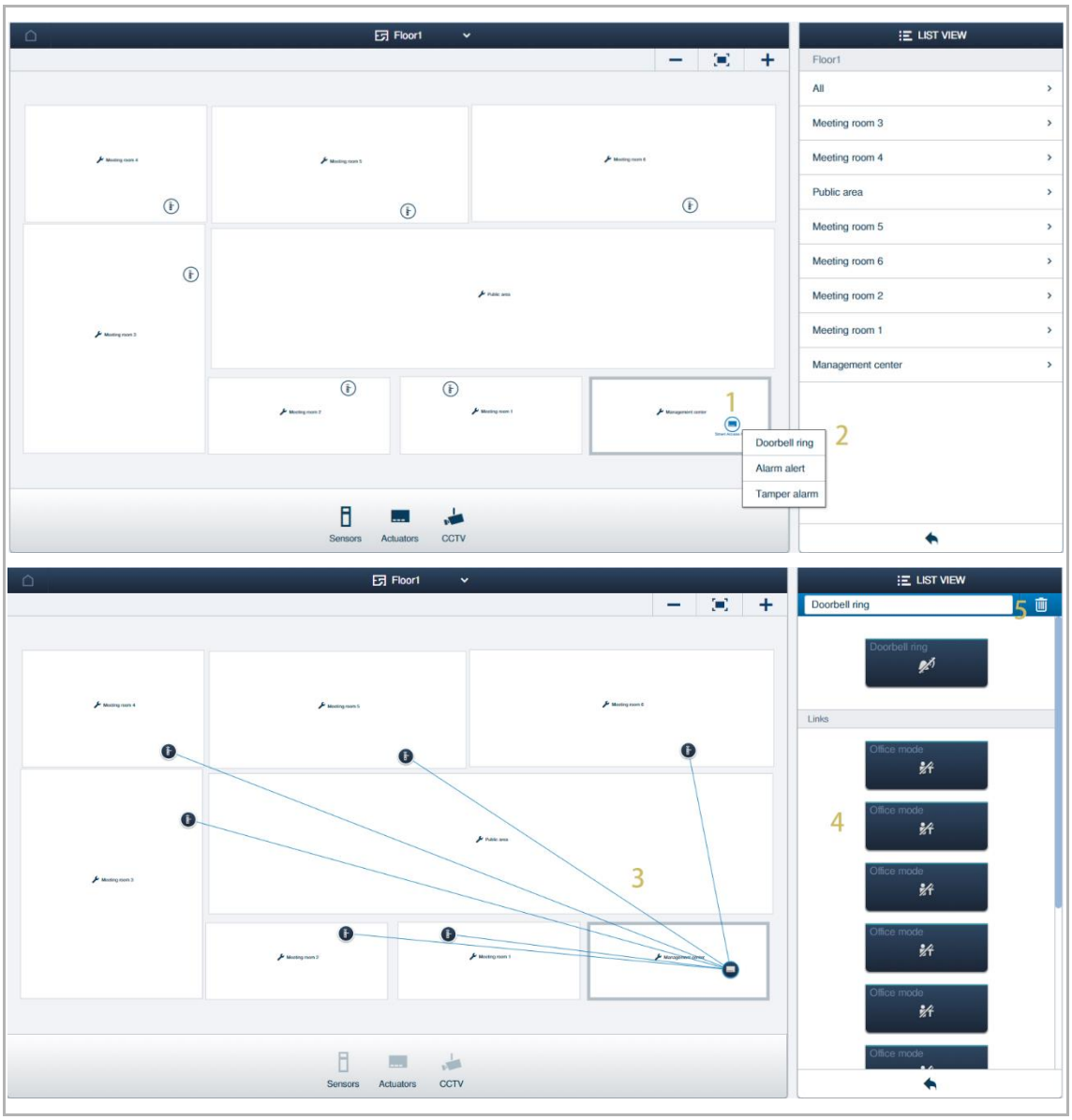
[1] Klik op het etagescherm op "Smart Access Point".

[2] Klik op "Deurbeloproep".

[3] De verknopingen worden weergegeven op het etagescherm.

[4] De gekoppelde apparaten worden ook in de lijst weergegeven.

[5] Het kanaal kan niet worden verwijderd als het meer dan 2 verknopingen heeft.



10.14.3 Verknopingen verwijderen

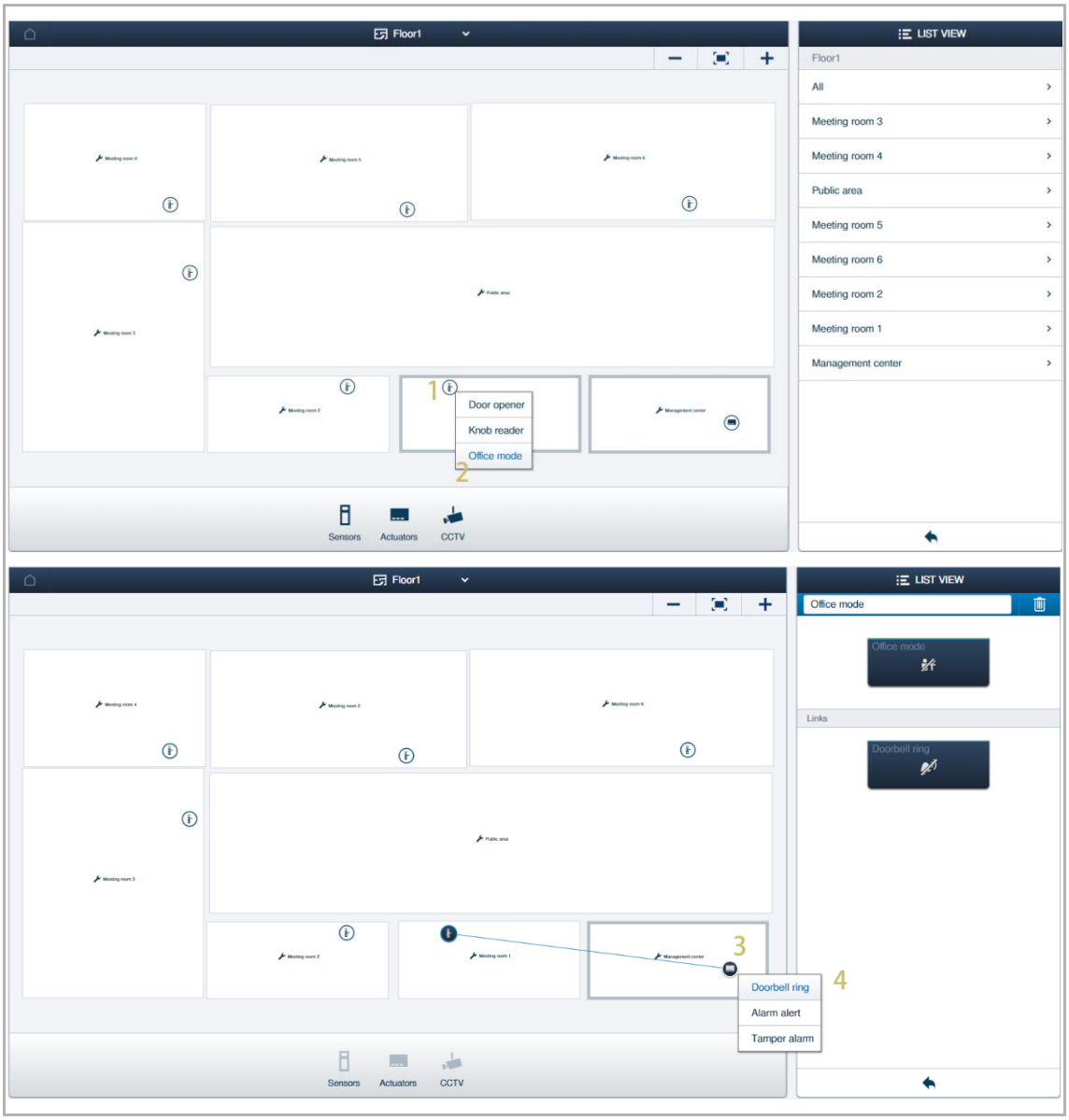
Volg de onderstaande stappen:

[1] Klik op het etagescherm op de betreffende "elektronische slotcilinder".

[2] Klik op "Kantoormodus".

[3] Klik op "Smart Access Point".

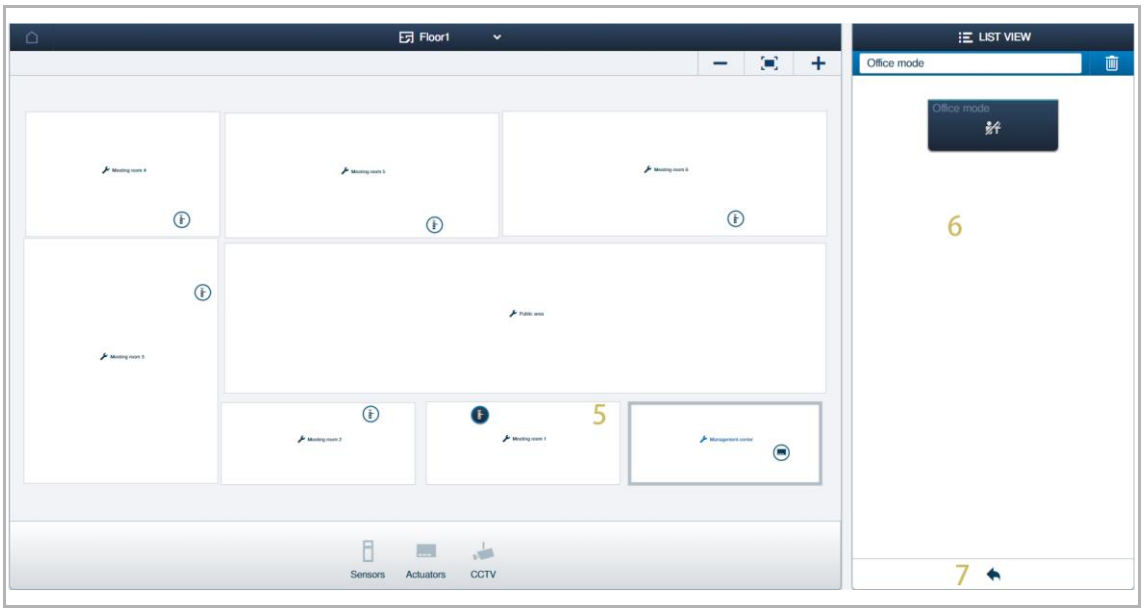
[4] Klik op "Deurbeloproep".



[5] Bij succes wordt geen verknoping weergegeven tussen de twee apparaten.

[6] Er wordt geen gekoppeld apparaat weergegeven in de lijst.

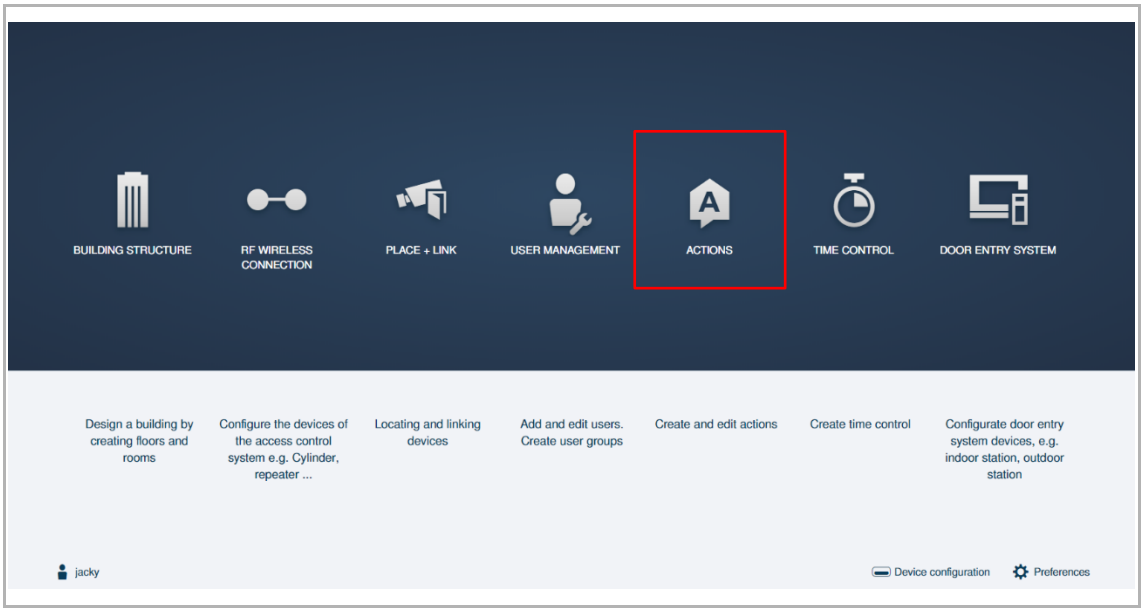
[7] Klik op " " om terug te gaan naar het etagescherm.



11 Acties beheren

Scherm "Actie" oproepen

Klik in het configuratiescherm op "Acties" om het scherm "Acties" te openen.



Demonstratie

In deze demonstratie is de "Cilinder 1" offline tijdens werktijd (bijvoorbeeld van 8:00 tot 17:00 uur) en het "Smart Access Point" krijgt en slaat alarm.

11.1 Actie toevoegen

De volgende handelingen zijn gebaseerd op de demonstratie.

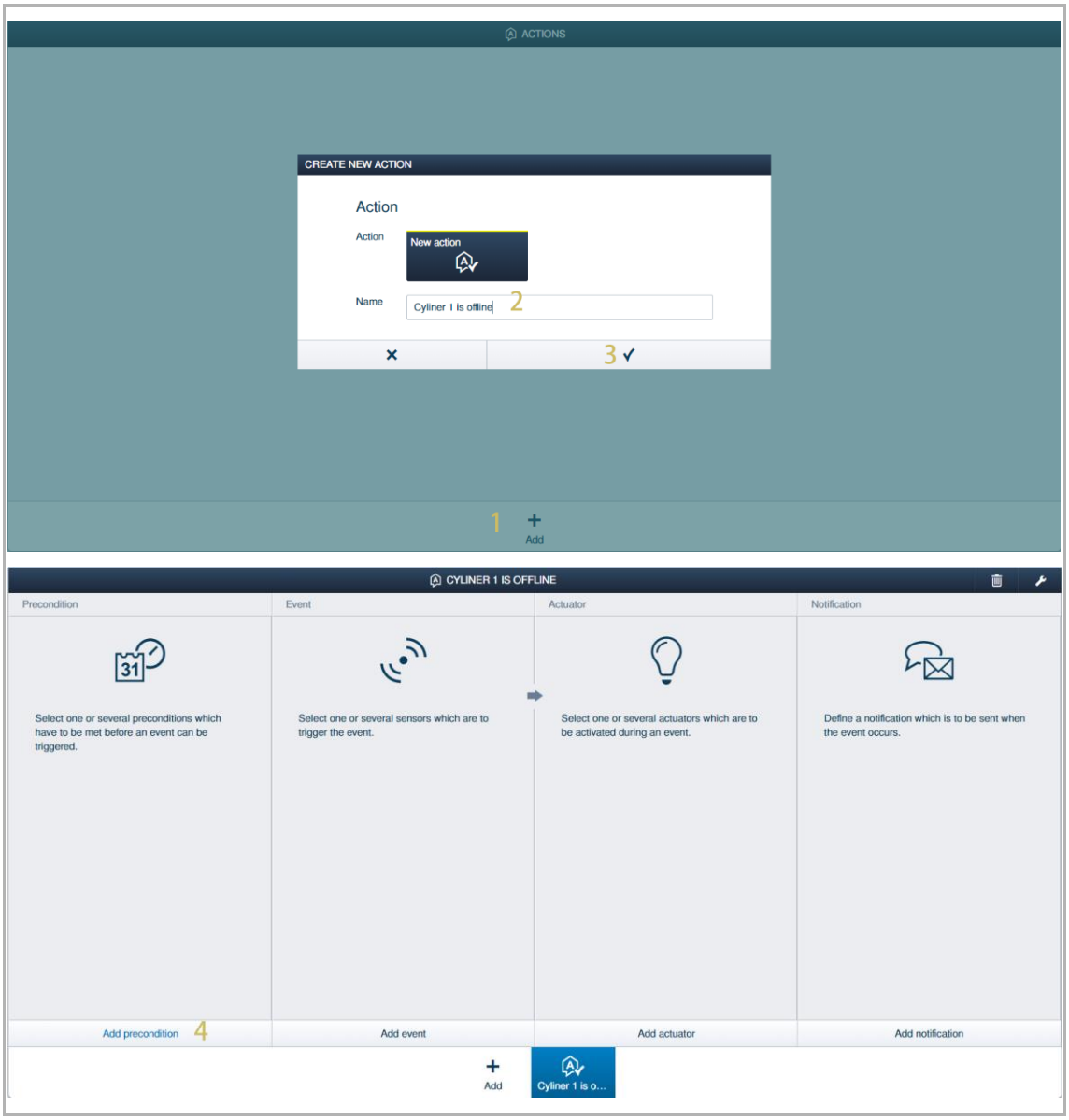
Volg de onderstaande stappen:

[1] Klik in het scherm "Actie" op "+".

[2] Voer de naam in voor de actie.

[3] Klik op "√" om op te slaan.

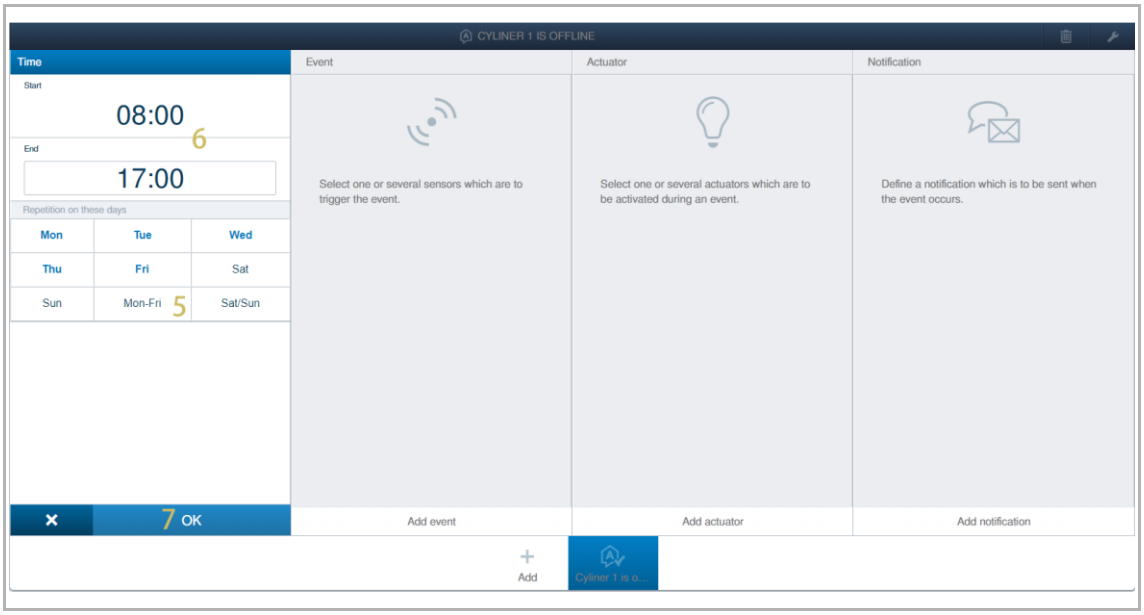
[4] Klik op het betreffende actiescherm, klik op "Voorwaarde toevoegen" en vervolgens op "Tijd".



[5] Klik op "ma-vr" om de dagen van maandag tot vrijdag op de selecteren.

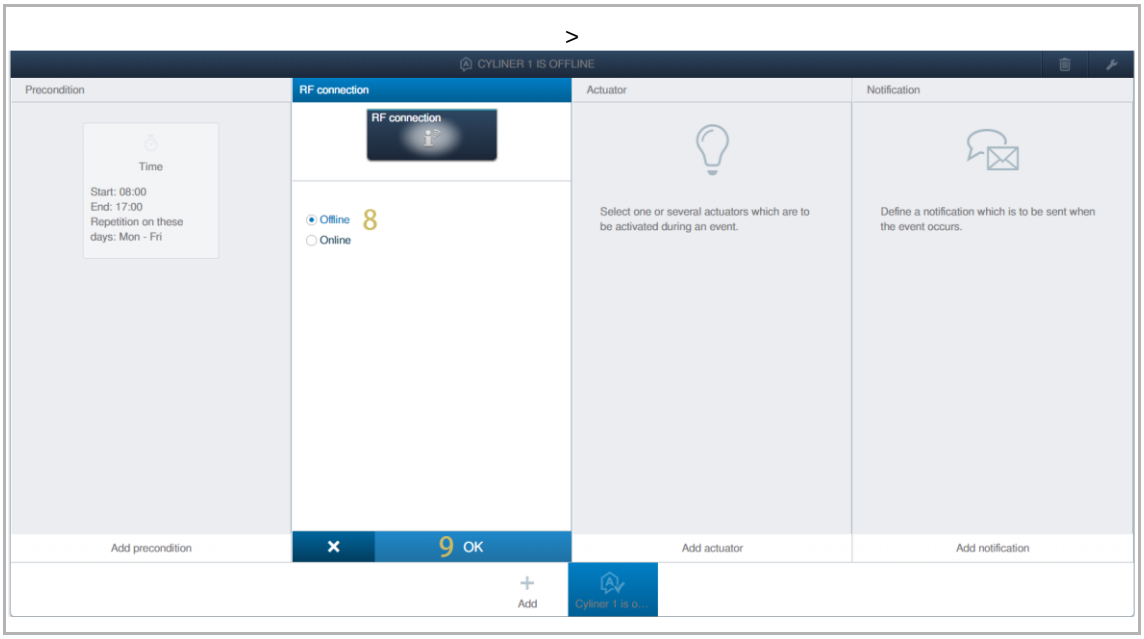
[6] Voer de start- en eind tijd in.

[7] Klik op "OK" om te bewaren.



[8] Klik op "Gebeurtenis toevoegen", gevolgd door "Toegangscontrole", "Cilinder 1", "RF-verbinding", selecteer "Offline".

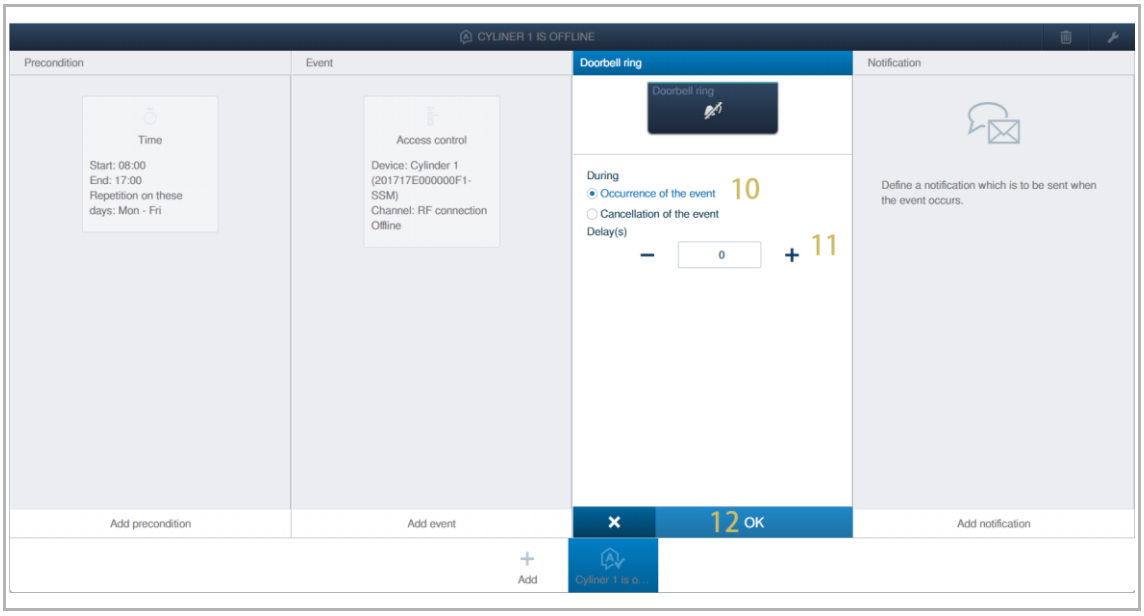
[9] Klik op "OK".



[10]Klik op "Aktor toevoegen", gevolgd door "SmartAP", "Smart Access Point", "Deurbeloproep" en selecteer "Intreden van de gebeurtenis".

[11]Voer de vertragingstijd tussen de activering van de aktor en het triggeren van de gebeurtenis.

[12]Klik op "OK".



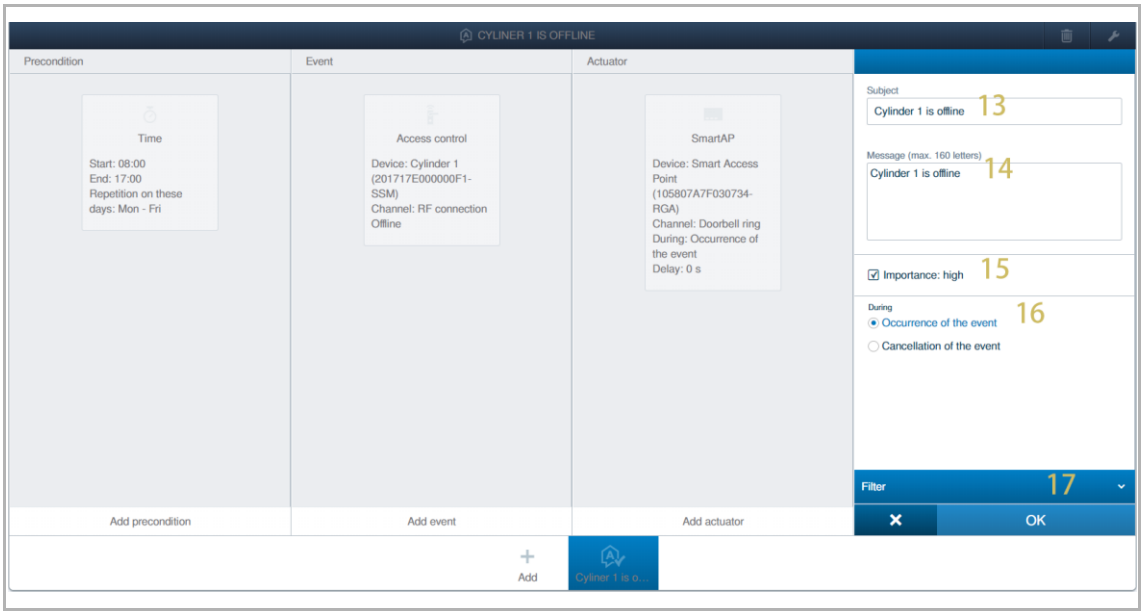
[13]Klik op "Melding toevoegen" en voer een onderwerp in.

[14]Voer de beschrijving in.

[15]Als het keuzevakje "Prioriteit: hoog" is geactiveerd, wordt het bericht als alarm ontvangen, anders wordt het bericht als bericht ontvangen.

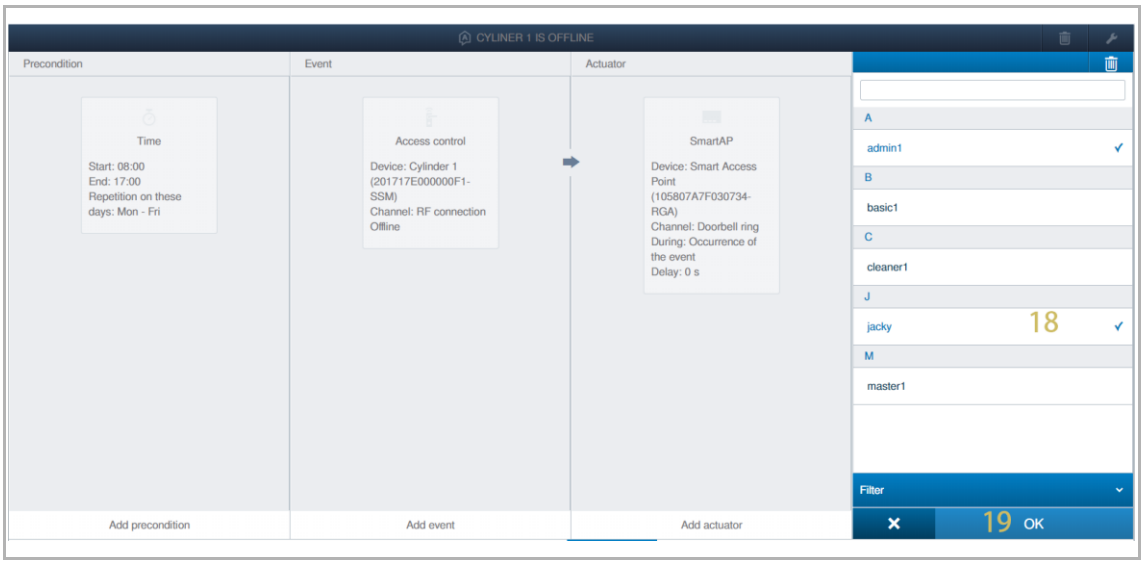
[16]Selecteer "Intreden van de gebeurtenis".

[17]Klik op "Filter".

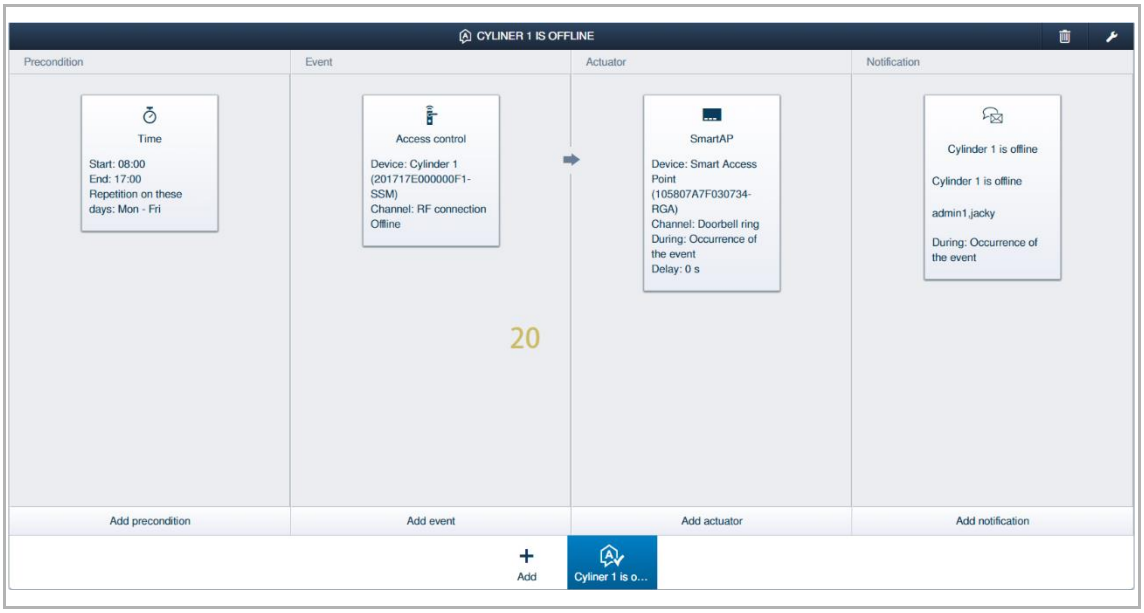


[18]Klik om de gebruikers te selecteren.

[19]Klik op "OK" om te bewaren.



[20]Het resultaat wordt weergegeven op het scherm.



11.2 Acties beheren

Volg de onderstaande stappen:

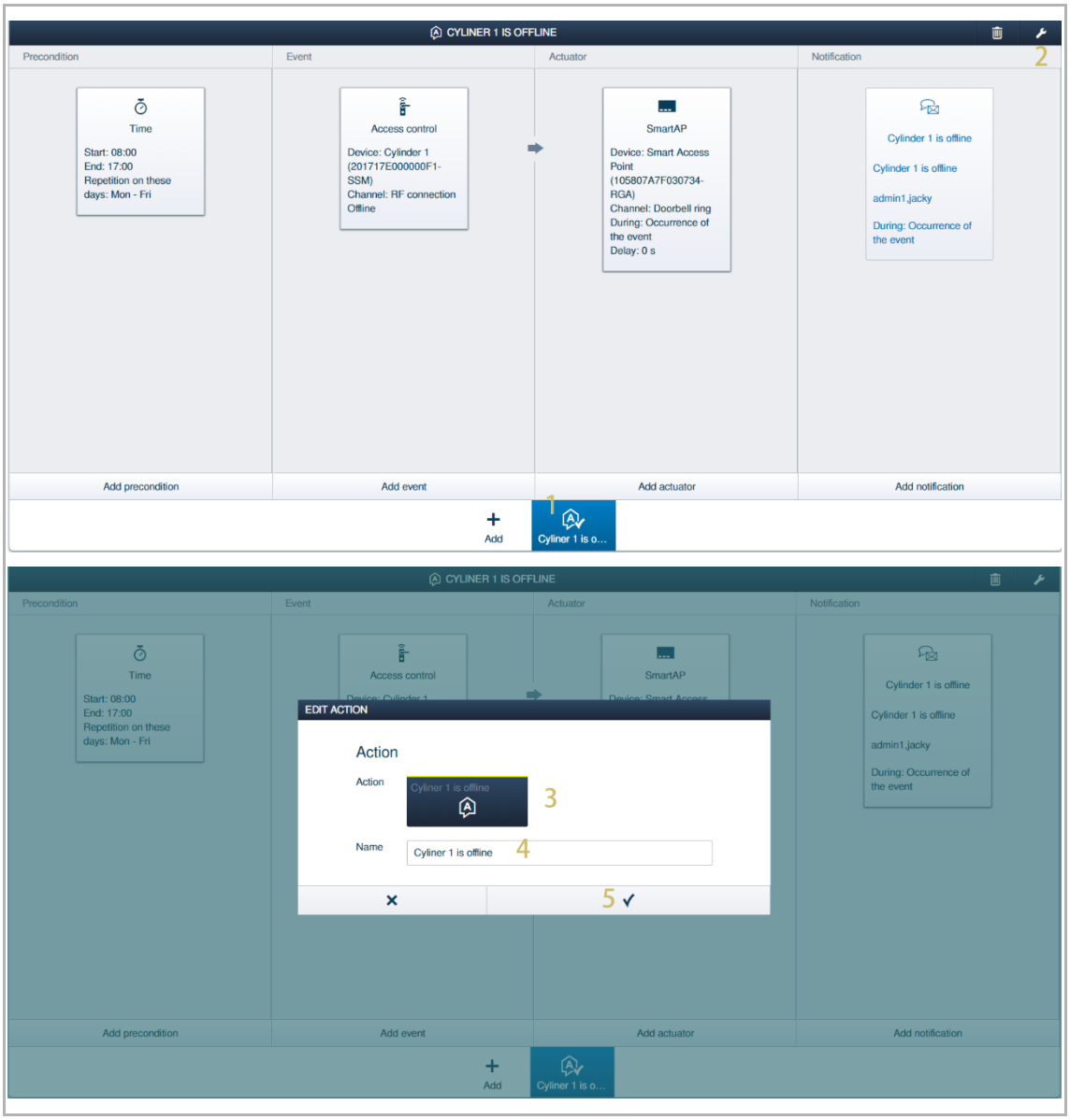
[1] Klik in het scherm "Acties" op de betreffende actie.

[2] Klik op "".

[3] Klik op het symbool om de actie te activeren of te deactiveren.

[4] Geef de actie een andere naam.

[5] Klik op "√" om op te slaan.



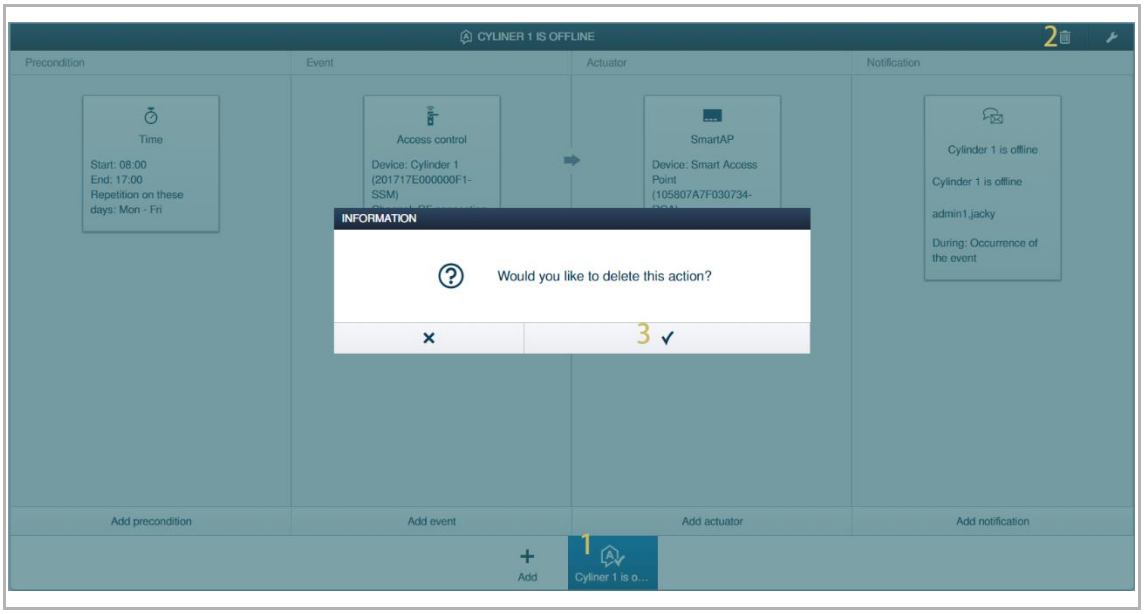
11.3 De actie verwijderen

Volg de onderstaande stappen:

[1] Klik in het scherm "Acties" op de betreffende actie.

[2] Klik op " ".

[3] Klik op "√" om op te slaan.



12 Cyberveiligheid

12.1 Disclaimer

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

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

12.2 Performance and service and network performance

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

Port and service

Port	Service	Purpose
53	TCP	DNS
80	TCP	HTTP web service
443	TCP	HTTPS web service
5222	TCP	Service for XMPP client
5280	TCP	Service for XMPP HTTP administrator service
5281	TCP	Service for XMPP HTTPS administrator service
49152	TCP	UPnP
53	UDP	DNS
1900	UDP	UPnP service
31002	UDP	Searched for & managed PC client tools
7000	TCP	Private protocol service
10700	TCP	Private protocol service (TLS)
8887	TCP	Used for upgrading process
7777	TCP	Private protocol service
10777	TCP	Private protocol service (TLS)
7777	UDP	Private protocol service

12.3 Deployment guideline

Please do not install it within a public place and ensure that physical access to the devices is granted only to trusted person.

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

During commissioning, the RF cylinder and RF repeater need to be added to the one by one following the SmartAP commissioning process, it’s extremely required that the observed indications from RF cylinder and repeater should be confirmed correctly.

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

12.4 Upgrading

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

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

12.5 Backup/restore

Some configurations of devices can be download to locally by webpage, the password is needed to encrypt the exported configuration data, the configurations include,

- SmartAP device configuration parameters
- User data
- Device data including Access control system device, Door entry system devices and CCTV system device

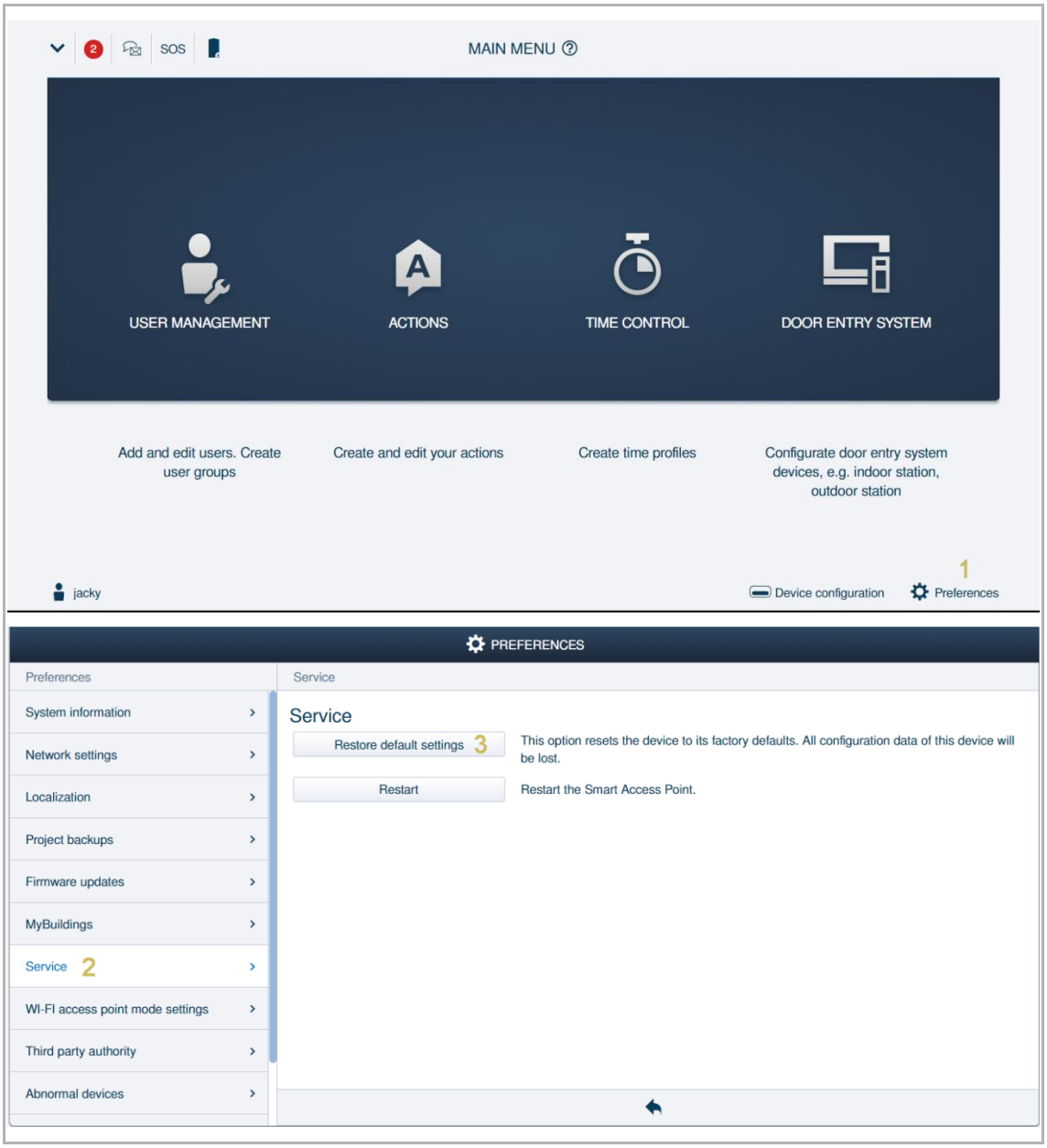
When restoring from the backup configured, the exported file needs to be updated to the device by webpage, and the respective password used when exporting the configuration is needed.

12.6 Data pursing

In case of quitting from the working system (e.g. replaced by another device, re-install in another system…), All the data stored in the device need to be purged by the “Restore default setting” in webpage as below,

Login in the web page by admin user account.

On the configuration screen, following the steps below,



12.7 Malware prevention solution

The device D0401. 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 ABB can be accepted.

12.8 Default passwords and user accounts

In factory default, the device has below passwords or user accounts,

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

All the mentioned default passwords and user accounts are mandatory to be changed during the first commissioning.

12.9 Password rule

The password for all user accounts need to fulfill below rules,

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

12.10 Logging

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

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

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

Device	Information for events
RF Repeater	Loss connection with SmartAP event
RF cylinder	Battery status Loss connection from system event Unlock event Battery low event Swipe Card event

Every log information contains time, event source, behavior, and signature.

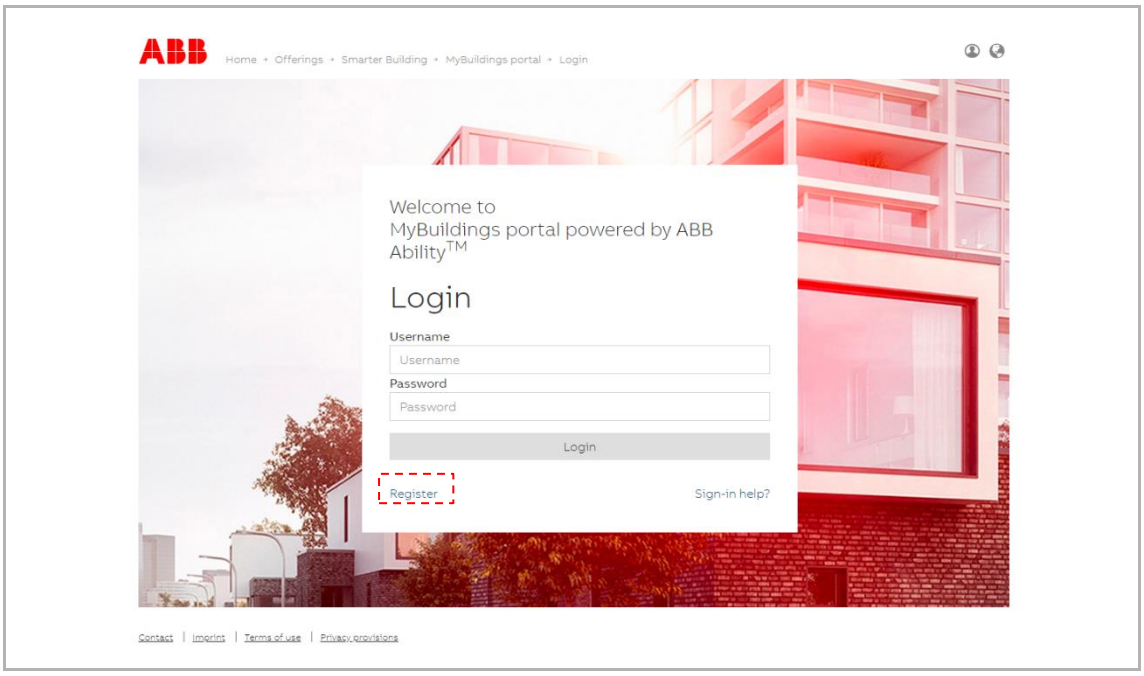
The device will automatically generate logs and store them when above events occur.

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

13 Bijlage

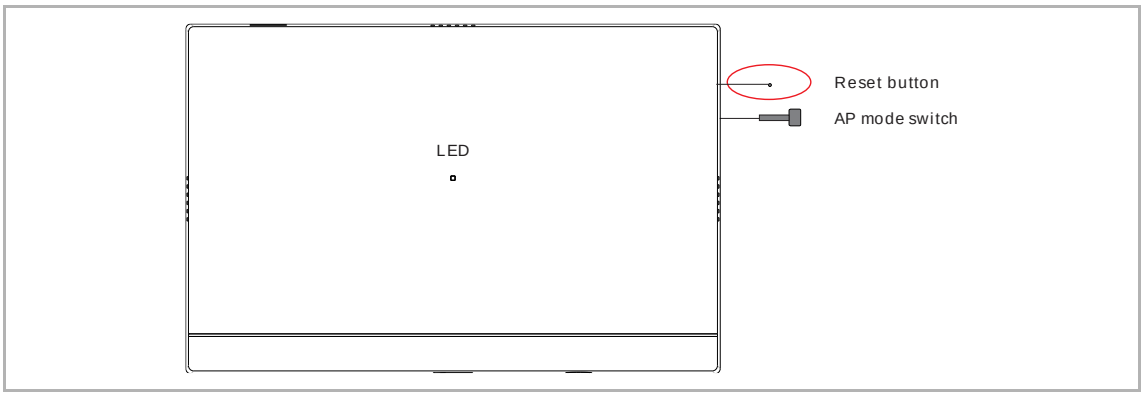
13.1 Een account registreren via het MyBuildings-portal

Ga naar de link: https://mybuildings.abb.com en klik op "Registreren". Vul het vereiste formulier in om een account te registreren. Vervolgens activeert u het gebruikersaccount nadat u een e-mail hebt ontvangen van het MyBuildings-portaal.



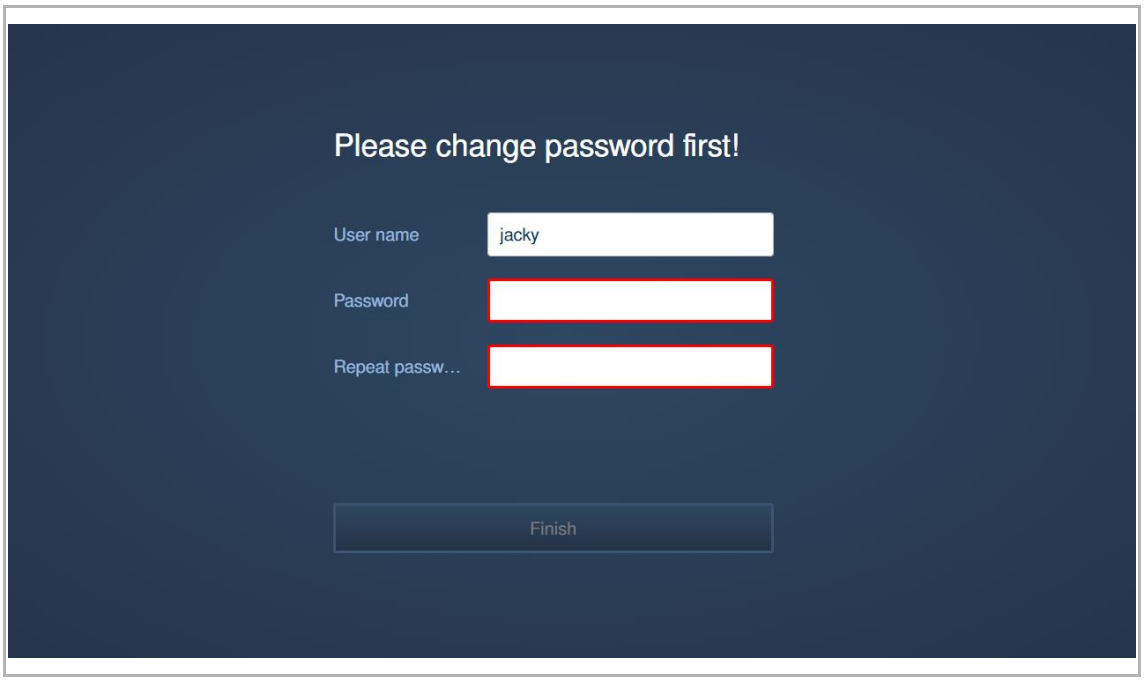
13.2 Wachtwoord voor de eerste beheerder resetten

Houd de resetknop 10 s lang ingedrukt.



1. Reset-optie = reset apparaat zonder MyBuildings-account

Als de reset-optie is ingesteld op "Reset apparaat zonder MyBuildings-account" in de eerste setup, kunt u het wachtwoord voor de eerste admin direct wijzigen door twee keer een nieuw wachtwoord in te voeren.

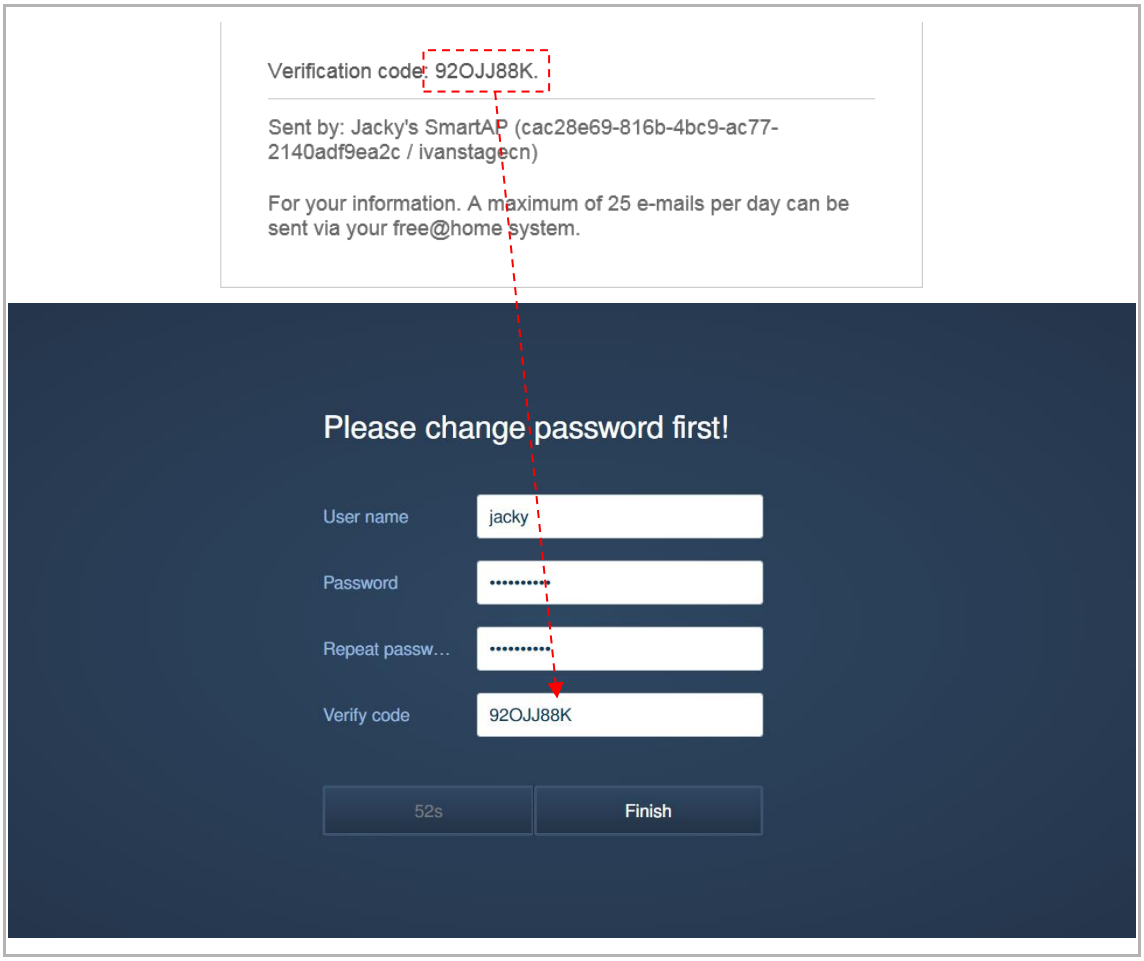


2. Reset-optie = reset apparaat met MyBuildings-account

Als de reset-optie is ingesteld op "Reset apparaat met MyBuildings-account" in de eerste setup, is naast het twee keer invoeren van het nieuwe wachtwoord ook een verificatiecode nodig.

Opmerking

Als u bij de eerste setup een e-mail hebt ingesteld voor het ontvangen van de verificatiecode, kunt u de verificatiecode per e-mail toegestuurd krijgen.



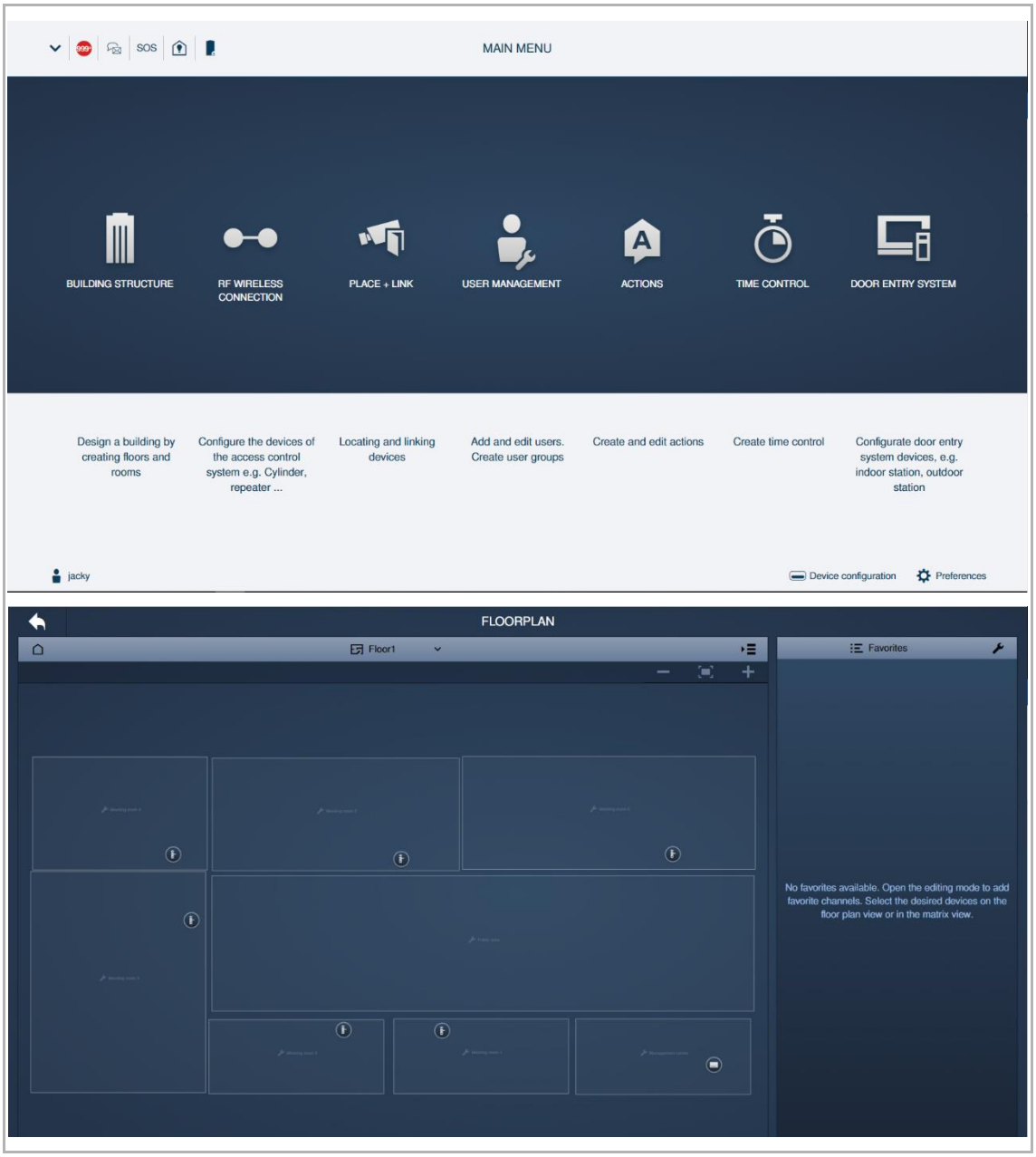
13.3 Gebruikersbeheer

13.3.1 Gebruikersrollen

Er zijn 4 optionele gebruikersrollen die worden ondersteund door het "Smart Access Point".

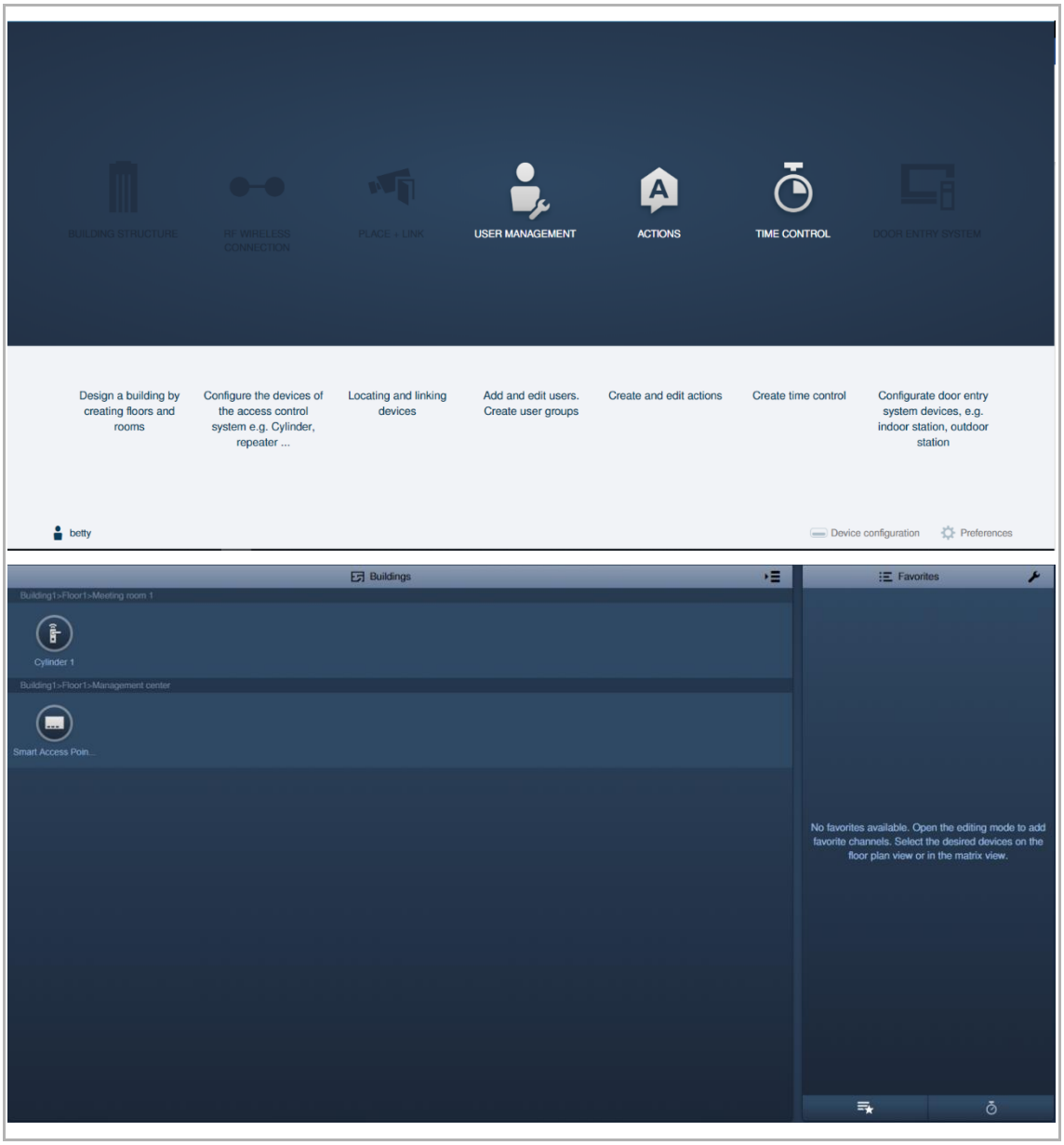
1. Admin-gebruikers

- De eerste admin-gebruiker wordt alleen bij de eerste setup aangemaakt. De andere admin-gebruikers kunnen worden aangemaakt door de eerste admin-gebruiker of andere admin-gebruikers. zie hoofdstuk 8.3 “Eerste configuratie“ op pagina 19.
- Admin-gebruikers kunnen andere admin-gebruikers, master-gebruikers, standaardgebruikers en gebruikers van derde aanbieders beheren.
- Admin-gebruikers kunnen alle functies op het configuratiescherm bedienen.
- Admin-gebruikers kunnen alle functies op het besturingsscherm bedienen.



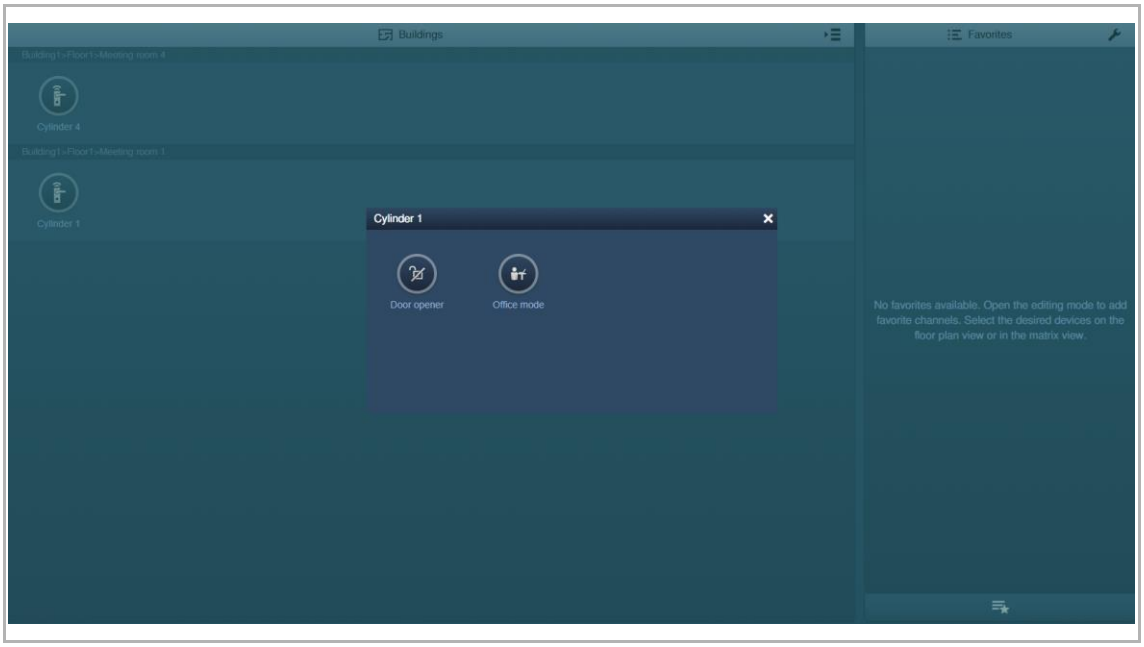
2. Master-gebruikers

- Master-gebruikers kunnen worden aangemaakt door een admin-gebruiker of een andere master-gebruiker.
- Master-gebruikers kunnen andere master-gebruikers, standaardgebruikers en gebruikers van derde aanbieders beheren.
- Master-gebruikers kunnen enkele functies op het configuratiescherm bedienen.
- Master-gebruikers kunnen het "Smart Access Point" en de toegewezen "elektronische slotcilinder" bedienen.



3. Standaardgebruikers

- Standaardgebruikers kunnen worden aangemaakt door een admin-gebruiker of een master-gebruiker.
- Standaardgebruikers kunnen alleen de toegewezen "elektronische slotcilinder" bedienen.



4. Gebruikers van derde aanbieders

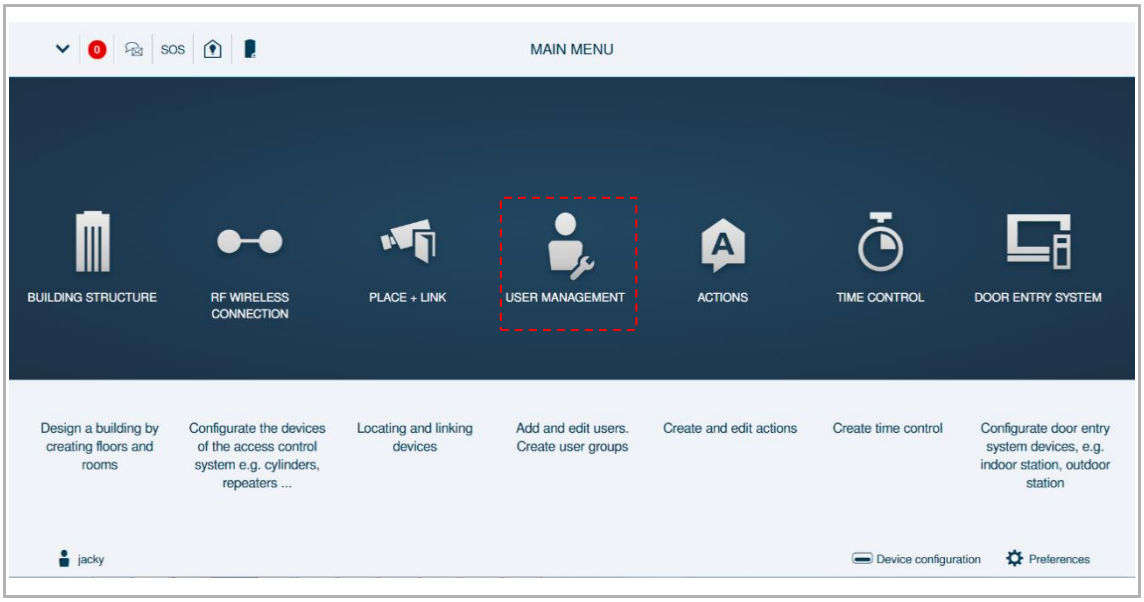
- Gebruikers van derde aanbieders kunnen worden aangemaakt door een admin-gebruiker of een master-gebruiker.
- Gebruikers van derde aanbieders kunnen alleen de toegewezen "elektronische slotcilinder" gedurende een aangegeven tijd bedienen.

13.3.2 Gebruikers toevoegen

Opmerking
Een "Smart Access Point" kan 2000 gebruikers hebben.

Scherm "Gebruikers" oproepen

Klik in het configuratiescherm op "Gebruikersbeheer" om het scherm "Gebruikers" te openen.

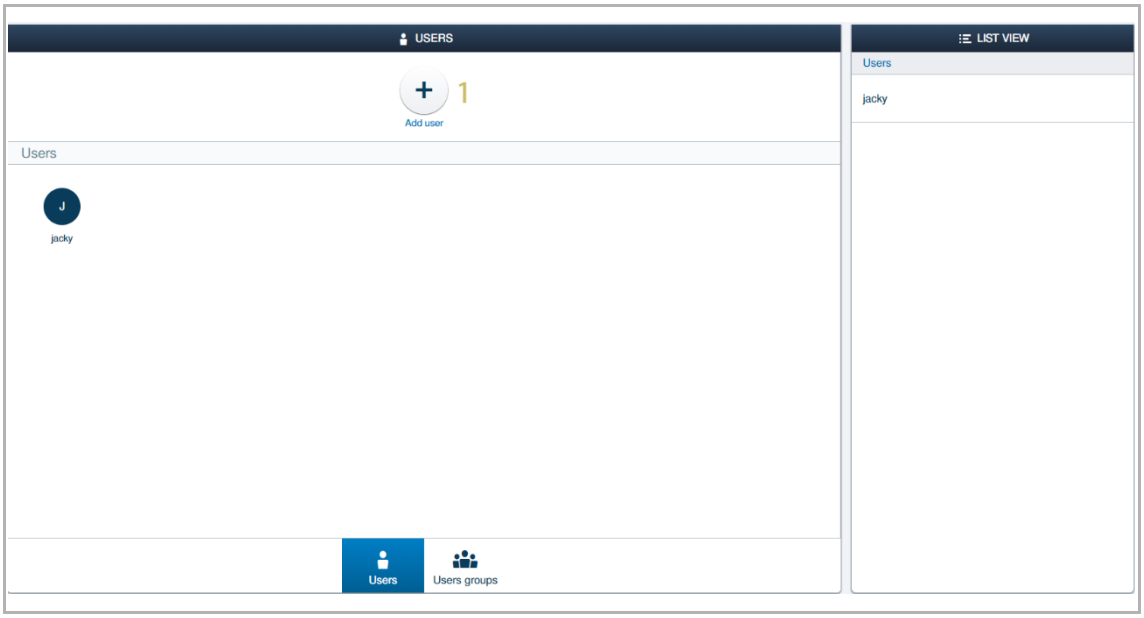


Gebruikers toevoegen

1. Admin-gebruikers toevoegen

Volg de onderstaande stappen:

[1] Klik in het scherm "Gebruikers" op "Naam toev".



[2] Voer de gebruikersnaam in; deze gebruikersnaam mag niet gelijk zijn aan een bestaande gebruikersnaam.

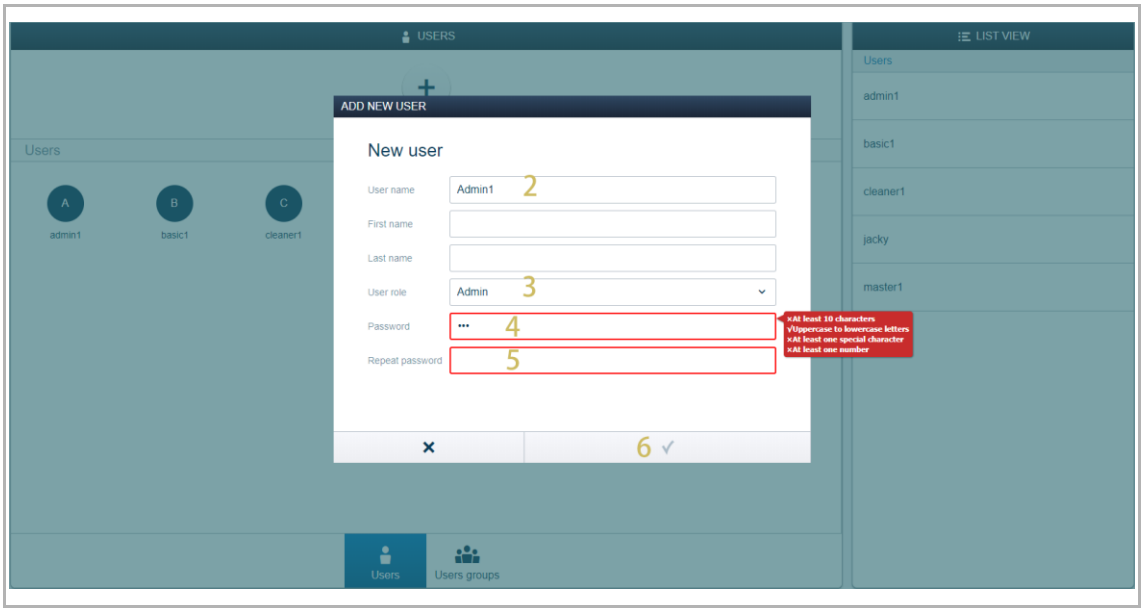
[3] Selecteer "Admin" uit de keuzelijst.

[4] Voer het wachtwoord volgens de op het scherm weergegeven regels in.

[5] Voer het wachtwoord opnieuw in

[6] Klik op "OK" om te bewaren.

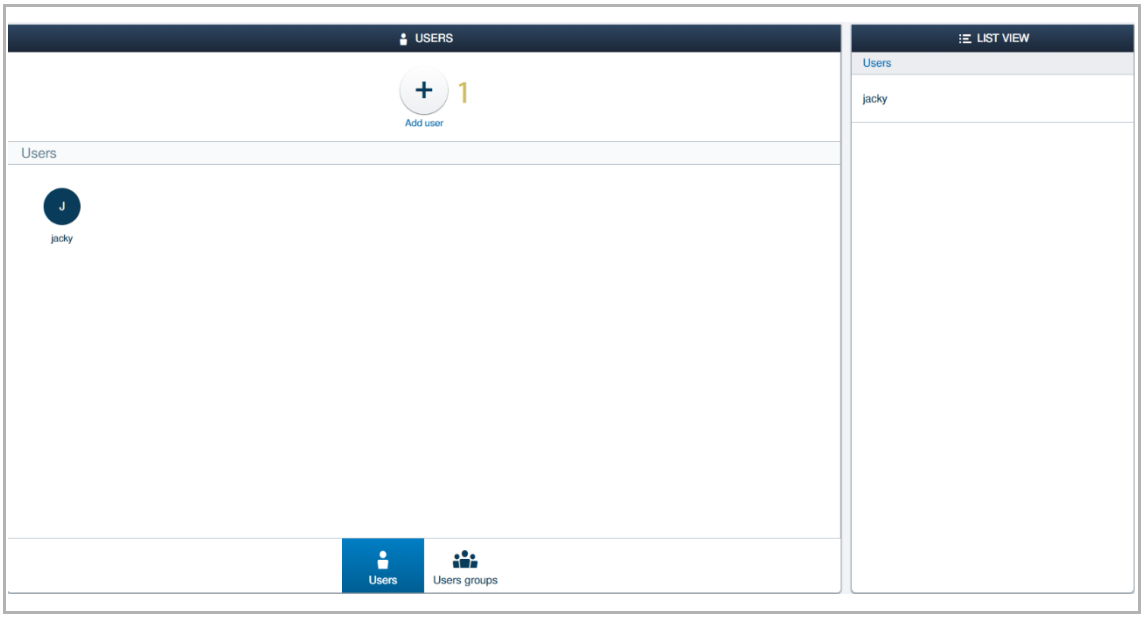
Herhaal de stappen 1-6 om admin-gebruikers toe te voegen.



2. Master-gebruikers toevoegen

Volg de onderstaande stappen:

[1] Klik in het scherm "Gebruikers" op "Naam toev".



[2] Voer de gebruikersnaam in; deze gebruikersnaam mag niet gelijk zijn aan een bestaande gebruikersnaam.

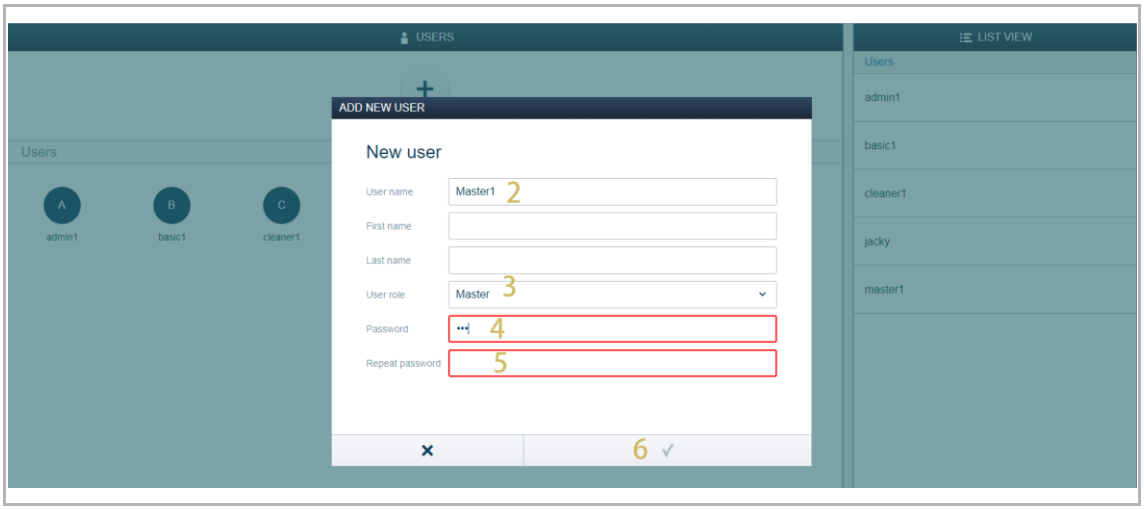
[3] Selecteer "Master" uit de keuzelijst.

[4] Voer het wachtwoord volgens de op het scherm weergegeven regels in.

[5] Voer het wachtwoord opnieuw in.

[6] Klik op "OK" om te bewaren.

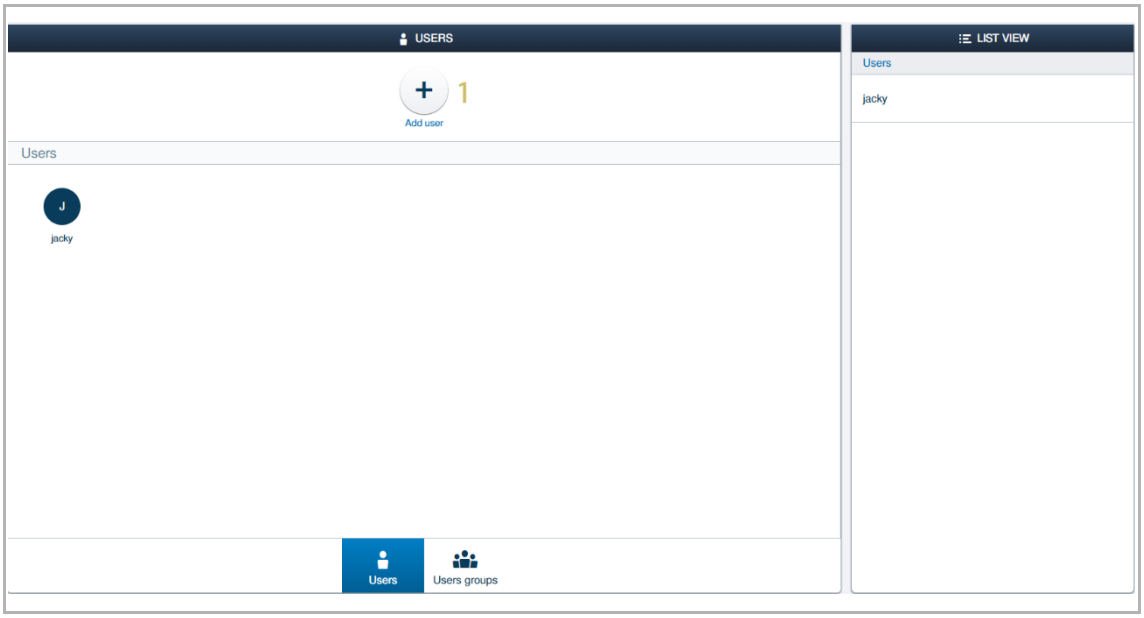
Herhaal de stappen 1-6 om master-gebruikers toe te voegen.



3. Standaardgebruikers toevoegen

Volg de onderstaande stappen:

[1] Klik in het scherm "Gebruikers" op "Naam toev".



[2] Voer de gebruikersnaam in; deze gebruikersnaam mag niet gelijk zijn aan een bestaande gebruikersnaam.

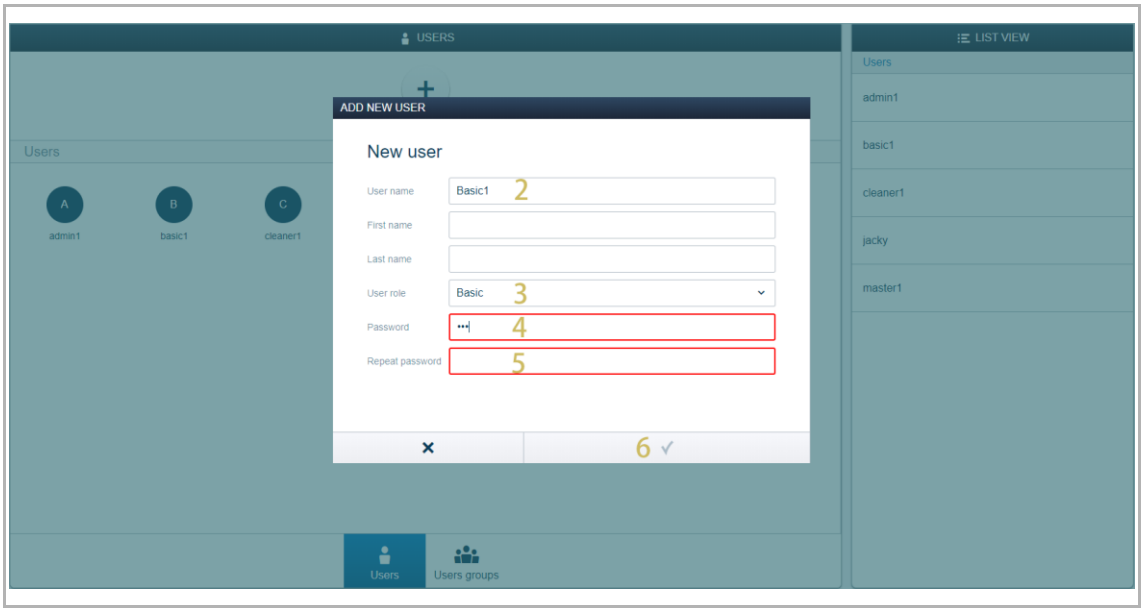
[3] Selecteer "Std.acc." uit de keuzelijst.

[4] Voer het wachtwoord volgens de op het scherm weergegeven regels in.

[5] Voer het wachtwoord opnieuw in.

[6] Klik op "OK" om te bewaren.

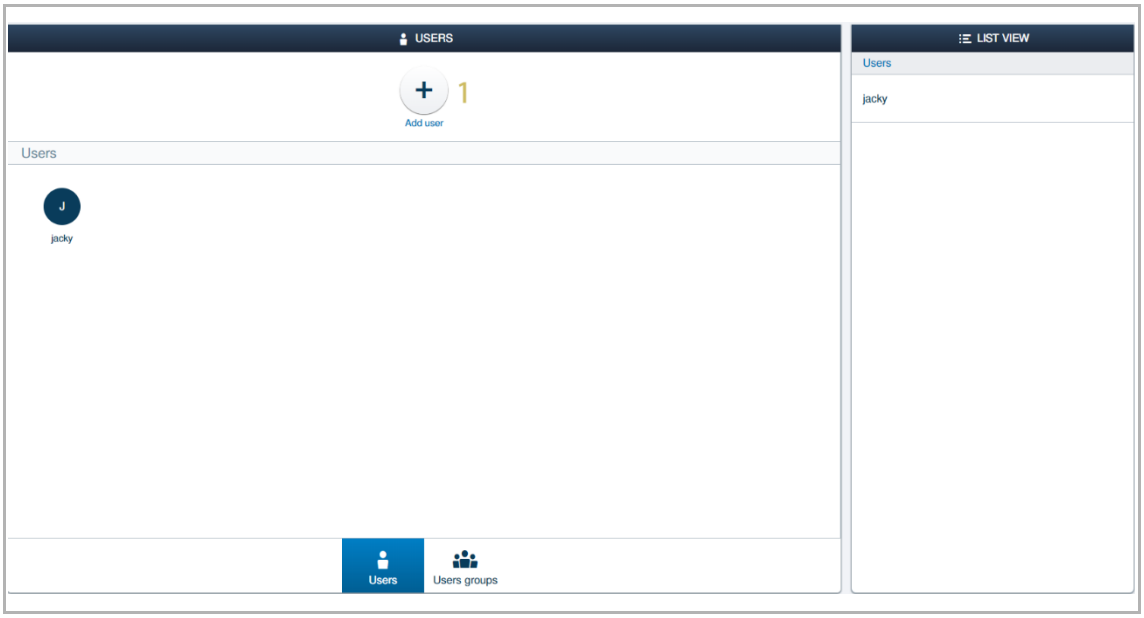
Herhaal de stappen 1-6 om standaardgebruikers toe te voegen.



4. Gebruikers van derde aanbieders toevoegen

Volg de onderstaande stappen:

[1] Klik in het scherm "Gebruikers" op "Naam toev".



[2] Voer de gebruikersnaam in; deze gebruikersnaam mag niet gelijk zijn aan een bestaande gebruikersnaam.

[3] Selecteer "Derde aanbieder" uit de keuzelijst.

[4] Voer het wachtwoord volgens de op het scherm weergegeven regels in.

[5] Voer het wachtwoord opnieuw in.

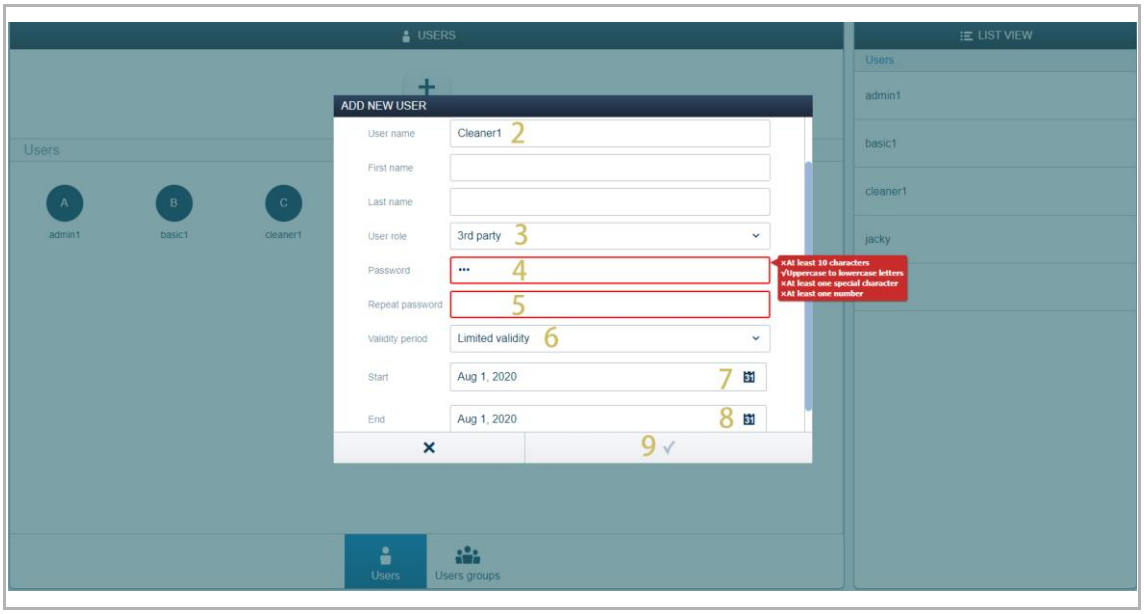
[6] Selecteer "Beperkte geldigheid" uit de keuzelijst.

[7] Stel de startdatum in de door op " 31 " te klikken.

[8] Stel de einddatum in de door op " 31 " te klikken.

[9] Klik op "OK" om te bewaren.

Herhaal de stappen 1-9 om gebruikers van derde aanbieders toe te voegen.



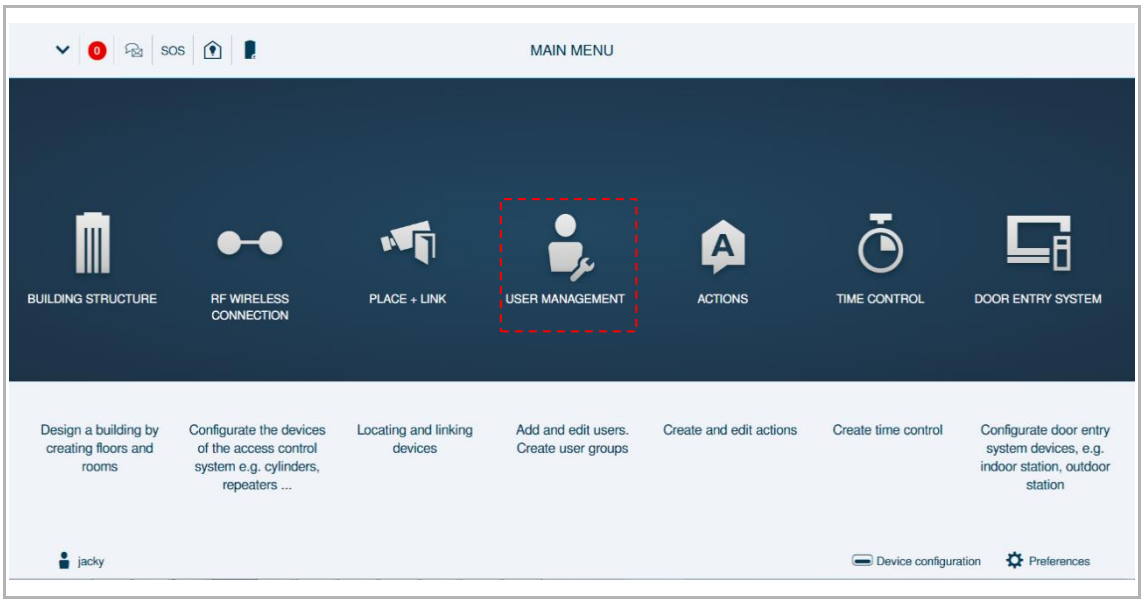
13.3.3 Gebruikersgroepen toevoegen

Opmerking

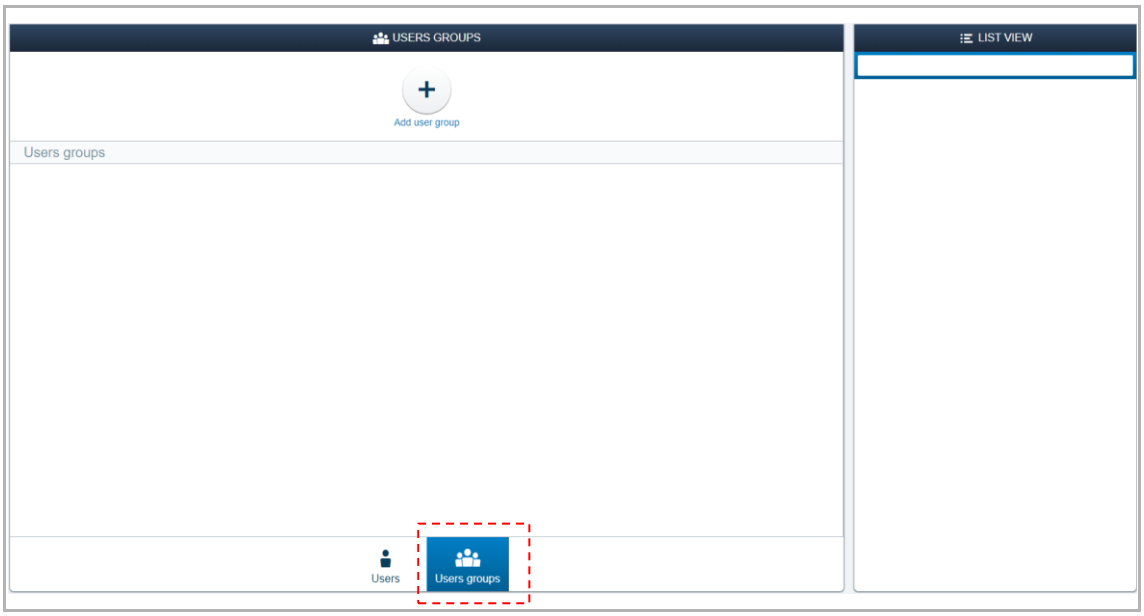
Gebruikersgroep is een verzameling van gebruikers. Alle gebruikers in de groep hebben dezelfde rechten voor de apparaten. Als er een wijziging in de rechten wordt aangebracht geldt deze voor alle gebruikers in de groep.

Het scherm "Gebruikersgroepen" oproepen

Klik in het configuratiescherm op "Gebruikersbeheer" om het scherm "Gebruikers" te openen.



Op het scherm "Gebruikers" klikt u op "Gebruikersgroepen" om toegang te krijgen tot het scherm "Gebruikersgroepen".



Gebruikersgroepen toevoegen

Volg de onderstaande stappen:

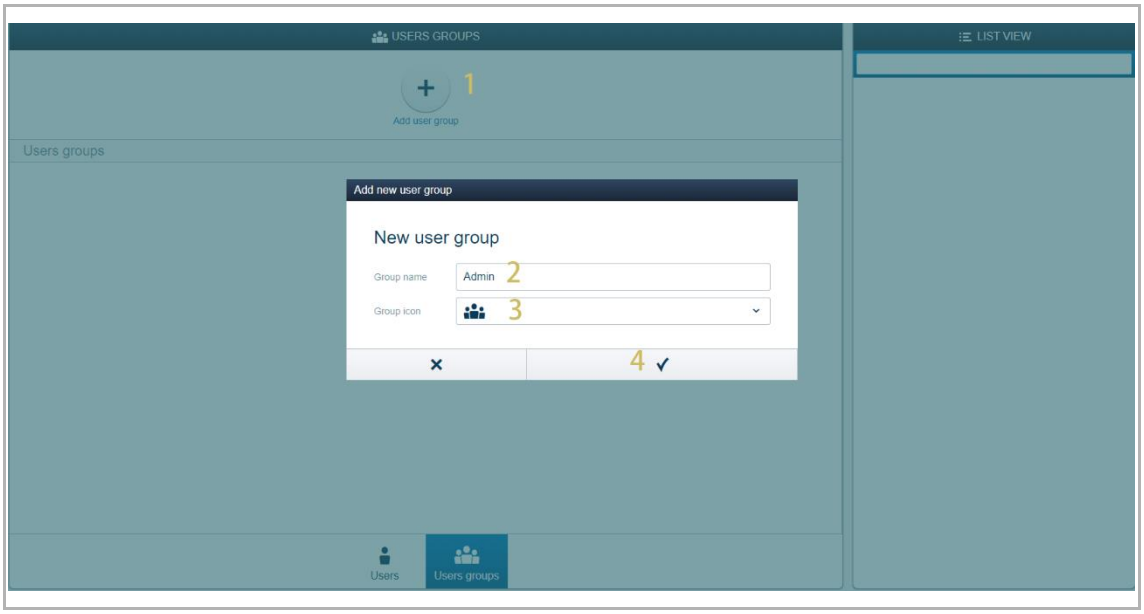
[1] Klik in de "Gebruikersgroepen" op "Gebruikersgroep toevoegen".

[2] Voer de naam van de groep in.

[3] Selecteer een groepssymbool uit de keuzelijst.

[4] Klik op "√" om op te slaan.

Herhaal de stappen van 1-4 om gebruikersgroepen toe te voegen.

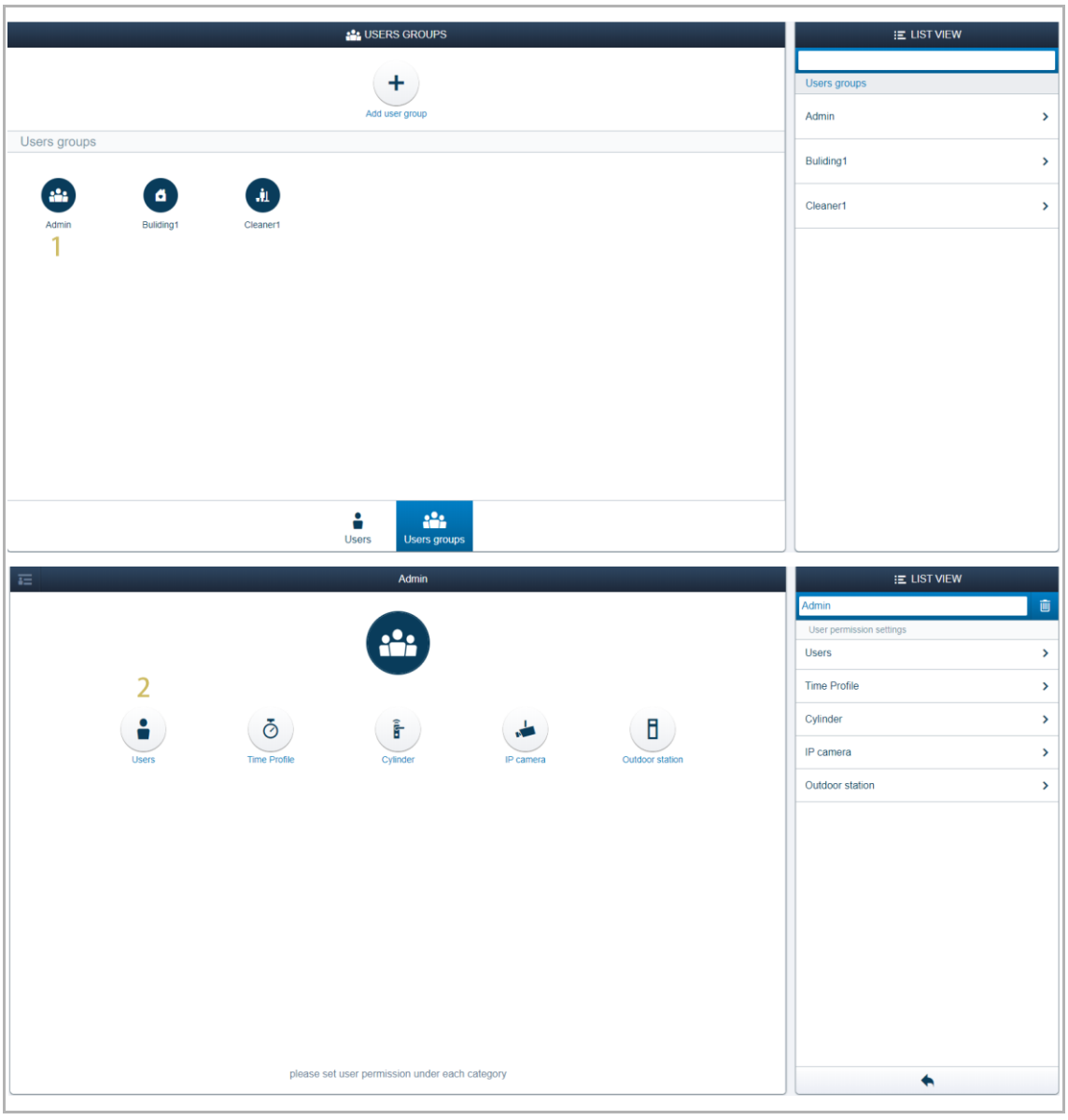


13.3.4 Gebruikers toewijzen aan een gebruikersgroep

Volg de onderstaande stappen:

[1] Klik in het scherm van de "Gebruikersgroepen" op een gebruikersgroep.

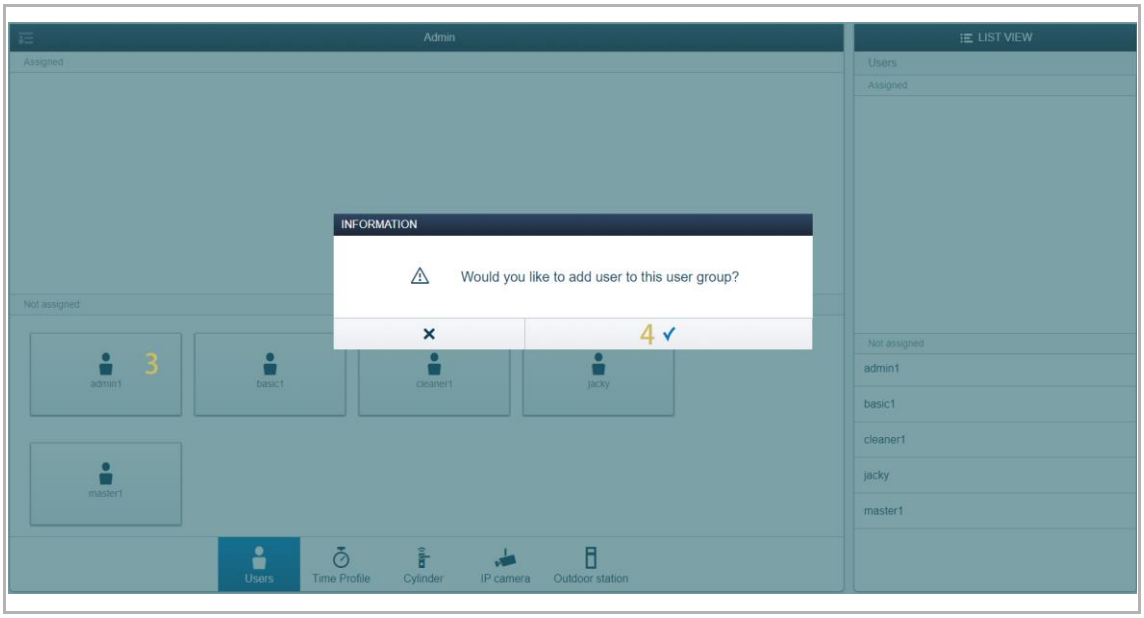
[2] Klik op "Gebruikers".



[3] Klik in het scherm van de betreffende gebruikersgroep op de gebruiker gebruiker in de sectie "Niet toegewezen".

[4] Klik op "√" om te bevestigen.

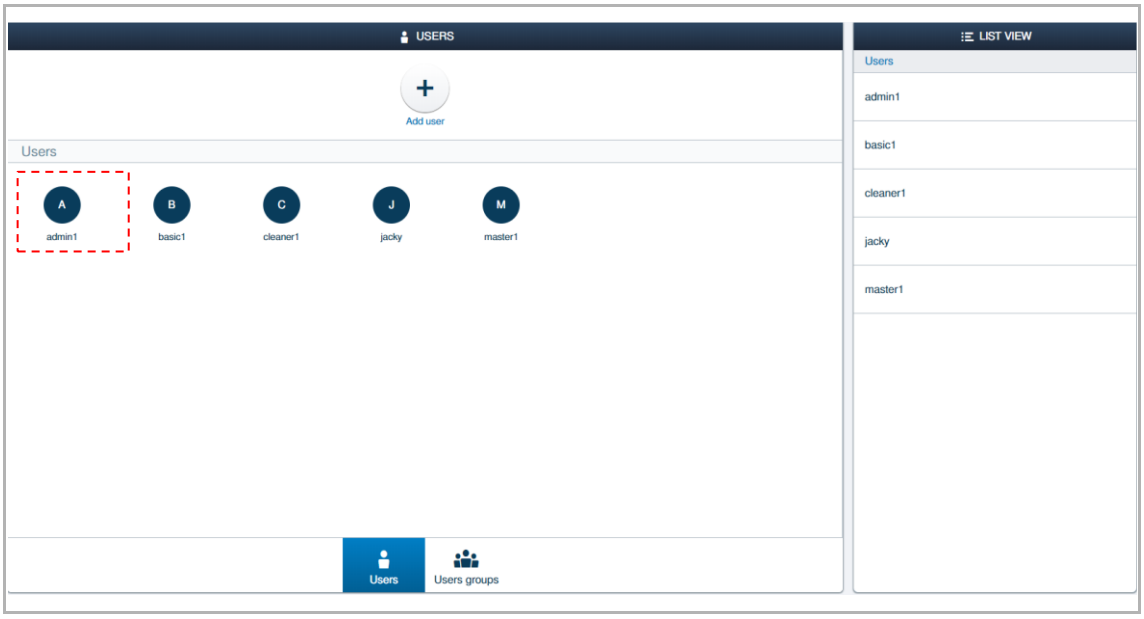
Herhaal de stappen 3-4 om de betreffende gebruikers aan een gebruikersgroep toe te wijzen.



13.3.5 Gebruiker configureren

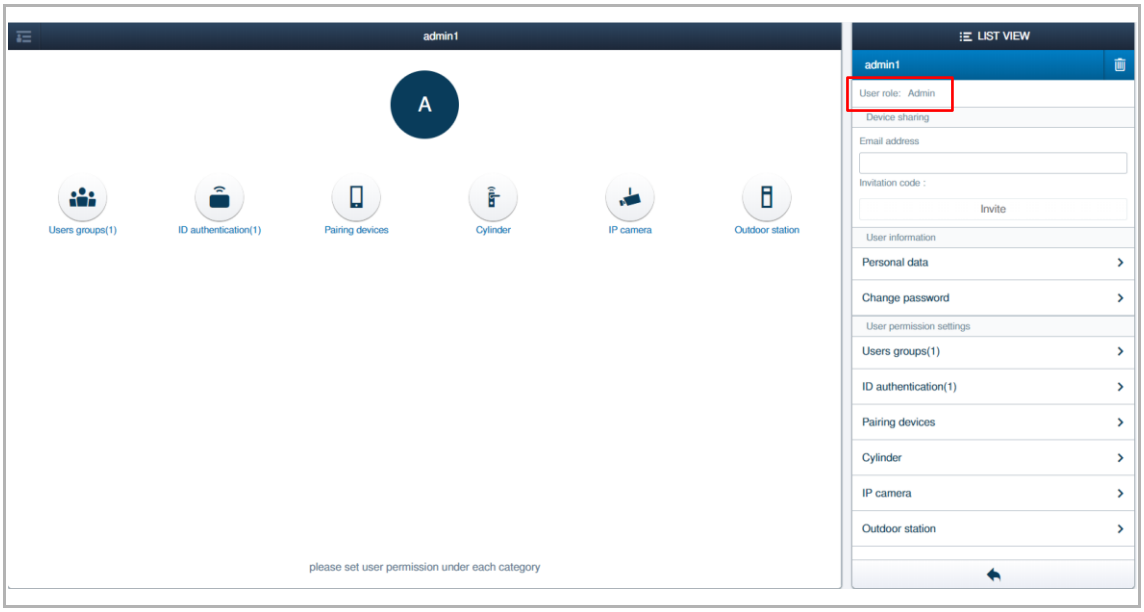
Het gebruikersscherm oproepen

Op het scherm "Gebruikers" klikt u op de gebruiker om toegang te krijgen tot het scherm van de gebruiker.



1. Bekijk de gebruikersrol

De gebruikersrol is vermeldt op het betreffende gebruikersscherm.



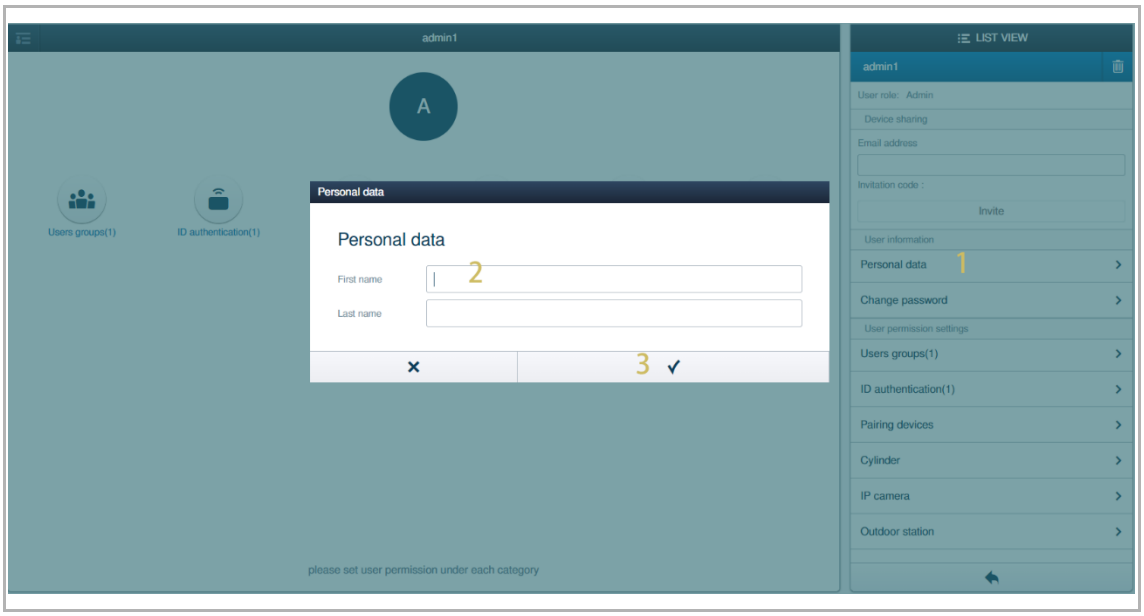
2. Gebruikersnaam wijzigen

Op het betreffende gebruikersscherm, volgt u de onderstaande stappen:

[1] Klik op "Gebruikersaccount bewerken".

[2] Voer de voornaam en de achternaam in.

[3] Klik op "√" om op te slaan.



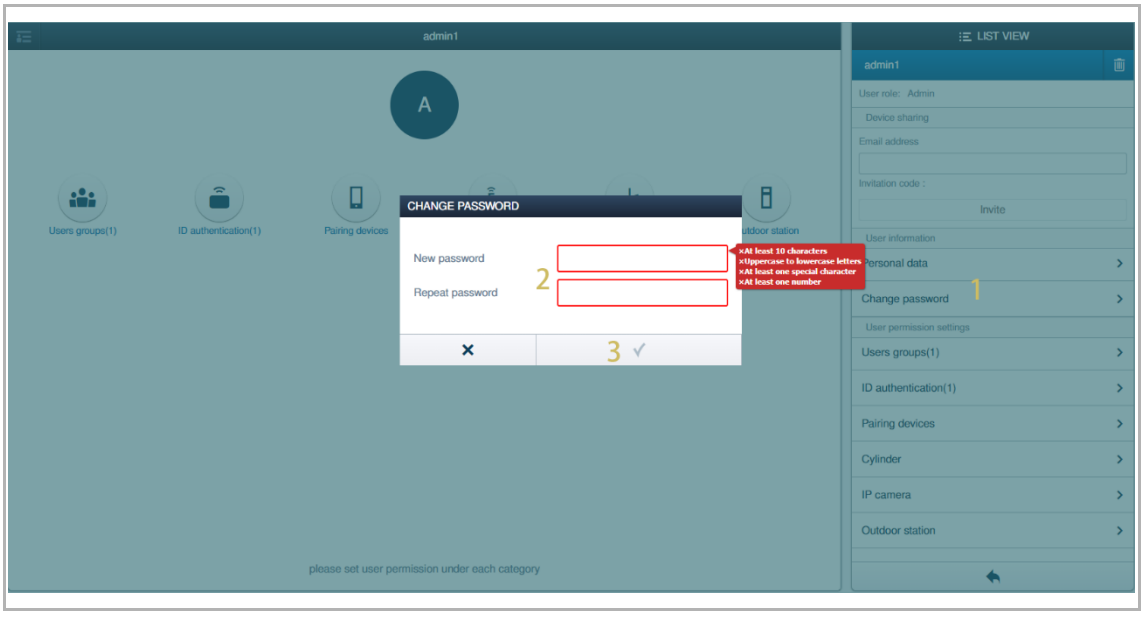
3. Wachtwoord wijzigen

Op het betreffende gebruikersscherm, volgt u de onderstaande stappen:

[1] Klik op "Wachtwoord wijzigen".

[2] Voer het wachtwoord volgens de op het scherm weergegeven regel twee keer in.

[3] Klik op "√" om op te slaan.



4. Geldigheidsperiode wijzigen

Opmerking
Dit is uitsluitend van toepassing op gebruikers van een derde aanbieder.

Op het betreffende gebruikersscherm, volgt u de onderstaande stappen:

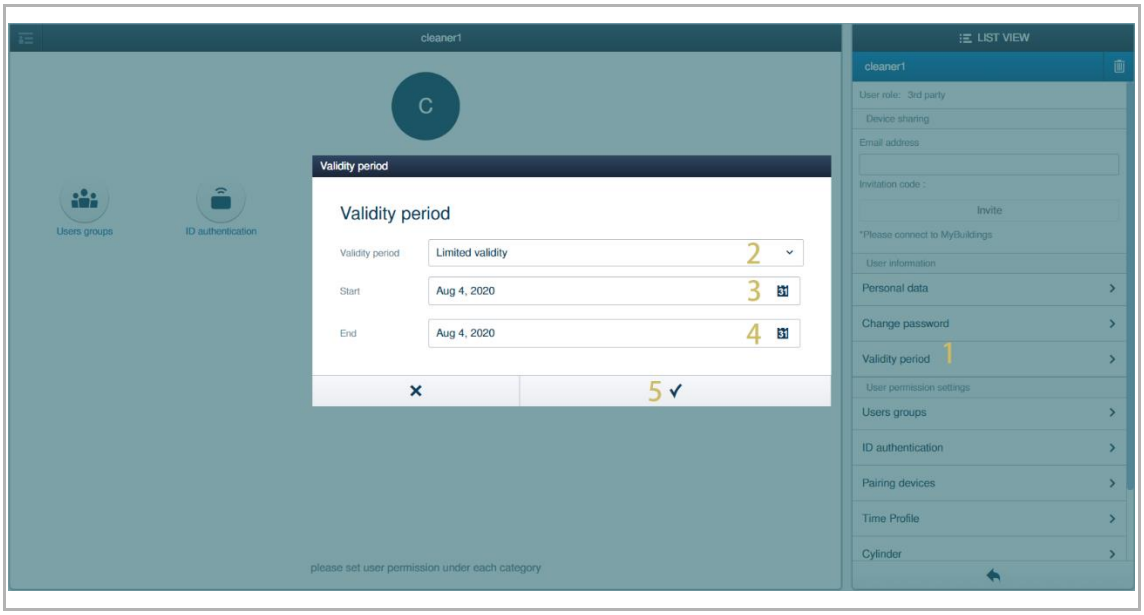
[1] Klik op "Geldigheidsperiode".

[2] Selecteer "Beperkte geldigheid" uit de keuzelijst.

[3] Stel de startdatum in de door op " " te klikken.

[4] Stel de einddatum in de door op " " te klikken.

[5] Klik op "OK" om te bewaren.

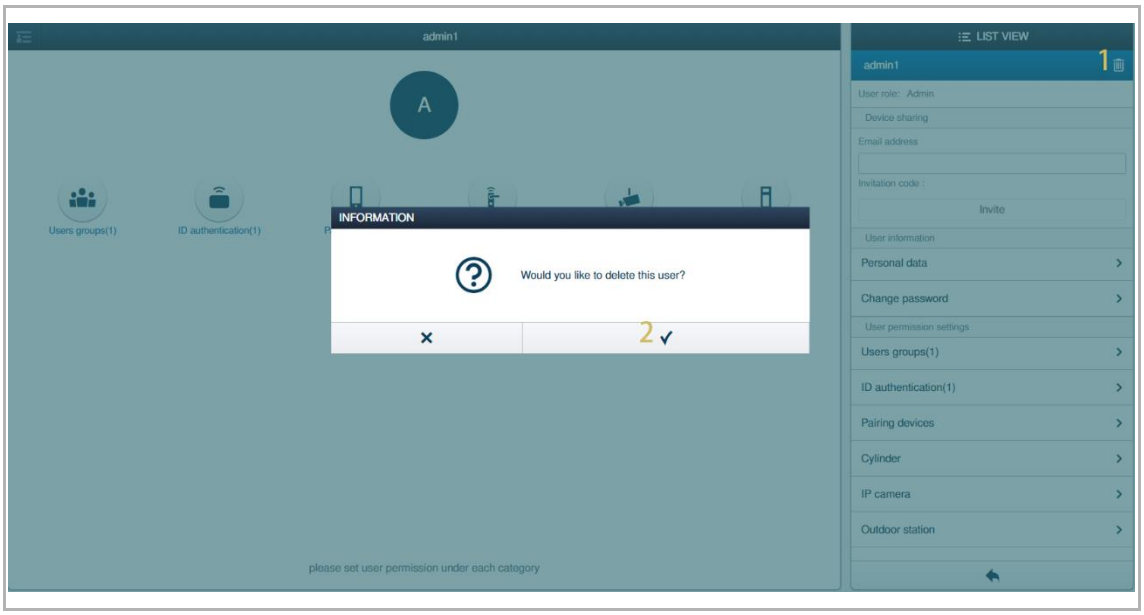


5. Gebruiker verwijderen

Op het betreffende gebruikersscherm, volgt u de onderstaande stappen:

[1] Klik op " ".

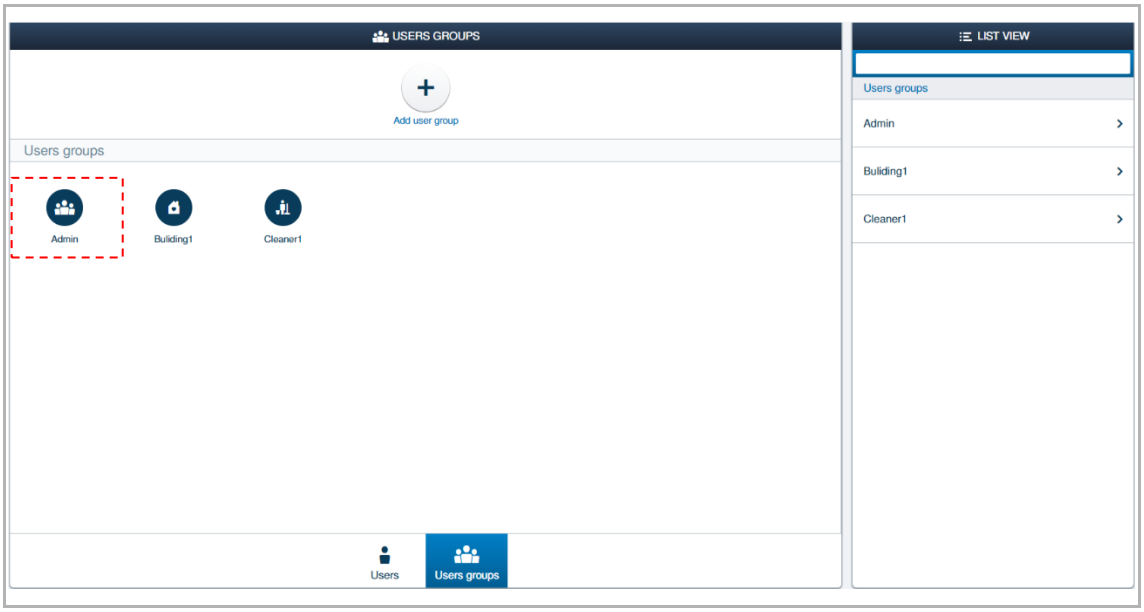
[2] Klik op "√" om op te slaan.



13.3.6 Gebruikersgroep configureren

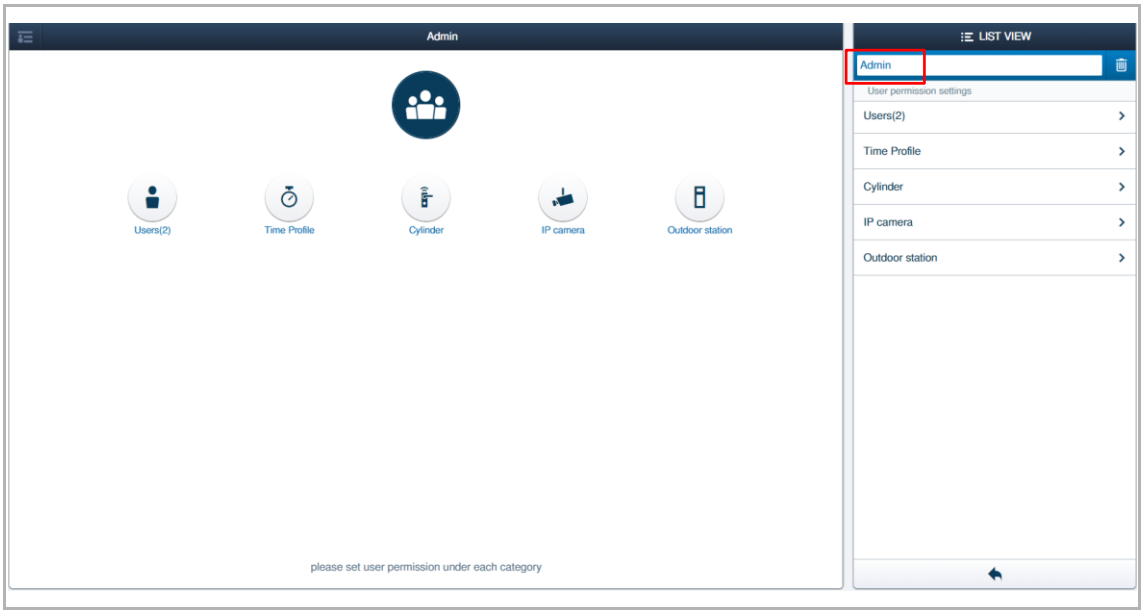
Het groepsscherm oproepen

Op het scherm "Gebruikersgroepen" klikt u op de groep om toegang te krijgen tot het scherm van de groep.



1. Groepsnaam wijzigen

Op het betreffende gebruikersgroep-scherm op de groepsnaam klikken en een nieuwe naam invoeren.



13.4 Firmware updaten

13.4.1 Firmware updaten voor "Smart Access Point"

1. Firmware updaten via lokale pc

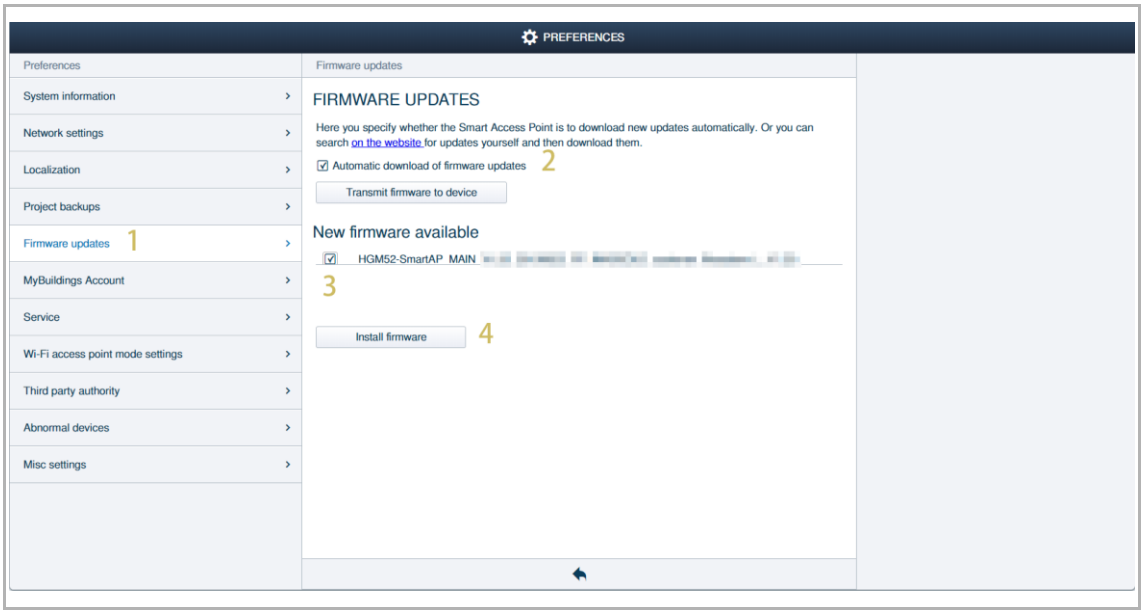
Volg de onderstaande stappen:

[1] Op het scherm "Instellingen" klikt u op "Firmware-updates".

[2] Vink het keuzevakje "Automatisch downloaden van de firmware-update" aan. "Smart Access Point" zal de nieuwste firmware automatisch downloaden van de website.

[3] De laatste firmwareversie wordt hier weergegeven. Vink het daarvoor juiste keuzevakje aan.

[4] Klik op "Firmware installeren".



Opmerking

"Smart Access Point" kan alleen geüpdatet worden naar nieuwere firmware.

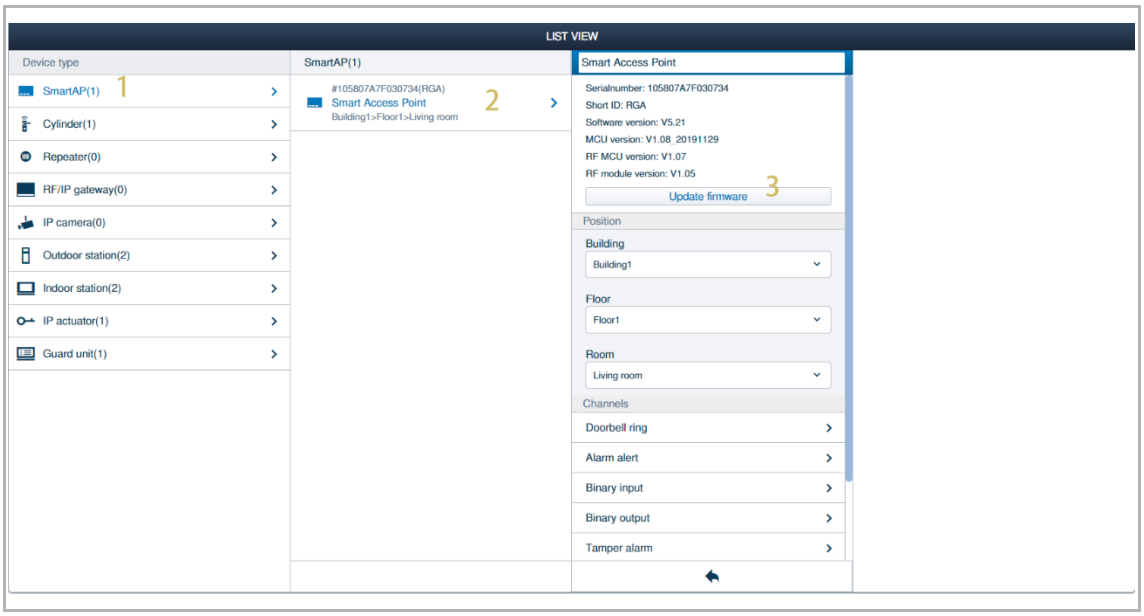
2. Firmware updaten via de website

Volg de onderstaande stappen:

[1] Klik in het scherm "Apparaatconfiguratie" op "SmartAP".

[2] Klik op "Smart Access Point".

[3] Klik op "Firmware-updates".



Opmerking

"Smart Access Point" kan alleen geüpdatet worden naar nieuwere firmware.

13.4.2 Firmware updaten voor buiten-/binnenpost

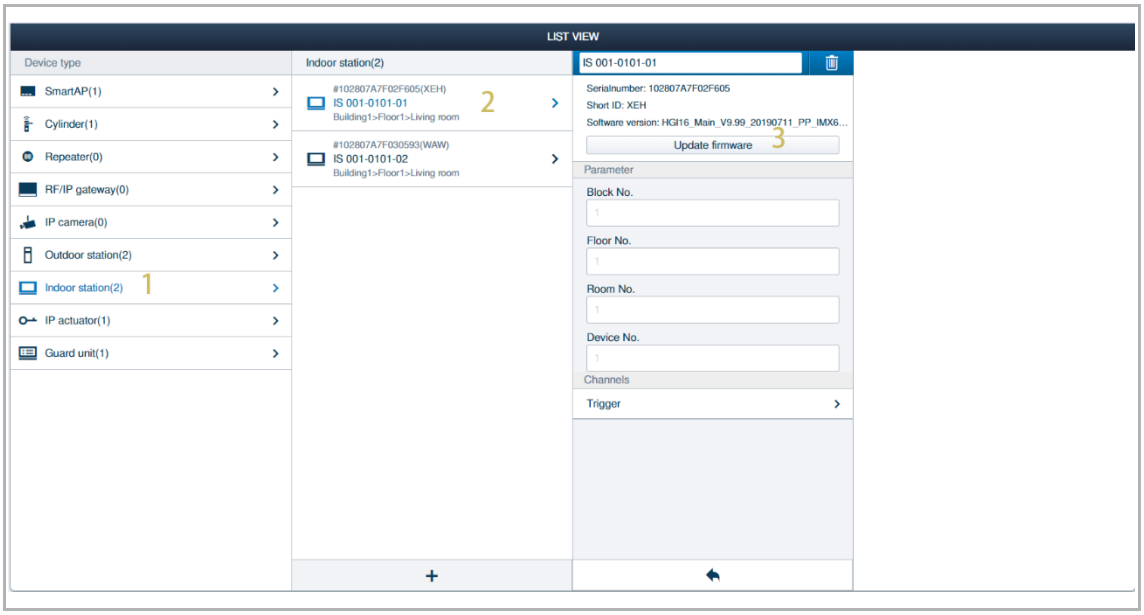
1. Apparaten een voor een updaten

Volg de onderstaande stappen:

[1] Klik in het scherm "Apparaatconfiguratie" klikt u op buiten-/binnenpost (bijv. "Binnenpost").

[2] Klik op de betreffende buiten-/binnenpost (bijvoorbeeld "Binnenpost 001").

[3] Klik op "Firmware-updates".



2. Updaten van dezelfde soorten apparaten in batch

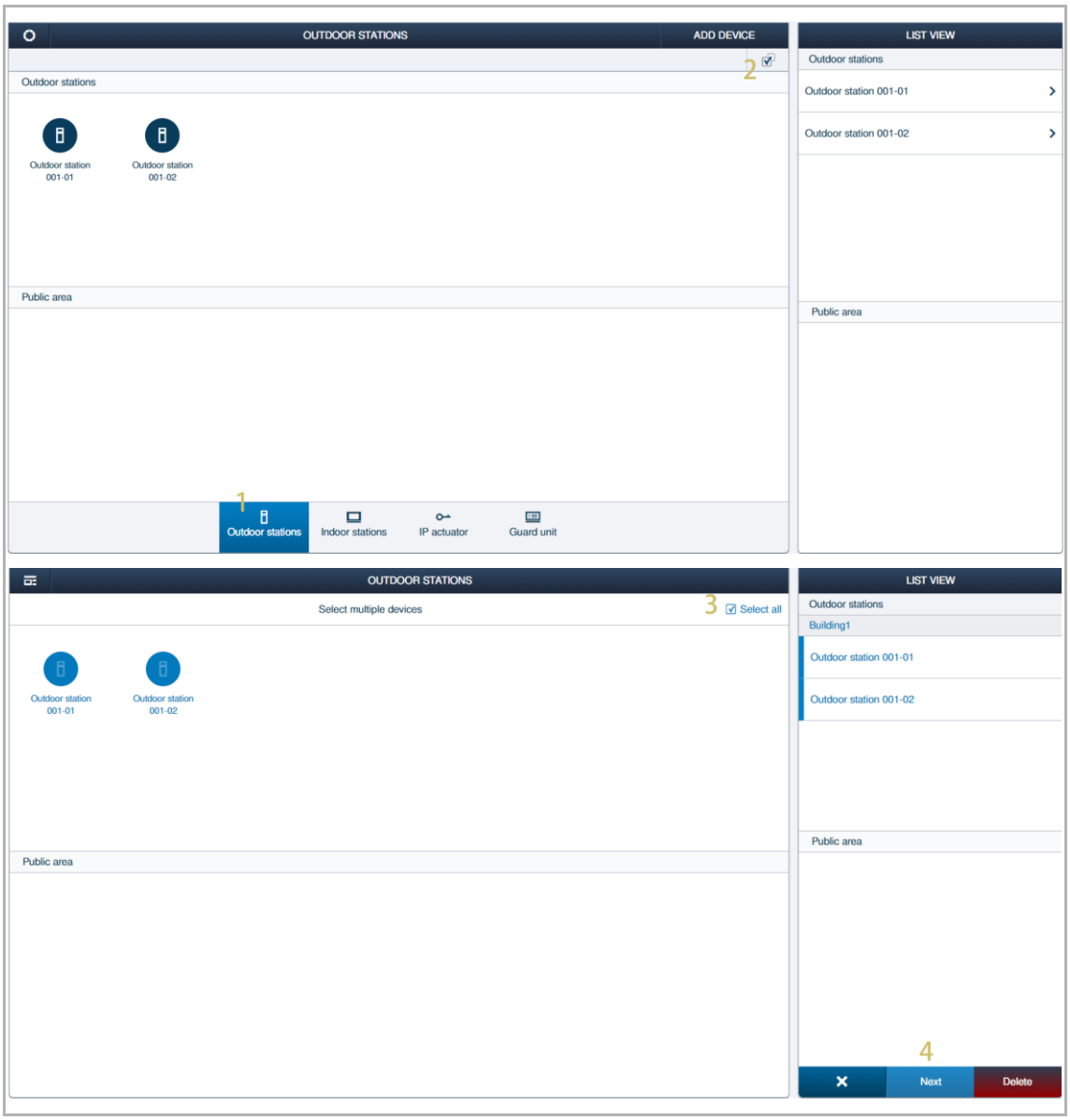
Volg de onderstaande stappen:

[1] Klik in het scherm "Apparaatconfiguratie" klikt u op buiten-/binnenpost (bijv. "Buitenpost").

[2] Klik op " ".

[3] Klik op "Alles selecteren" om alle apparaten te selecteren of klik één voor één op het betreffende apparaat om meerdere apparaten te selecteren.

[4] Klik op Volgende".

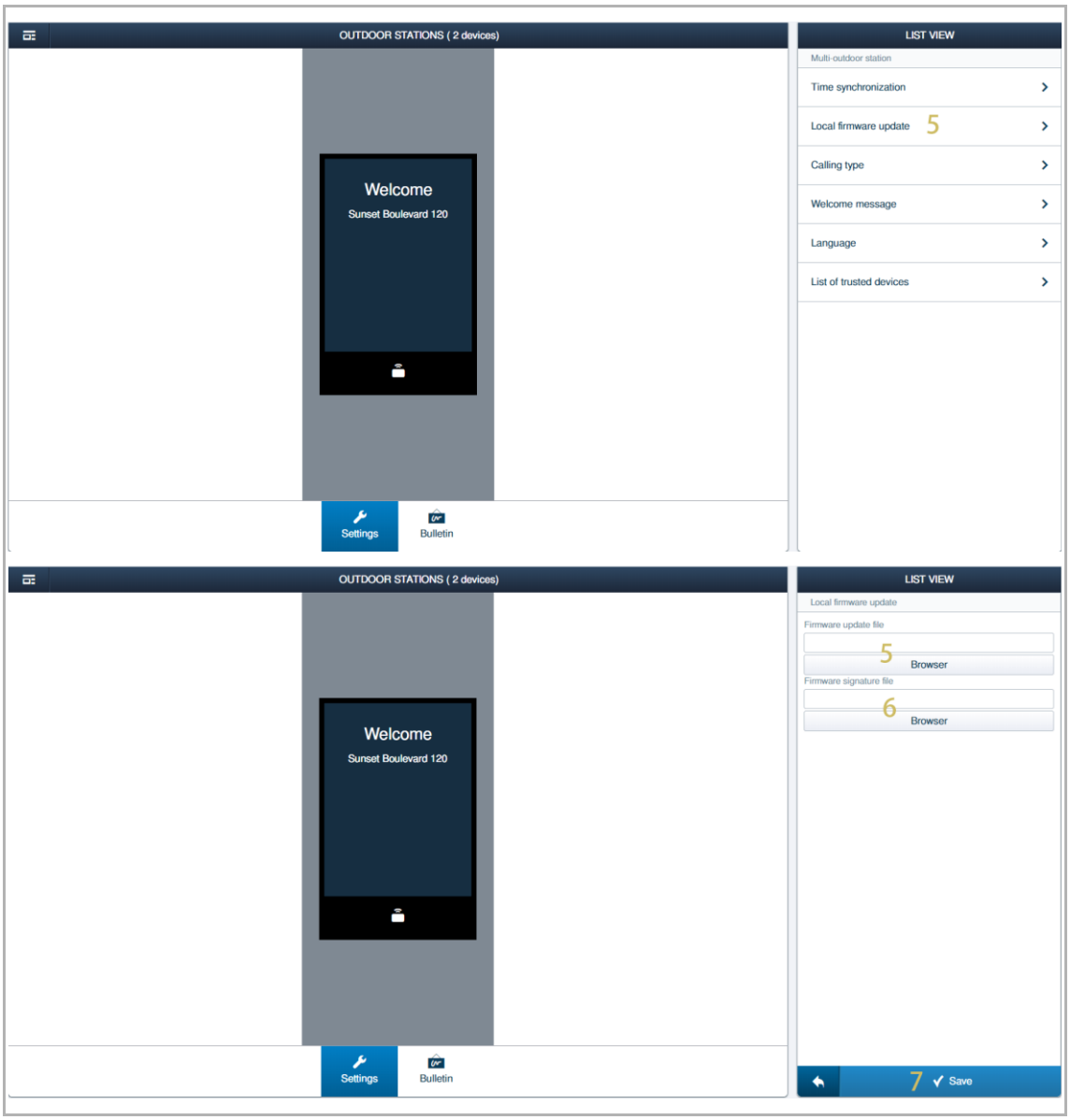


[5] Klik op "Lokale firmware-update".

[6] Upload de firmware.

[7] Upload de handtekening.

[8] Klik op "√" om op te slaan.



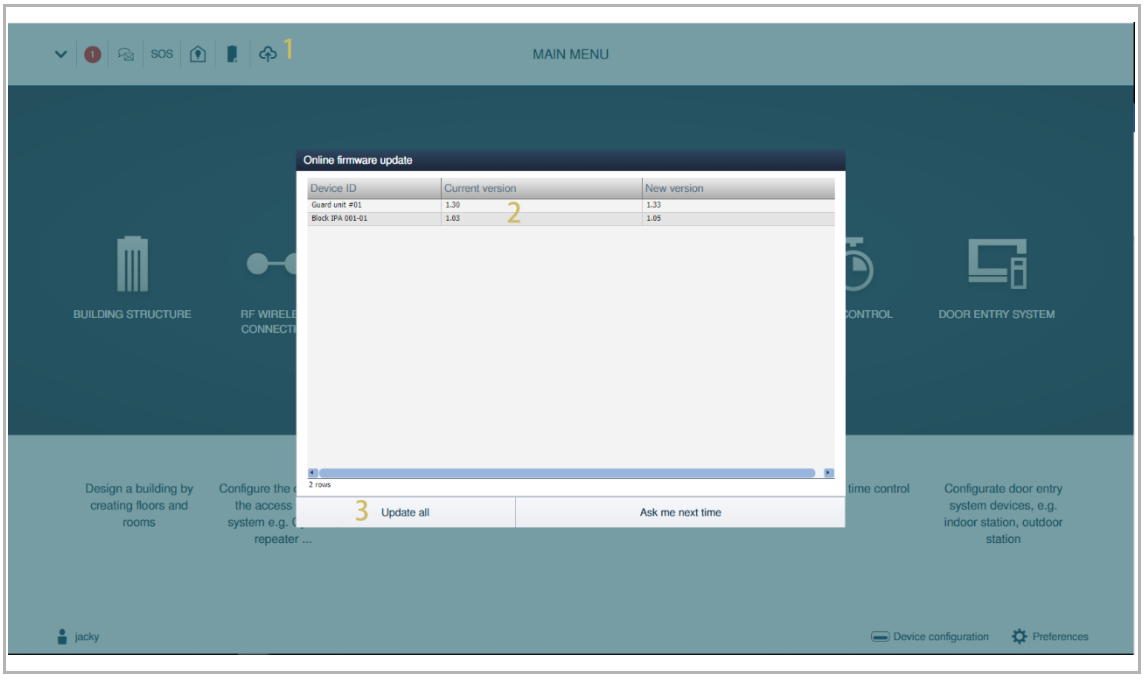
3. Het updaten van de verschillende soorten apparaten in batches

Volg de onderstaande stappen:

[1] Klik in het configuratiescherm op "".

[2] De te updaten apparaten worden op het scherm weergegeven.

[3] Klik op "Alles updaten" om alle apparaten in batches te updaten.



Opmerking

Alleen de buiten/binnenposten die in een openbaar bereik zijn geplaatst (bijv. portiercentrale, gebouw-IPA, netwerk-IPA etc.) kunnen via deze methode worden geüpdatet.

13.4.3 Firmware updaten voor AccessControl-apparaten

1. Firmware updaten via lokale pc

Volg de onderstaande stappen:

[1] Klik in het scherm "Apparaatconfiguratie" op een AccessControl-apparaat (bijv. "Cilinder").

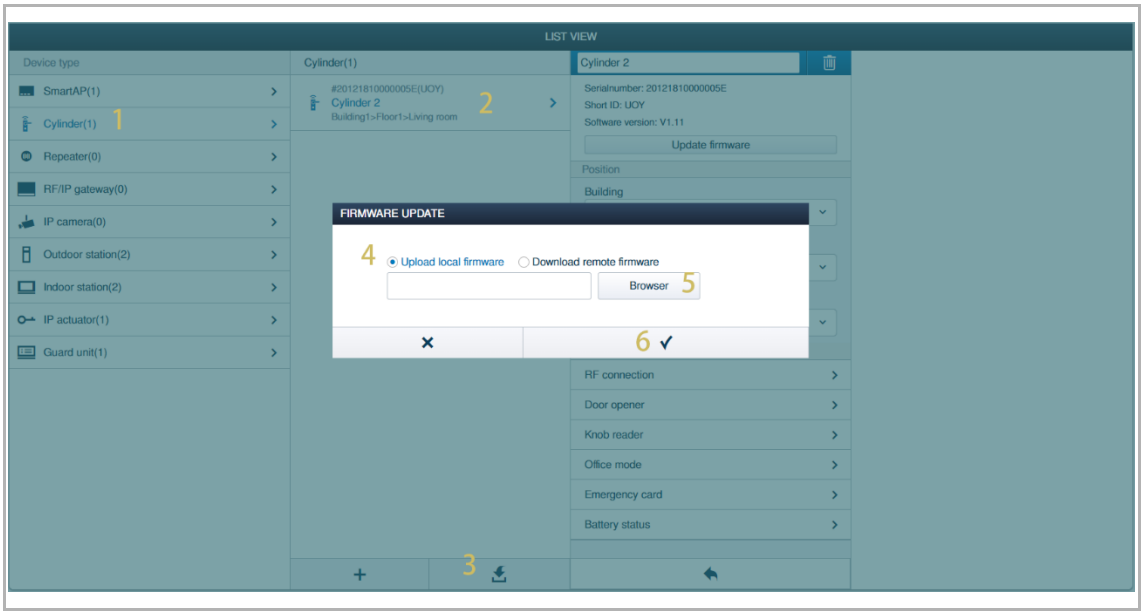
[2] Klik op het AccessControl-apparaat (bijv. "Cilinder2").

[3] Klik op " ".

[4] Klik op "Lokale firmware uploaden".

[5] Blader door uw pc om de firmware te selecteren.

[6] Klik op "√".



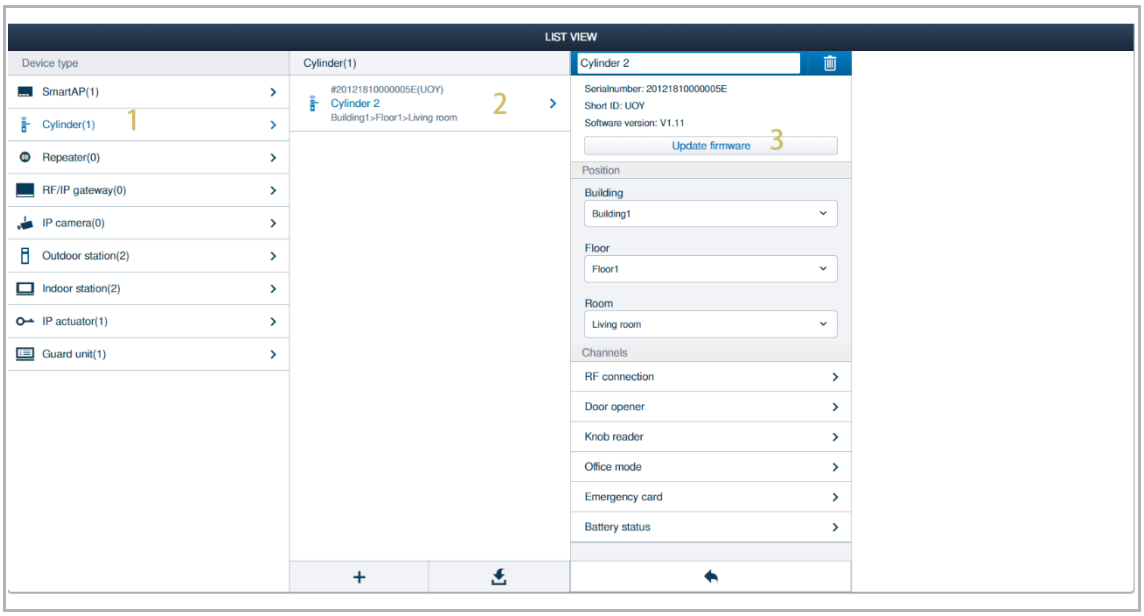
2. Firmware updaten via de website

Volg de onderstaande stappen:

[1] Klik in het scherm "Apparaatconfiguratie" op een AccessControl-apparaat (bijv. "Cilinder").

[2] Klik op het AccessControl-apparaat (bijv. "Cilinder2").

[3] Klik op "Firmware-updates".



13.5 Back-up beheren

Overzicht back-up

De volgende informatie wordt opgeslagen in de back-up:

- Apparaatinstellingen, gebruikersinstellingen, gebouwstructuur, plaats + link, bericht en logboeken.
- RF-verbindingen van de AccessControl-apparaten.
- RF-verbindingen van "RF/IP-gateways".
- Certificaten.

Let op!

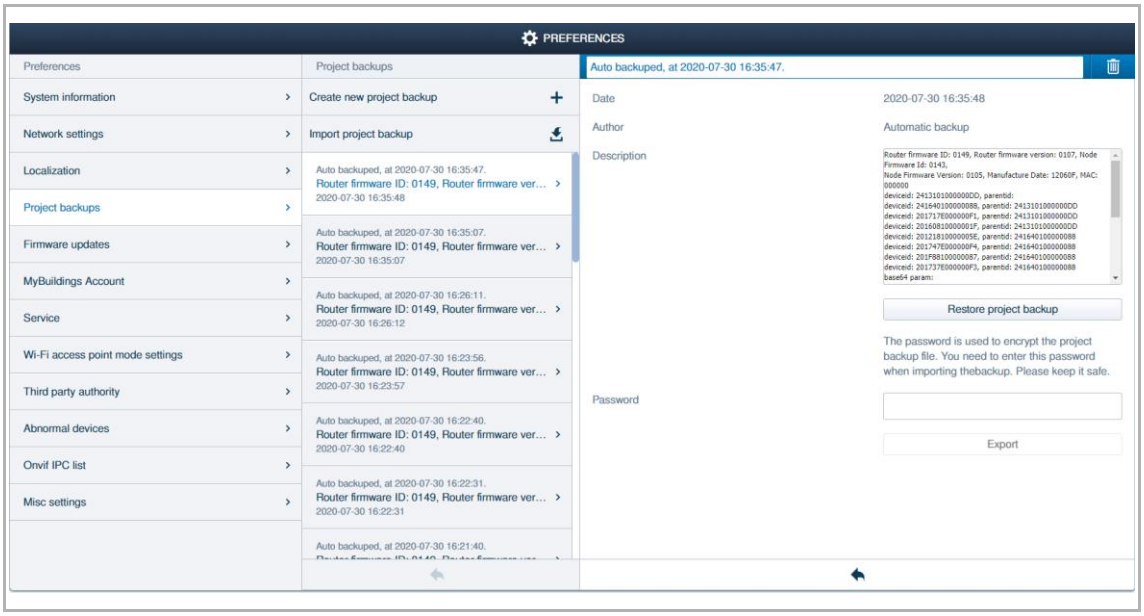
Een projectback-up is belangrijk en noodzakelijk voor de AccessControl-apparaten.

Als er vooraf geen back-up wordt gemaakt, zijn alle AccessControl-apparaten ongeldig wanneer het huidige "Smart Access Point" defect raakt. Deze AccessControl-apparaten kunnen zonder back-up niet direct door een nieuw "Smart Access Point" worden gebruikt. U moet deze apparaten terugsturen naar de fabriek om ze te laten repareren.

Back-upscherm oproepen

Klik in het configuratiescherm op "Instellingen", gevolgd door "Back-up" om toegang te krijgen tot het back-upscherm.

Er worden een aantal automatisch opgeslagen back-ups weergegeven in de lijst.



13.5.1 Back-up maken

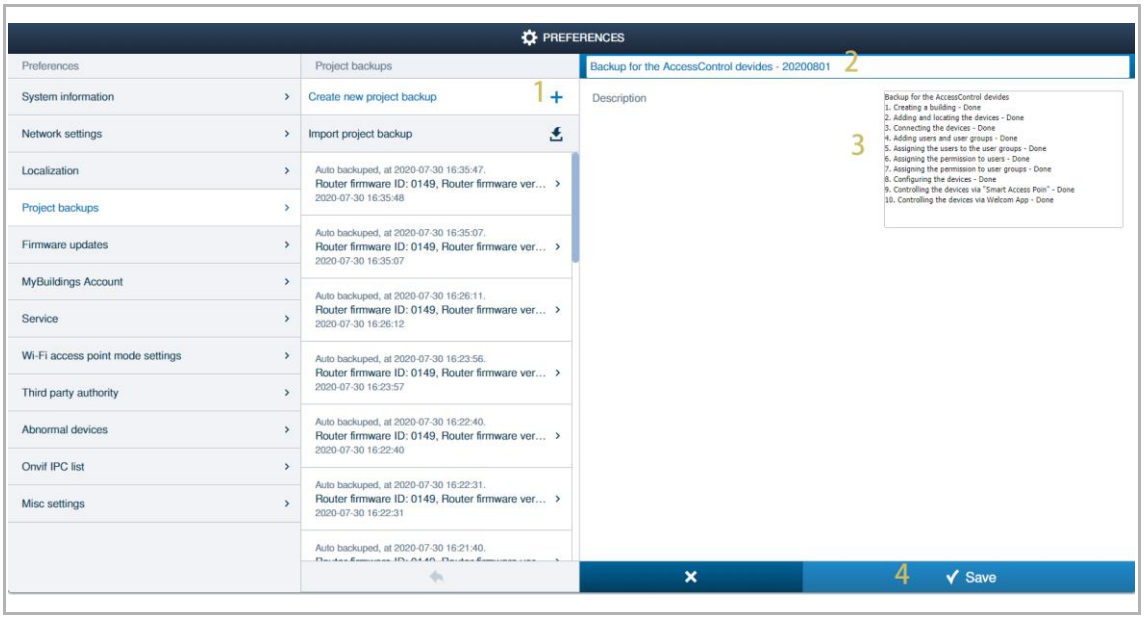
Volg de onderstaande stappen om een back-up te maken en deze op te slaan op het huidige "Smart Access Point":

[1] Op het back-upscherm klikt u op "+".

[2]E Voer de naam in.

[3] Voer de beschrijving in.

[4] Klik op "√" om op te slaan.



Let op!

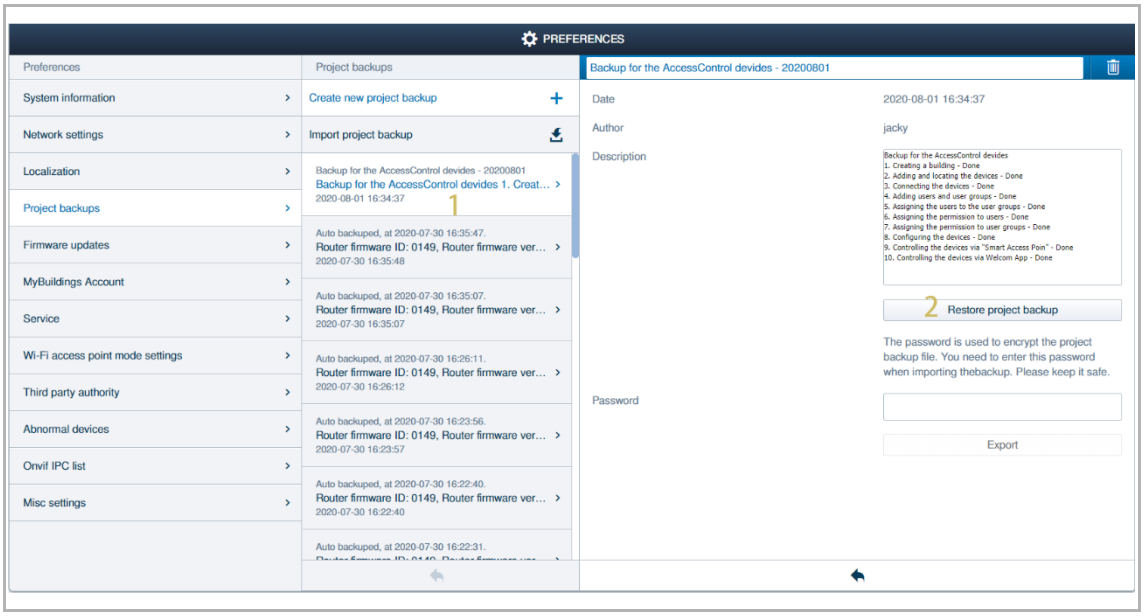
De back-up wordt opgeslagen in het huidige "Smart Access Point". Aanbevolen wordt om de back-up te exporteren naar de pc voor het geval dat het huidige "Smart Access Point" defect raakt.

13.5.2 Back-up herstellen

Volg de onderstaande stappen om een back-up te herstellen vanaf het huidige "Smart Access Point":

[1] Klik op het back-upscherm op de betreffende back-up.

[2] Klik op "Projectback-up herstellen".



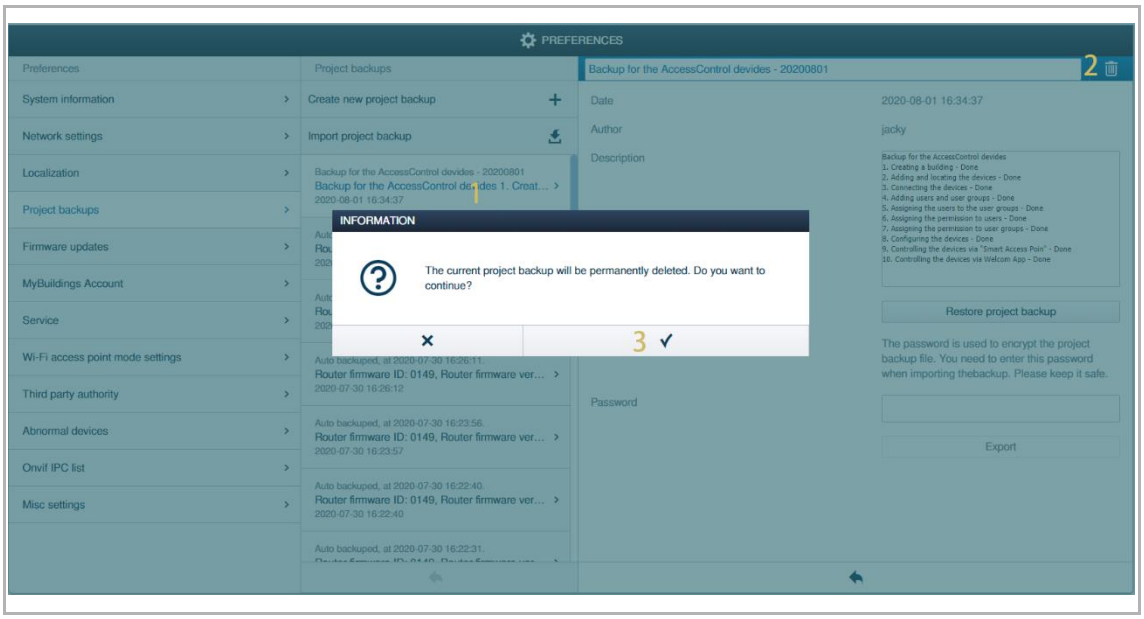
13.5.3 Back-up verwijderen

Volg de onderstaande stappen om een back-up te verwijderen van het huidige "Smart Access Point":

[1] Klik op het back-upscherm op de betreffende back-up.

[2] Klik op " ".

[3] Klik op "√" om te bevestigen.



13.5.4 Back-up naar pc exporteren

Volg de onderstaande stappen om een back-up te exporteren van het huidige "Smart Access Point" naar een pc:

[1] Klik op het back-upscherm op de betreffende back-up.

[2] Voer een herstelwachtwoord volgens de op het scherm weergegeven regel in. Het herstelwachtwoord wordt gebruikt om de back-up vanaf de pc te importeren.

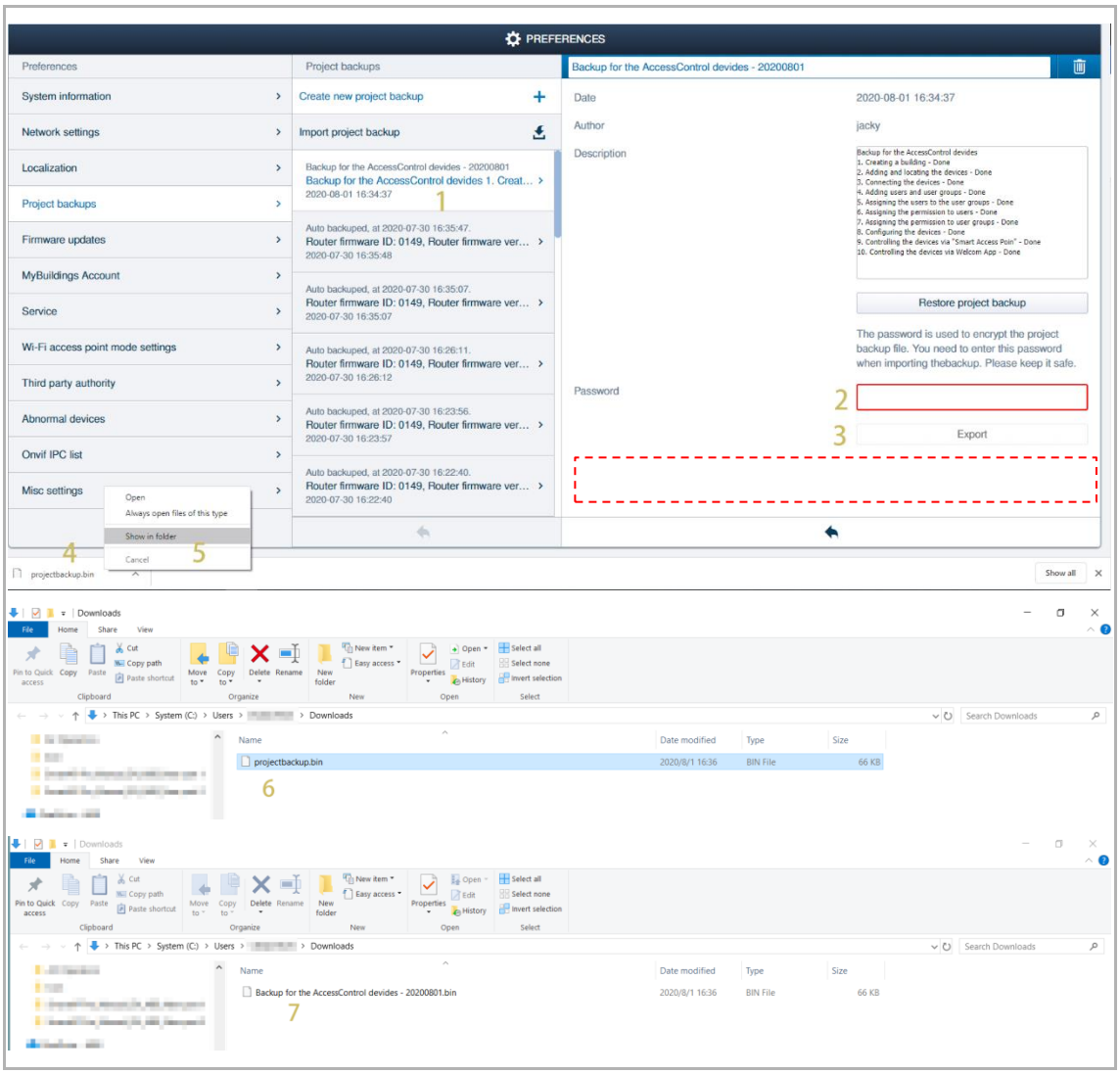
[3] Klik op "Exporteren" om de back-up naar de pc te exporteren.

[4] Rechtsklik op het back-upbestand.

[5] Klik op "In map weergeven".

[6] De back-up wordt weergegeven in de map.

[7] Geef de back-up een andere naam.



13.5.5 Back-up vanaf de pc importeren

Volg de onderstaande stappen om de back-up vanaf de pc te importeren.

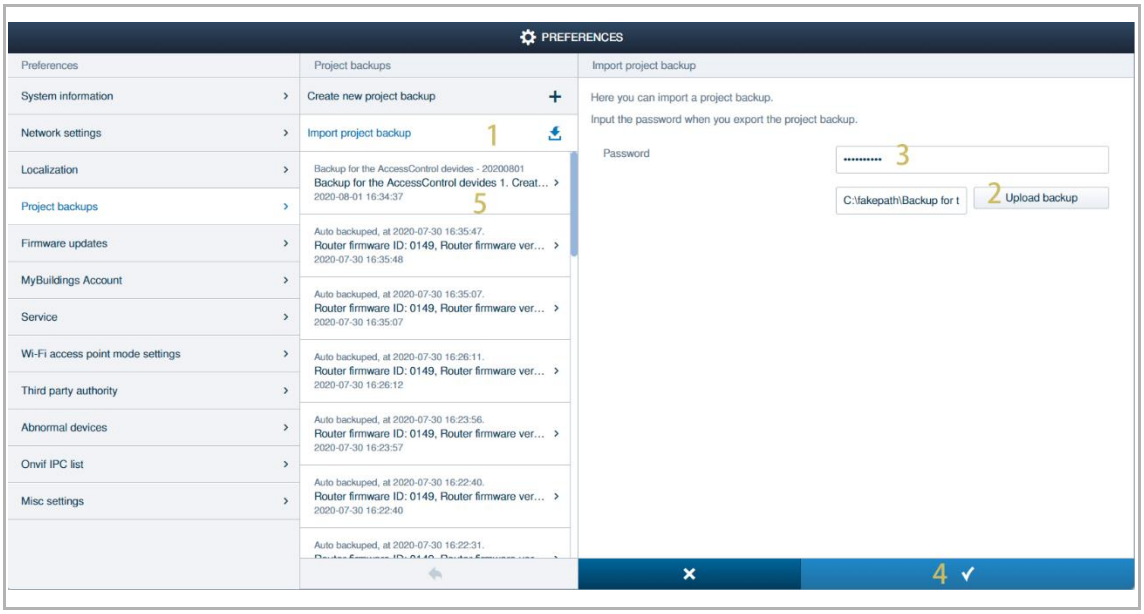
[1] Op het back-upscherm klikt u op " ".

[2] Klik op "Projectback-up uploaden" en selecteer de back-up van uw pc.

[3] Voer het herstelwachtwoord in. zie hoofdstuk 13.5.4 “Back-up naar pc exporteren“ op pagina 284

[4] Klik op "√".

[5] De back-up wordt weergegeven in de lijst.



Opmerking

U moet het "Herstel van een back-up" voortzetten om het geïmporteerde bestand in werking te laten treden. zie hoofdstuk 13.5.2 “Back-up herstellen“ op pagina 282.

13.6 Voorinstellingen herstellen

13.6.1 AccessControl-apparaten herstellen

Als u alle AccessControl-apparaten wilt resetten, kunt u het gebouw resetten.

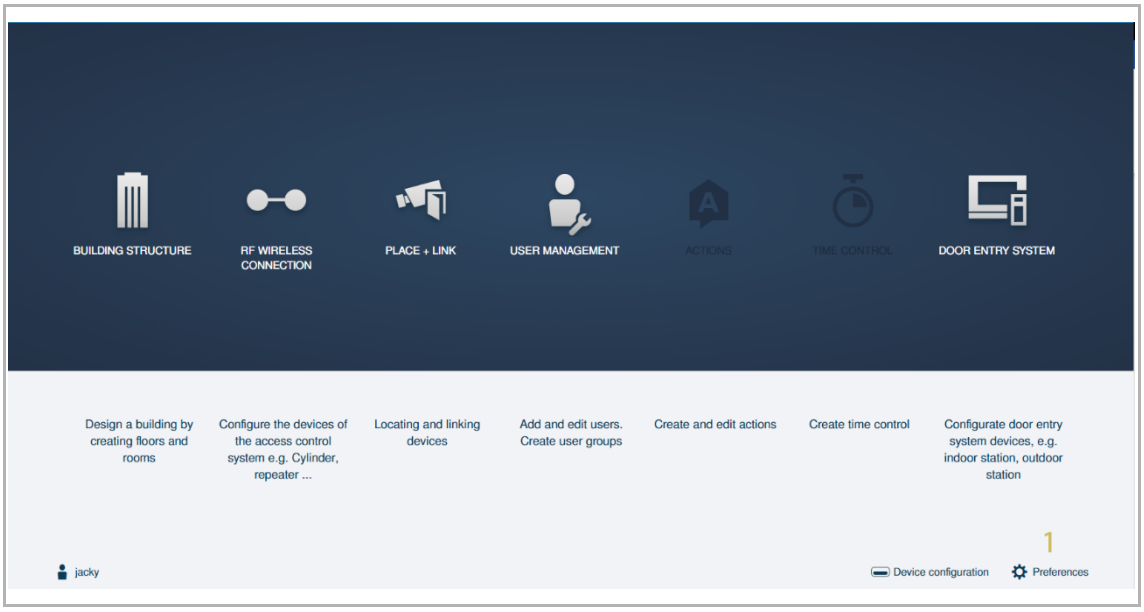
Let op!

U moet een back-up maken voor de AccessControl-apparaten voordat u het gebouw reset. zie hoofdstuk 13.5.1 “Back-up maken“ op pagina 281.

U moet alle AccessControl-apparaten loskoppelen voordat u het gebouw reset. zie hoofdstuk 10.11 “Apparaten loskoppelen“ op pagina 215.

Volg de onderstaande stappen:

[1] Klik in het configuratiescherm op "Instellingen" om het bijbehorende scherm te openen.



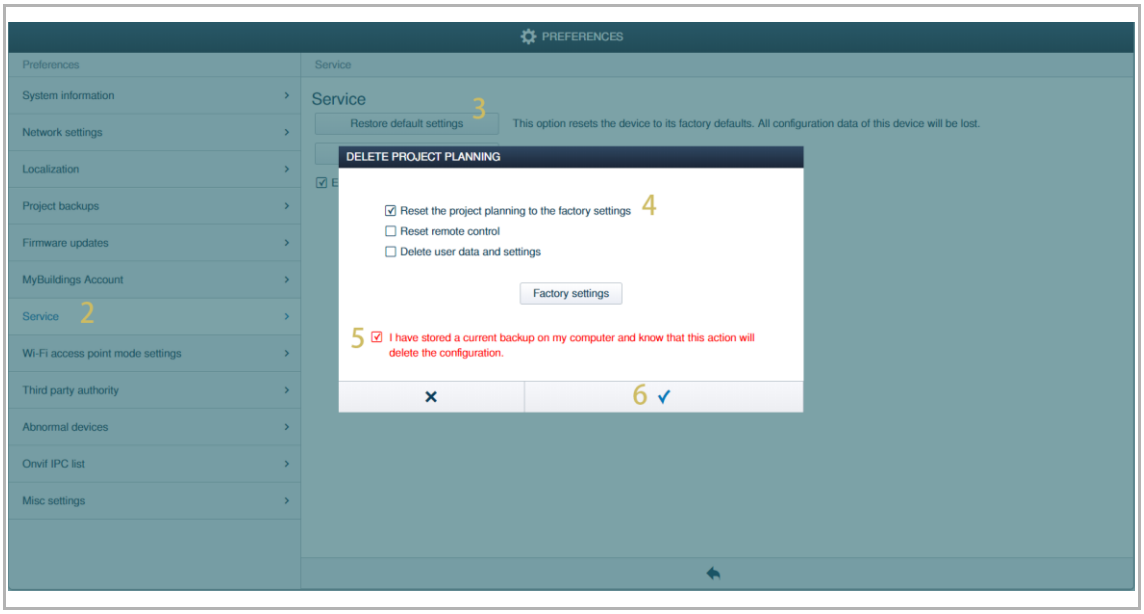
[2] Op het scherm "Instellingen" klikt u op "Service".

[3] Klik op "Voorinstellingen herstellen".

[4] Vink het keuzevakje "Projectplanning naar fabrieksinstellingen resetten" aan.

[5] Vink het keuzevakje "Ik heb opgeslagen …" aan.

[6] Klik op "√" om te bevestigen.



13.6.2 Toegang tot het "Smart Access Point" op afstand

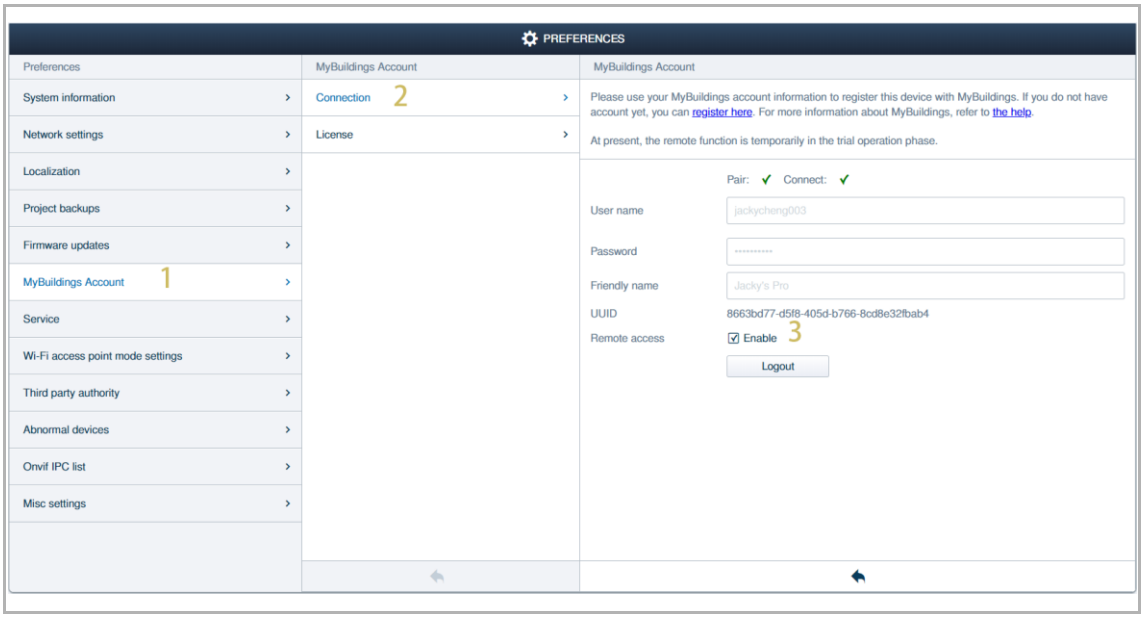
1. Functie "Toegang op afstand" activeren

Volg de onderstaande stappen:

[1] Op het scherm "Instellingen" klikt u op "MyBuildings-account".

[2] Klik op "Connection".

[3] Vink het keuzevakje "Toegang op afstand" aan.

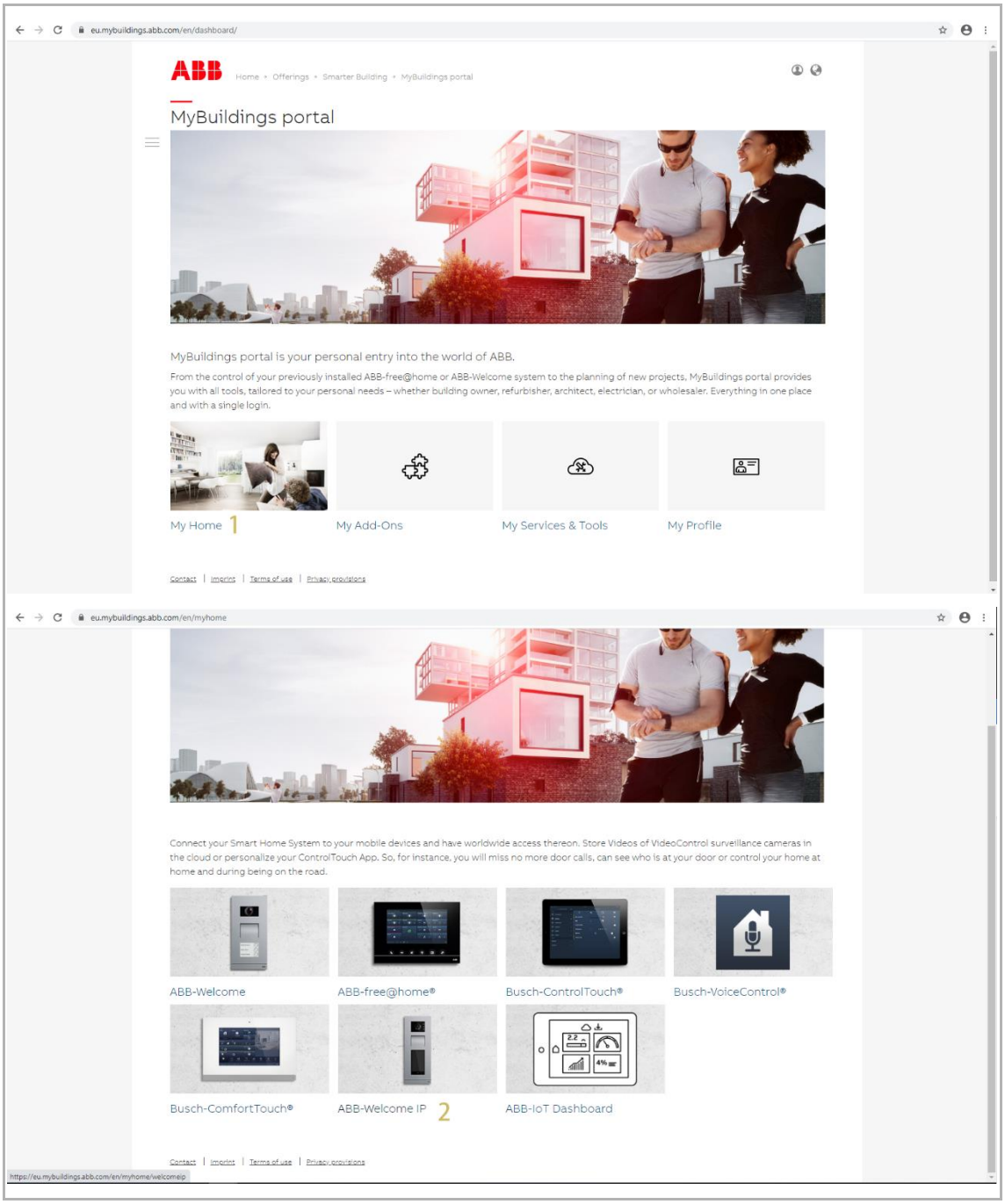


2. "Smart Access Point" in MyBuildings-portaal openen

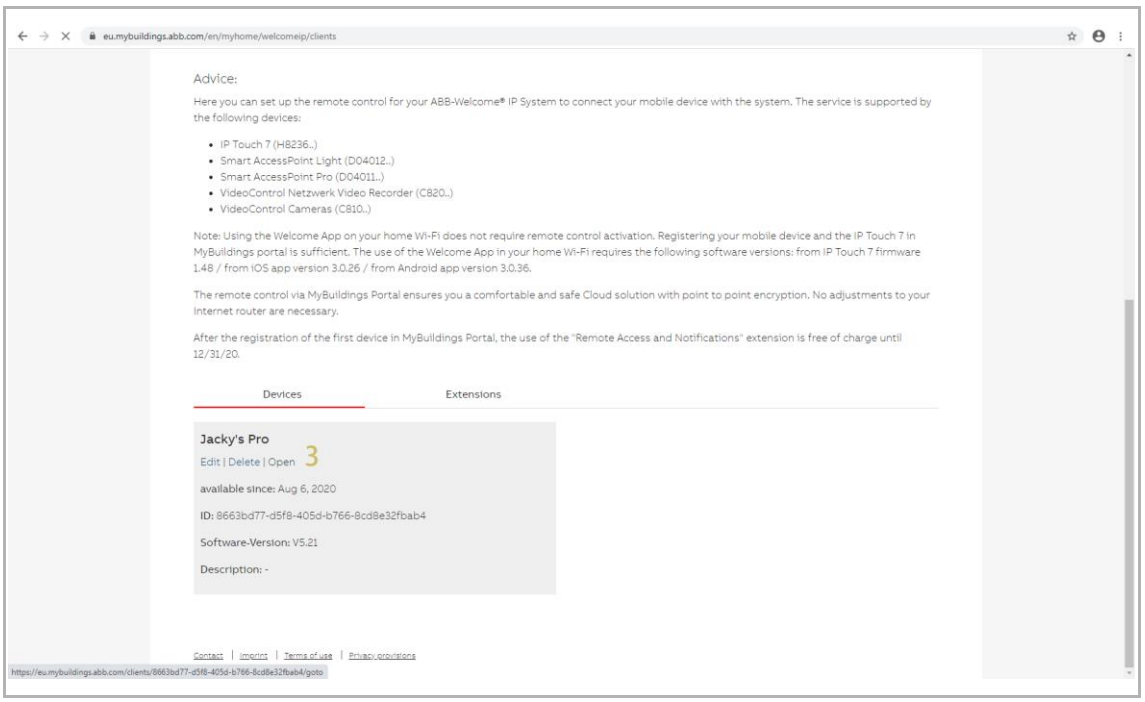
Volg de onderstaande stappen:

[1] Op de startpagina van het MyBuildings-portaal klikt u op "Mijn huis".

[2] Klik op "ABB-Welcome IP".



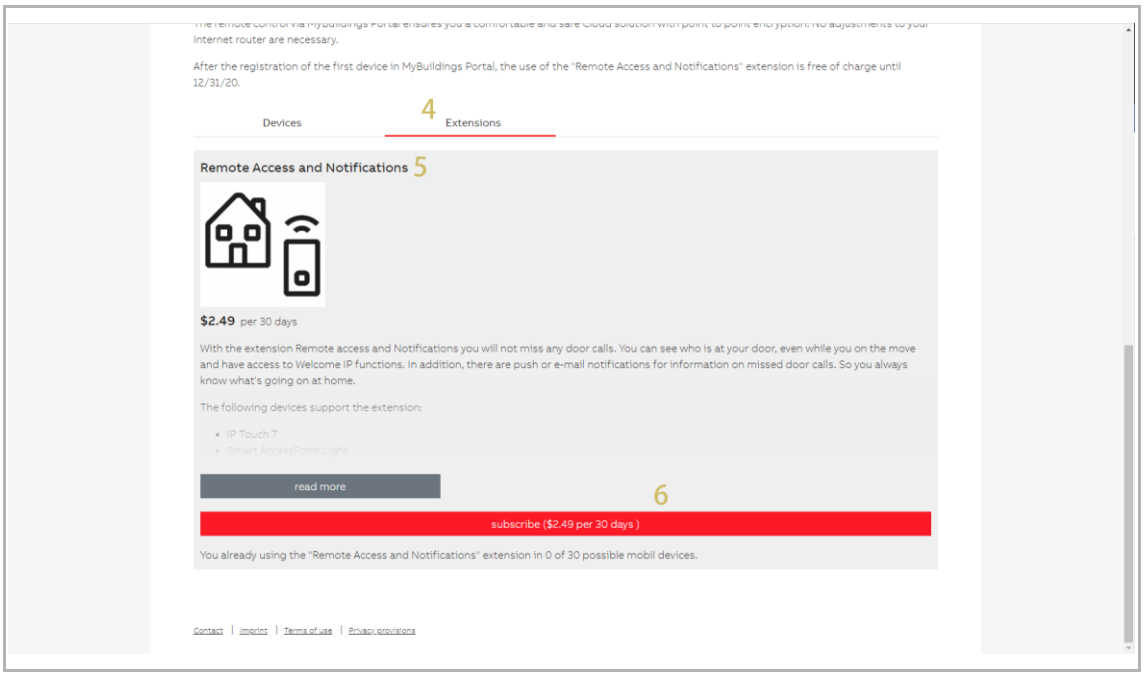
[3] Scroll naar beneden, zoek het "Smart Access Point" en klik op "Open".



[4] Als u het scherm niet kunt openen, klikt u op "Uitbreidingen".

[5] Zoek het item "Toegang op afstand en meldingen".

[6] Klik op "Abonneren" om de service te kopen.



13.6.3 Functie "Afstandsbediening" herstellen

Er kan toegang worden verkregen tot het "Smart Access Point" op afstand via het MyBuildings-portaal. zie hoofdstuk 13.6.2 “Toegang tot het "Smart Access Point" op afstand“ op pagina 288.

Als u de functie "afstandsbediening" wilt herstellen, volgt u de onderstaande stappen:

[1] Klik in het configuratiescherm op "Instellingen" om het bijbehorende scherm te openen.

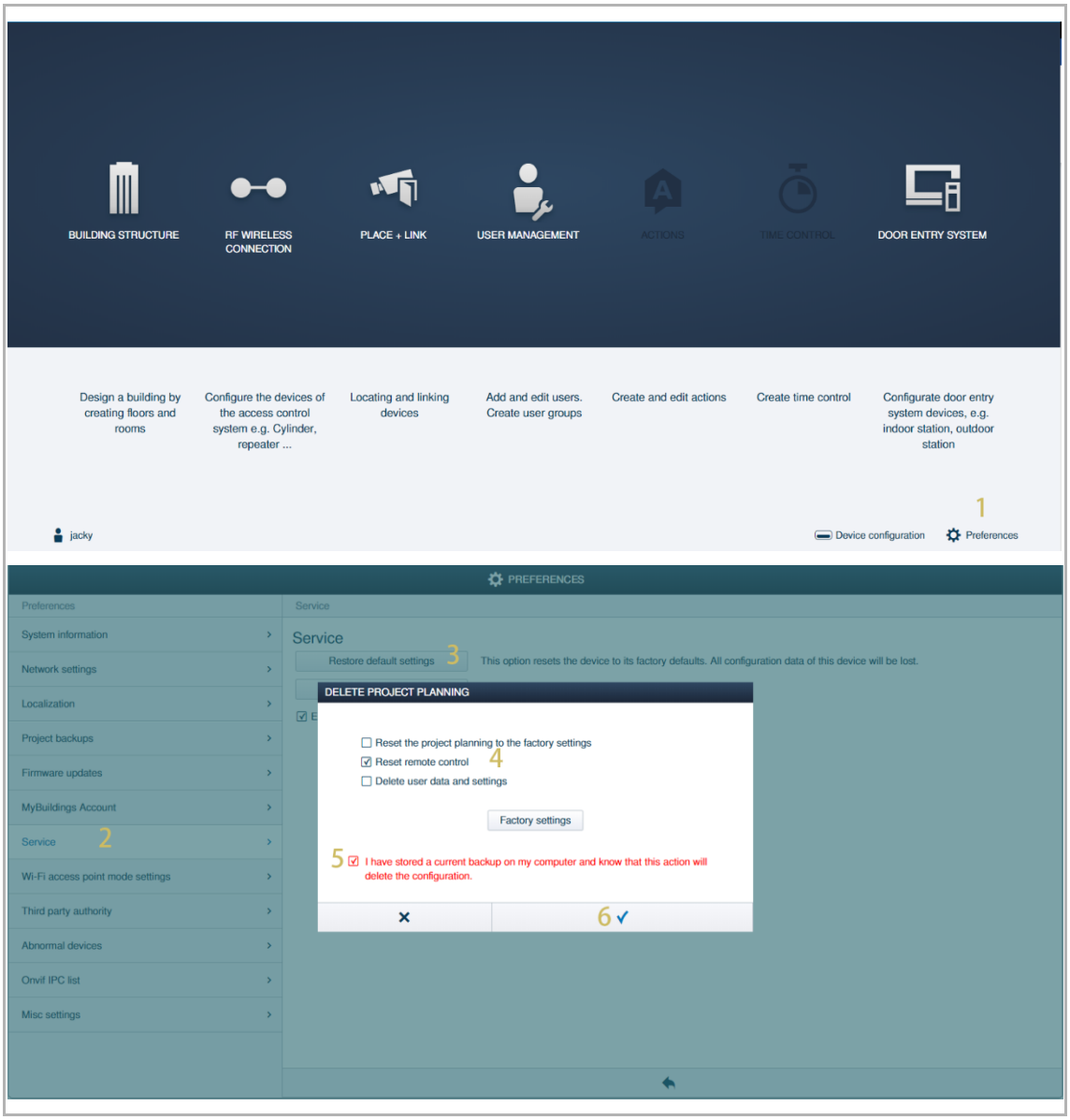
[2] Op het scherm "Instellingen" klikt u op "Service".

[3] Klik op "Voorinstellingen herstellen".

[4] Vink het keuzevakje "Toegang op afstand resetten" aan.

[5] Vink het keuzevakje "Ik heb opgeslagen …" aan.

[6] Klik op "√" om te bevestigen.



13.6.4 Alle voorinstellingen herstellen

Volg de onderstaande stappen:

[1] Klik in het configuratiescherm op "Instellingen" om het bijbehorende scherm te openen.

[2] Op het scherm "Instellingen" klikt u op "Service".

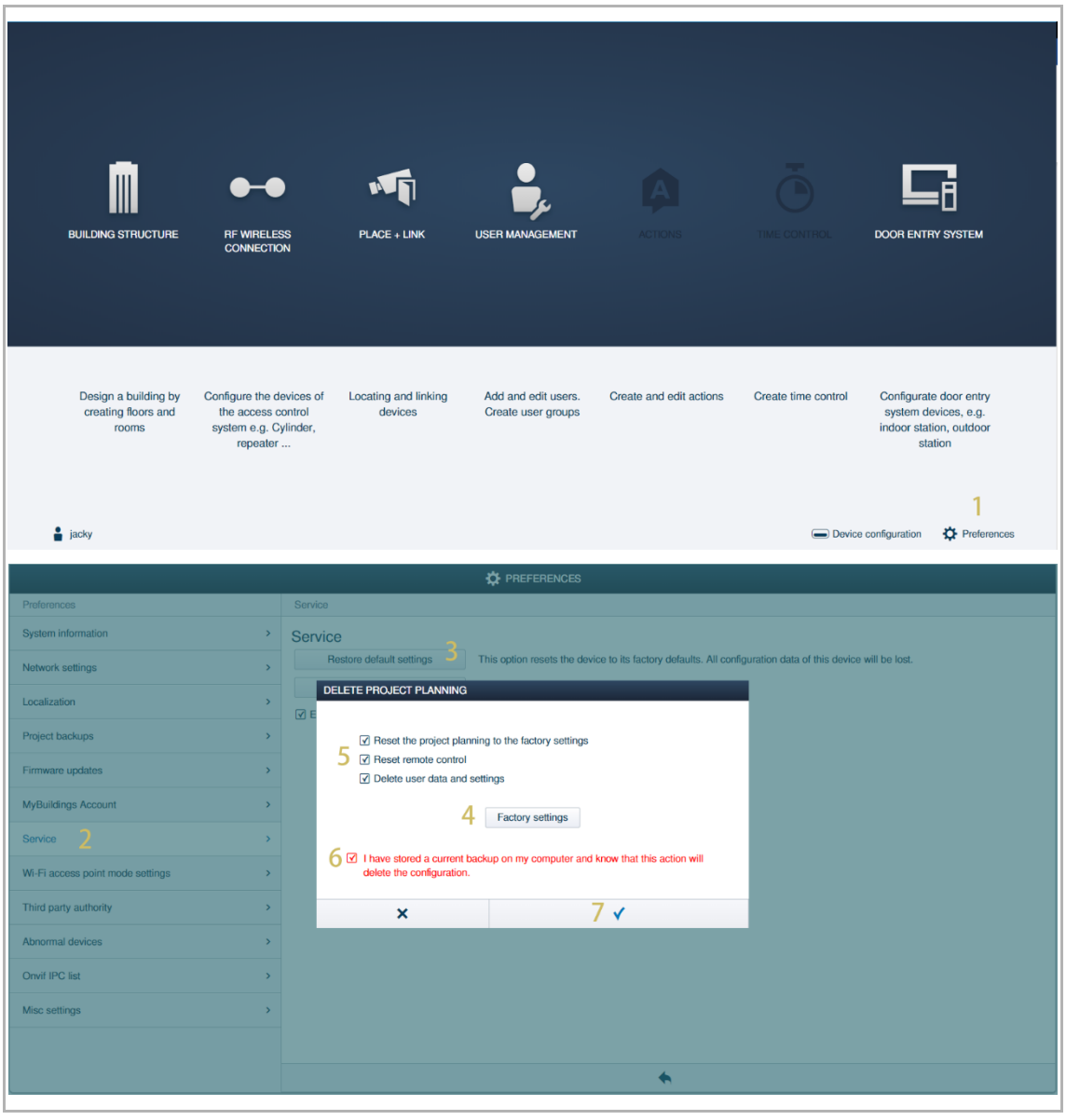
[3] Klik op "Voorinstellingen herstellen".

[4] klik op "Fabrieksinstellingen".

[5] Alle selectievakjes worden automatisch aangevinkt.

[6] Vink het keuzevakje "Ik heb opgeslagen …" aan.

[7] Klik op "√" om te bevestigen.

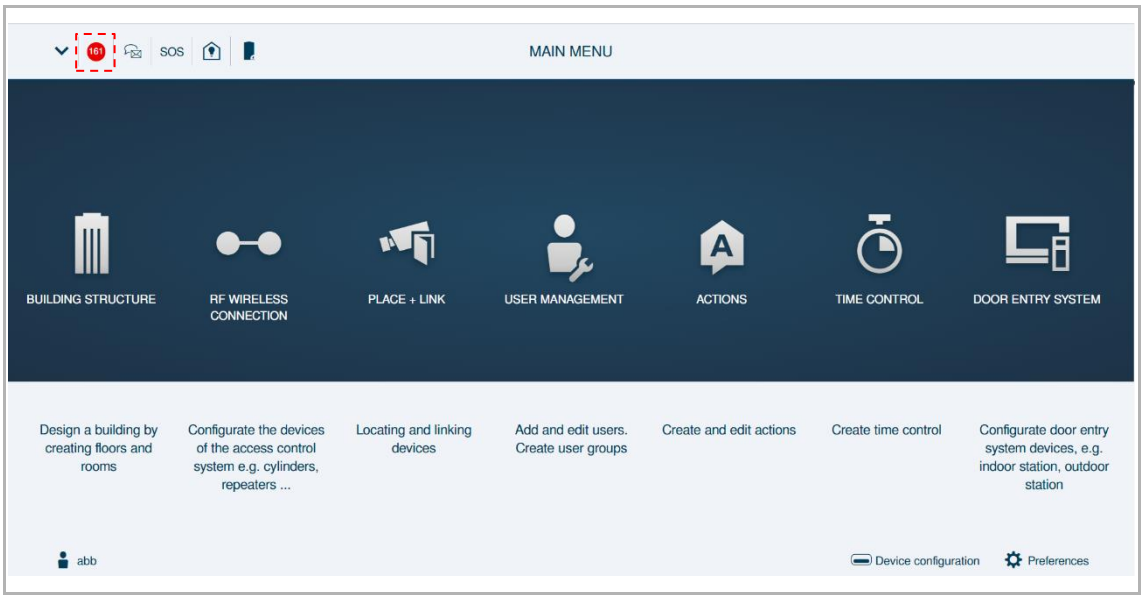


13.7 Melding

"Melding"-scherm oproepen

Klik in het configuratiescherm op " 0 " om het scherm "Melding" te openen.

Er worden maximaal 16.000 meldingen ondersteund op het Smart Access Point.



13.7.1 Melding

Wanneer de actie "Smart Access Point" is geactiveerd, ontvangt het "Smart Access Point" een melding.

Volg de onderstaande stappen:

[1] In het scherm "Melding" klikt u op "Melding".

[2] Voer het sleutelwoord in om te zoeken.

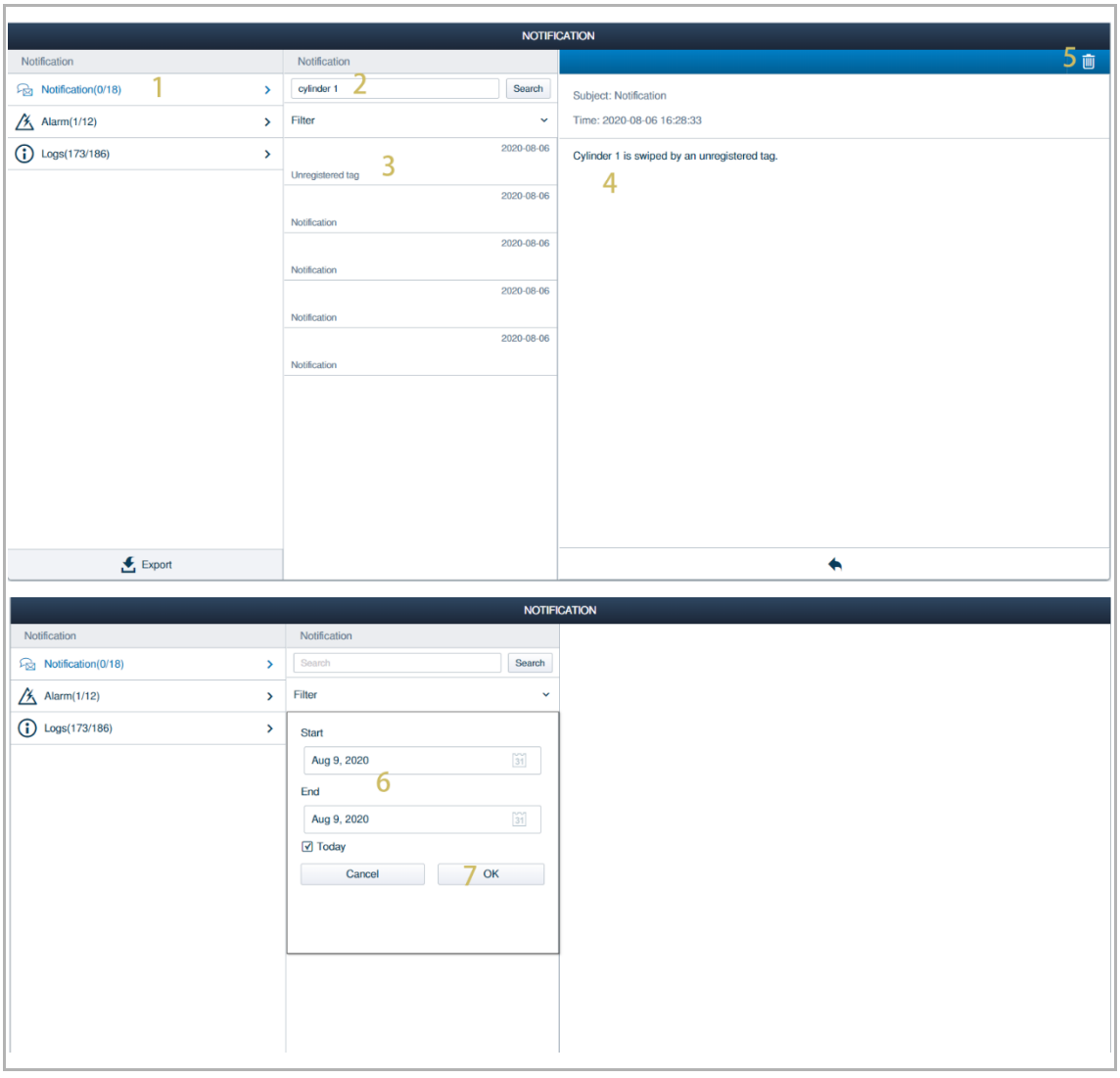
[3] De resultaatmeldingen worden op het scherm weergegeven.

[4] Klik op een melding om de details te bekijken.

[5] Klik op " " om de melding te verwijderen.

[6] Klik op "Filter", voer de begindatum en einddatum in om de meldingen te filteren op de datum. Vink het keuzevakje "Vandaag" aan om de meldingen van vandaag te filteren.

[7] Klik op "OK" om te bevestigen.



13.7.2 Alarmrapport

Volg de onderstaande stappen:

[1] In het scherm "Melding" klikt u op "Alarm".

[2] Voer het sleutelwoord in om te zoeken.

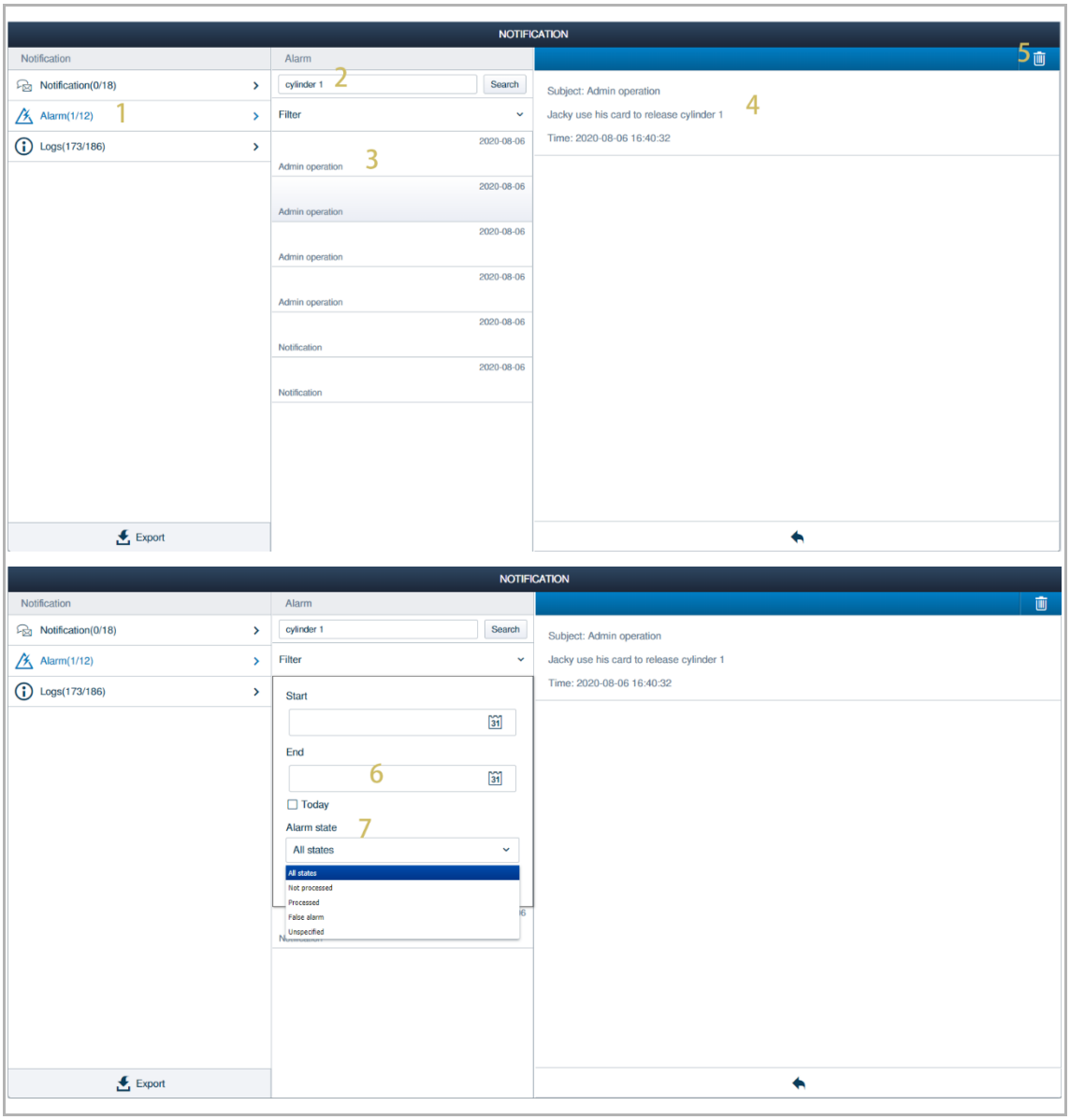
[3] De resulterende alarmen worden weergegeven op het scherm.

[4] Klik op een alarm om de details te bekijken.

[5] Klik op "" om het alarm te verwijderen.

[6] Klik op "Filter", voer de begindatum en einddatum in om de alarmen te filteren op de datum. Vink het keuzevakje "Vandaag" aan om de alarmen van vandaag te filteren.

[7] Selecteer de alarmstatus in de keuzelijst om de alarmen te filteren.



13.7.3 Protocollen

Volg de onderstaande stappen:

[1] In het scherm "Melding" klikt u op "Protocollen".

[2] Voer het sleutelwoord in om te zoeken.

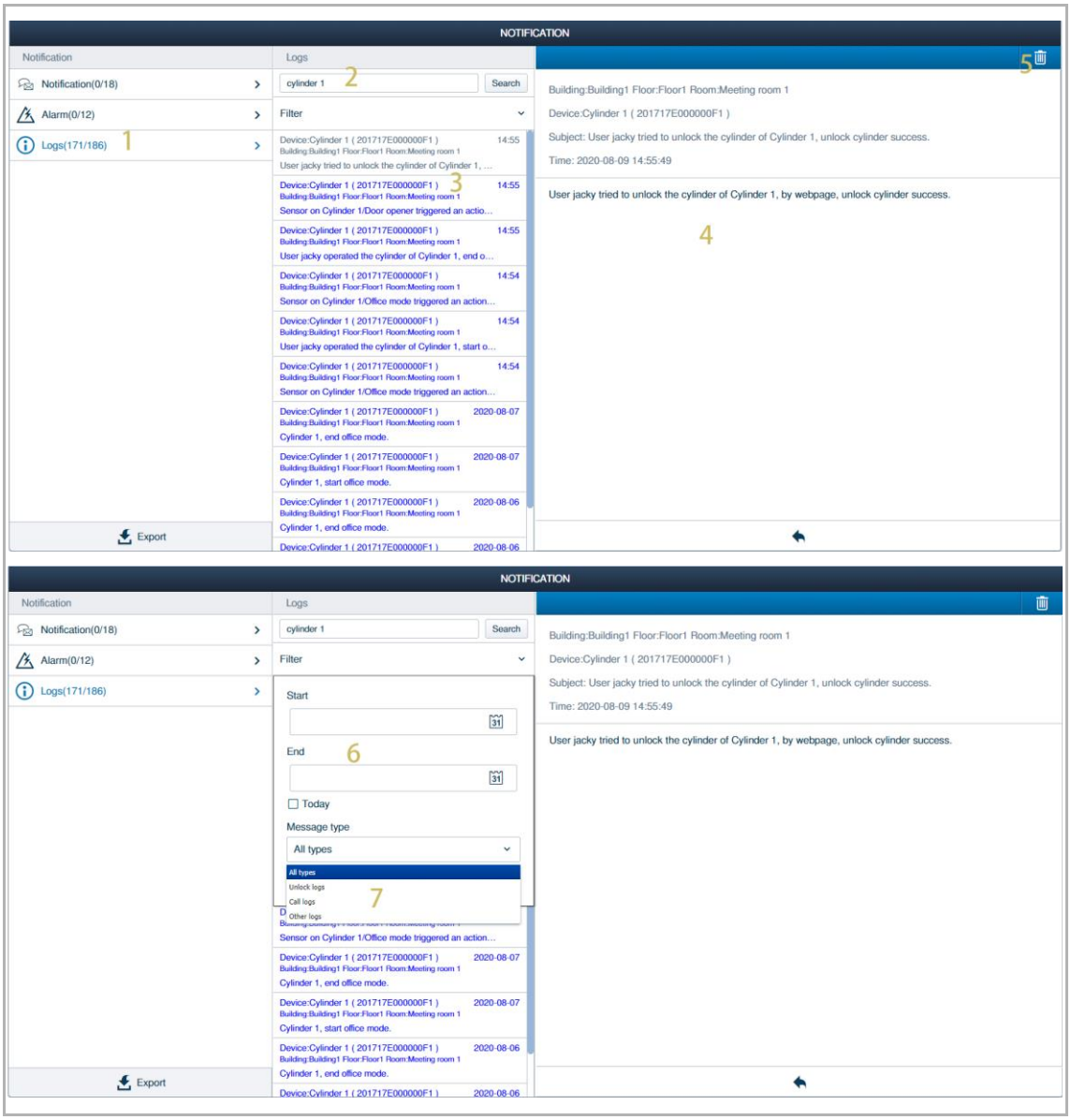
[3] De resulterende protocollen worden weergegeven op het scherm.

[4] Klik op een protocol om de details te bekijken.

[5] Klik op "" om het protocol te verwijderen.

[6] Klik op "Filter", voer de begindatum en einddatum in om de protocollen te filteren op de datum. Vink het keuzevakje "Vandaag" aan om de protocollen van vandaag te filteren.

[7] Selecteer het protocoltype in de keuzelijst om de protocollen te filteren.



13.7.4 Meldingen exporteren

Volg de onderstaande stappen:

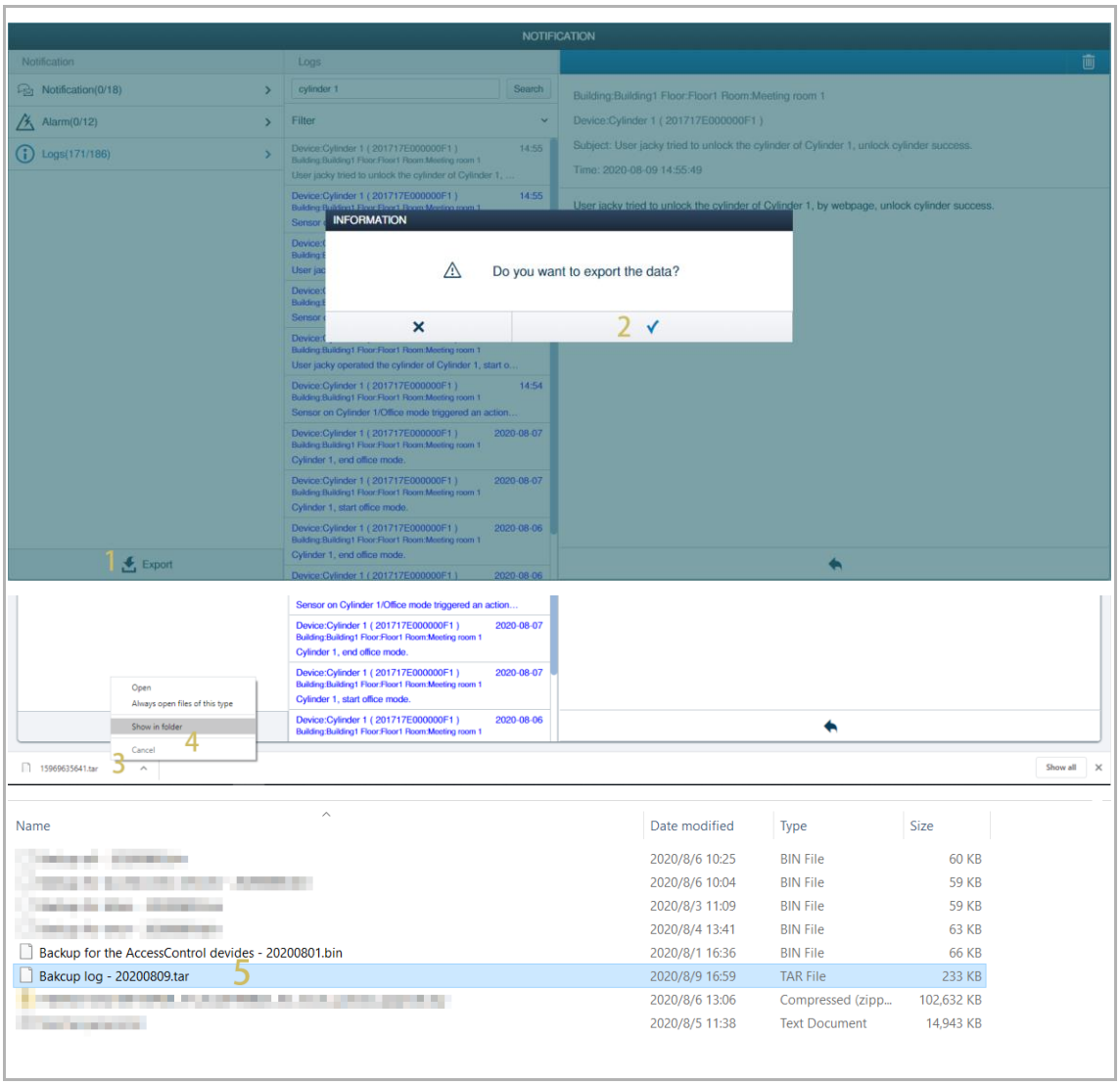
[1] In het scherm "Melding" klikt u op "Exporteren".

[2] Klik op "√".

[3] Rechtsklik op het geëxporteerde bestand.

[4] Klik op "In map weergeven".

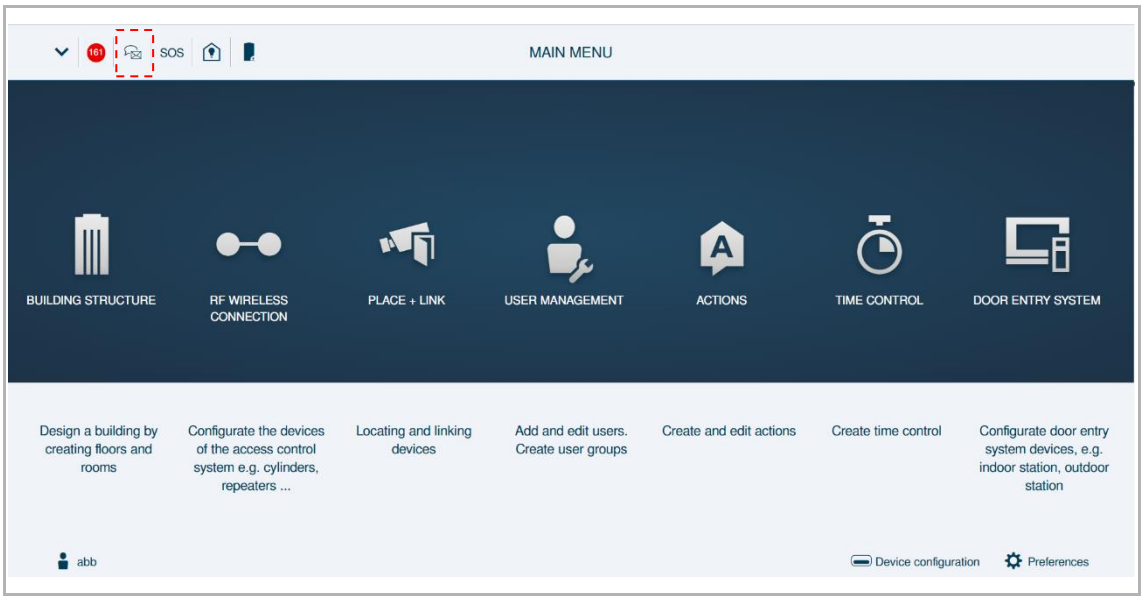
[5] Geef het logbestand een andere naam.



13.8 Berichtencentrale

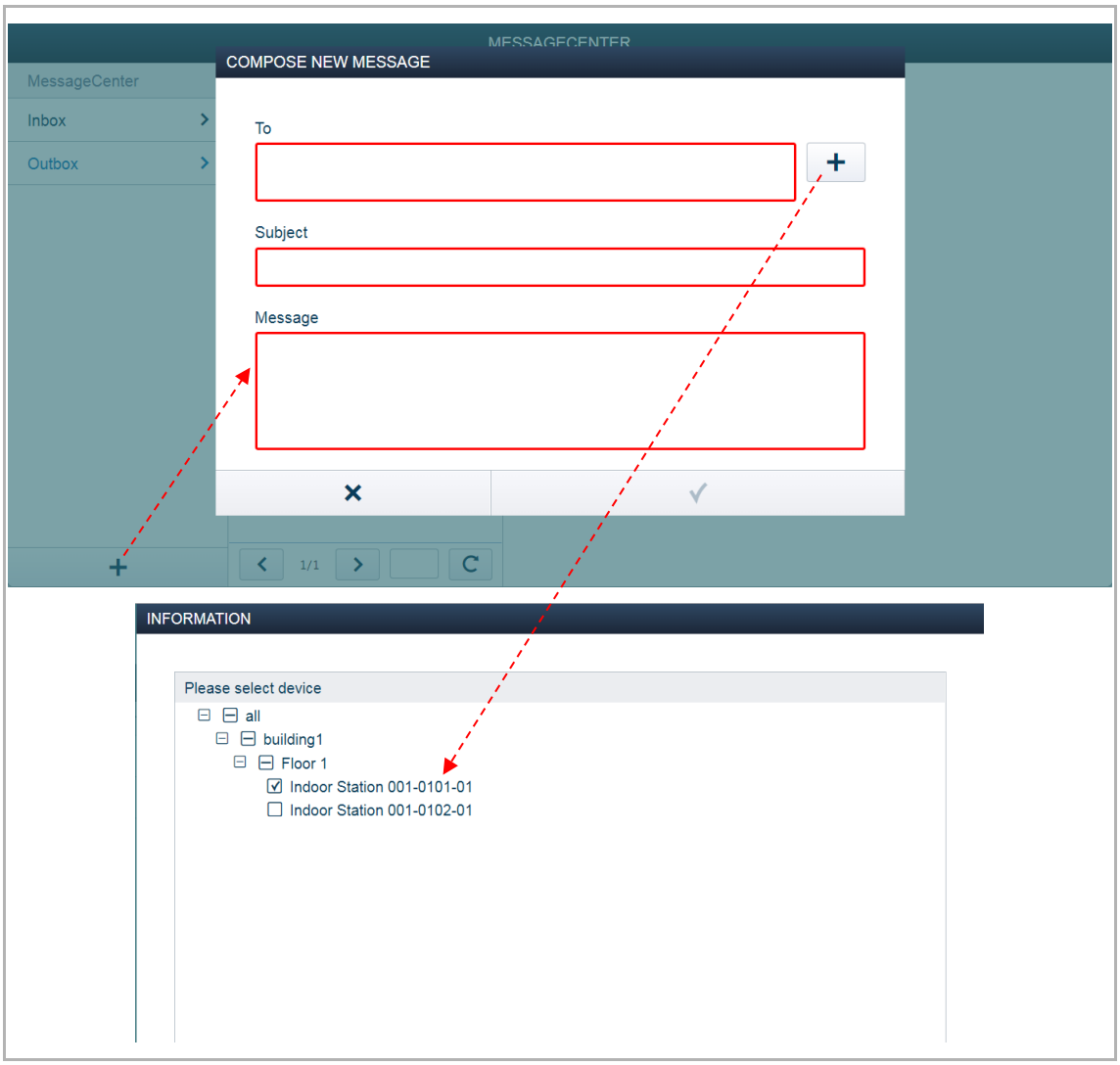
Het scherm "Berichtencentrale" openen

Klik in het configuratiescherm op " " om het bijbehorende scherm te openen.



13.8.1 Een bericht maken en versturen

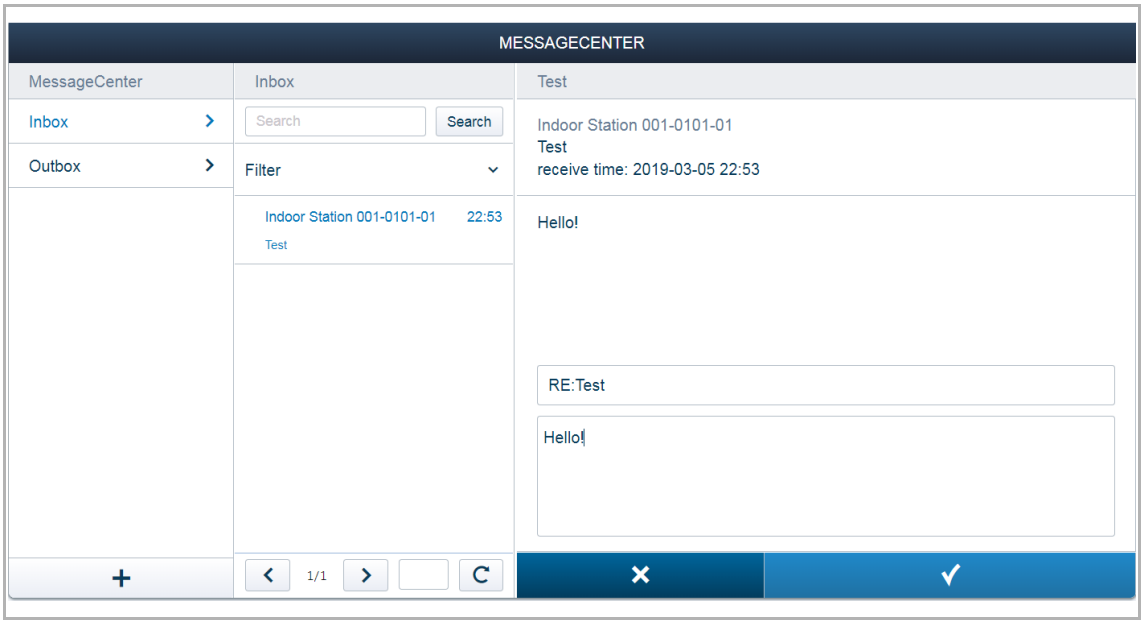
In het scherm "Berichtencentrale" klikt u op "+" om een ontvanger in te stellen, voer vervolgens het onderwerp en het bericht in en klik op "√" om het bericht aan te maken en te verzenden.



13.8.2 Een bericht bekijken en beantwoorden

Op het scherm "Berichtencentrale" klikt u op "Postvak in" om het van de binnenpost ontvangen tekstbericht te bekijken. U kunt op een bericht klikken om deze direct te beantwoorden.

Maximaal 1000 berichten worden ondersteund.



Uw antwoordberichten kunnen worden bekeken in het "Postvak uit". Maximaal 100 berichten kunnen worden ondersteund.

14 Opmerkingen

We behouden ons het recht voor om te allen tijde technische wijzigingen aan te brengen, evenals wijzigingen in de inhoud van dit document zonder voorafgaande kennisgeving.

De gedetailleerde specificaties die op het moment van bestellen zijn overeengekomen, zijn van toepassing op alle bestellingen. ABB aanvaardt geen verantwoordelijkheid voor mogelijke fouten of onvolledigheden in dit document.

We behouden ons alle rechten op dit document en de daarin opgenomen onderwerpen en illustraties. Het document en de inhoud ervan, of uittreksels daarvan, mogen niet worden gereproduceerd, overgedragen of hergebruikt door derden zonder voorafgaande schriftelijke toestemming van ABB.

Contact met ons opnemen

ABB Xiamen Smart Technology Co., Ltd.
No. 881, FangShanXiEr Road, Xiang'An Industrial Area, Torch Hi-Tech Industrial Development Zone, Xiamen
Tel: +86 592 295 9000
Fax: +86 592 562 5072

www.abb.com

Goedkeuringen en conformiteiten

Opmerking
We behouden ons het recht voor om te allen tijde zonder voorafgaande kennisgeving technische wijzigingen en wijzigingen in de inhoud van dit document aan te brengen.
Voor bestellingen gelden de overeengekomen gedetailleerde specificaties. ABB aanvaardt geen aansprakelijkheid voor mogelijke fouten of gebreken in dit document.

We behouden ons alle rechten voor op dit document en de daarin opgenomen onderwerpen en illustraties. Het document en de inhoud ervan, of uittreksels daarvan, mogen niet worden gereproduceerd, doorgegeven of hergebruikt door derden zonder voorafgaande schriftelijke toestemming van ABB.

Copyright© 2024 ABB
Alle rechten voorbehouden