



Security Tech Germany

FUAA85000

ERRICHTERANLEITUNG

Comfion Pro Funk-Sicherheitssystem



Deutsch



English



Français



Nederlands

1.	Aktualisierungen	5
1.1.	Anleitung	5
1.2.	Comfion Pro Firmware & Release notes	5
2.	Allgemeines	6
2.1.	Einführung	6
2.2.	Bestimmungsgemäße Verwendung / Rechtliche Hinweise	6
2.3.	Kundendienst / Customer Support	6
2.4.	Impressum	6
2.5.	Symbolerklärung	7
2.	Funktionsprinzip und Leistungsmerkmale	7
2.1.	Produktmerkmale	7
2.2.	Lieferumfang	8
2.3.	Gerätebeschreibung	9
2.4.	Technische Daten	11
3.	Montage & Inbetriebnahme	12
3.1.	Wandmontage der Zentrale	12
3.2.	Inbetriebnahme des Systems	15
3.2.1.	Einrichtung via App & Abschluss der Hardware-Vorbereitungen	15
3.2.2.	Dashboard (nach Erst-Anmeldung)	18
3.2.3.	Bereiche	18
3.2.4.	Räume	19
3.2.5.	Komponenten	20
3.2.6.	Komponenten-Einstellungen	22
3.2.7.	Hinweise zur Verdrahtung (Eingänge/Ausgänge/BUS)	23
3.2.8.	Alarmmodi	24
3.3.	WLX Pro Installation & Einlernen	25
3.3.1.	Installation, Konfiguration und Benutzung der WLX Pro Zylinder und Wandleser	26
3.3.2.	WLX Pro Funktionen – Fernöffnung und Büromodus	27
3.4.	Kameras (NVR)	28
3.4.1.	Einbinden von Kameras per ONVIF	28
3.4.2.	Einbinden von Kameras per RTSP	29
3.4.3.	Kamera Einstellungen (global)	30
3.4.4.	Kamera Einstellungen (einzeln)	30
3.4.5.	NVR-Bedienung	32

4.	Benutzer und Berechtigungsgruppen	33
4.1.	Erklärung der verschiedenen Rollen	33
4.2.	Inbetriebnahme	34
4.2.1.	Übergabe an den Besitzer	34
4.3.	Einladen/Hinzufügen von Benutzern	34
4.4.	Bearbeiten von Benutzern	34
4.4.1.	Zugriffsrechte	34
4.4.2.	Benachrichtigungen	35
4.4.3.	Erlaubte Alarmmodi im Betrieb	36
4.5.	Löschen von Benutzern	36
5.	Kommunikation	36
5.1.	Mobilfunkmodul	36
5.2.	E-Mail	37
5.3.	Telefonanruf	38
5.4.	SMS	38
5.5.	SIA DC-09 (Leitstellenaufschaltung)	39
6.	Allgemeines, Wartung und Hinweise	40
6.1.	Zentralen-Konfiguration	40
6.1.1.	Allgemeine Informationen	40
6.1.2.	Netzwerk	40
6.1.3.	Sicherheitseinstellungen	41
6.1.4.	PIN-Codes	42
6.1.5.	Benachrichtigungsverzögerungen	43
6.1.6.	HomeKit	43
6.1.7.	Backup	43
6.1.8.	WLX-Informationen	44
6.2.	Dashboard (System eingerichtet)	45
6.3.	Zentralenübersicht	46
6.3.1.	Account-Informationen	46
6.3.2.	Mitglieder	47
6.3.3.	Account-Logbuch	47
6.4.	Automationen & Szenen	47
6.5.	Resets	51
6.5.1.	Werksreset	51
6.5.2.	Neustart (Reboot)	51

6.5.3.	User-Reset	51
6.5.4.	Netzwerk-Reset	51
6.6.	Bedienung	52
6.6.1.	Scharf- / Unscharfschaltung	52
6.6.2.	Rückstellung von Alarmen	53
6.6.3.	Zwangsscharf	54
6.7.	Symbolerklärung	55
6.8.	ABUS-Cloud	57
6.9.	Hinweise zur Festplatte / SSD-Datenspeicher	57
6.10.	Wartung und Instandhaltung durch Errichter	57
6.11.	Tabelle Funk-Signalstärken	58
7.	Gewährleistung	58
8.	Entsorgungshinweise	58
9.	Konformität	58
9.1.	EU-Konformitätserklärung	58
9.2.	Konformität nach EN 50131	58
10.	Anhang	59
10.1.	Contact-ID Codetabelle	59

1. Aktualisierungen

1.1. Anleitung

Version	Datum Veröffentlichung	Änderungen
1.0	12.05.2026	Initiale Version
1.1	13.05.2026	Ergänzungen: - Neu: Kapitel 1 Aktualisierungen (vorher Kapitel 7) - Kapitel 3.2.6: Ergänzung IP-Kameras & MotionAlarm - Neu: Kapitel 3.3 WLX Pro Installation & Einlernen - Neu: Kapitel 3.4.3 Kamera Einstellungen (global) - Neu: Kapitel 3.4.4 Kamera Einstellungen (einzeln) - Neu: Kapitel 3.3.2 Einbinden von Kameras per RTSP - Neu: Kapitel 10.1 Contact-ID Codetabelle - Kapitel 6.6.1: Scharf/Unscharf WLX Pro Zylinder & Wallreader ergänzt
1.2	30.06.2026	Ergänzungen: - Neu: Sprachen Englisch, Französisch, Niederländisch ergänzt - Neu: Änderungen durch FW Release 1.0.2945

1.2. Comfion Pro Firmware & Release notes

Firmware-Version	APP-Version	Datum Veröffentlichung	Änderungen
1.0.2864	2.1.96	12.05.2026	Initiale Version
1.0.2945	2.1.134	30.06.2026	Änderungen: - Anpassung Default-Werte FUBE80100 zur Erhöhung der Batterielaufzeit (nur für neu eingelernte Geräte) - Anpassung Aufwach-Zeit FUBE80100 zur Erhöhung der Batterielaufzeit - Anpassung diverser Logbuch-Einträge (Ergänzung Benutzer, Bereich, etc.) - Anpassung Vorkonfiguration Hybridmodul bei Nutzung mit wAppLoxx - Verbesserungen Videostream H.26 - Sicherheitsanpassungen - Design & String-Anpassungen Fehlerkorrekturen: - Zwangsläufigkeit WLX Access Komponenten - Berechtigungs-Meldung „Zugriff auf Galerie“ bei App-start - Korrektor Sicherheitseinstellungen - Zentralensabotage

Die Release-Notes zum aktuellen Firmware-Update finden Sie in Ihrer Comfion App oder unter dem folgenden Link:
<https://l.ead.me/bgICEA>

2. Allgemeines

2.1. Einführung

Vielen Dank, dass Sie sich mit dem **Comfion Pro Funk-Sicherheitssystem** für ein Produkt von ABUS Security Center (in der Kurzform auch "ABUS" genannt) entschieden haben.

Das vorliegende Handbuch enthält wesentliche Beschreibungen, Technischen Daten, Übersichten und weiterführende Informationen zur Projektierung, Inbetriebnahme und Bedienung des **Comfion Pro Funk-Sicherheitssystems**.

Die hier beschriebenen Produkte/Systeme dürfen nur von Personen installiert und gewartet werden, die für die jeweilige Aufgabenstellung qualifiziert sind. Qualifiziertes Personal für die Installation und Wartung des Systems ist i. d. R. ein geschulter ABUS-Fachpartner.

2.2. Bestimmungsgemäße Verwendung / Rechtliche Hinweise

Die Verantwortung für den rechtskonformen Einsatz des Produkts liegt beim Käufer bzw. Kunden und dem Endnutzer. Gemäß der im Produkthaftungsgesetz definierten Haftpflicht des Herstellers für seine Produkte sind die vorstehenden Informationen zu beachten und an die Betreiber und Nutzer weiterzugeben. Die Nichtbeachtung entbindet ABUS Security Center von der gesetzlichen Haftung.

Nicht vereinbarungsgemäße bzw. unübliche Verwendung, nicht ausdrücklich von ABUS zugelassene Reparaturarbeiten bzw. Modifikationen sowie nicht fachgemäßer Service können zu Funktionsstörungen führen und sind zu unterlassen. Jegliche, nicht ausdrücklich von ABUS zugelassene, Änderungen führen zu Verlust von Haftungs-, Gewährleistungs- und gesondert vereinbarten Garantieansprüchen.

Architekten, Technische Gebäudeplaner (TGA) und weitere beratende Institutionen sind angehalten, alle erforderlichen Produktinformationen von ABUS einzuholen, um den Informations- und Instruktionspflichten gemäß Produkthaftungsgesetz nachzukommen. Fachhändler und Verarbeiter sind angehalten, die Hinweise in der ABUS-Dokumentation zu beachten und diese gegebenenfalls an ihre Kunden weiterzuleiten.

Weiterführende Informationen finden Sie auf www.abus.com auf der allgemeinen Seite oder für Händler und Installateure im Partnerportal auf <https://partner-asc.abus.com/>

2.3. Kundendienst / Customer Support

Für weitere Hilfe steht unser Support-Team für Sie zur Verfügung: support@abus-sc.com

Allgemeine Informationen zum **Comfion Pro Funk-Sicherheitssystem** finden Sie auf unserer Homepage unter: <https://www.abus.com/de/Privat/Alarmsysteme/Comfion-Funk-System>

2.4. Impressum

Mit dem Erscheinen einer neueren Installationsanleitung verliert diese Ausgabe ihre Gültigkeit.

Alle Rechte vorbehalten. Ohne schriftliche Zustimmung des Herausgebers darf diese Installationsanleitung, auch nicht auszugsweise, in irgendeiner Form reproduziert oder unter Verwendung elektronischer, mechanischer oder chemischer Verfahren vervielfältigt oder verarbeitet werden.

Für Fehler technischer oder drucktechnischer Art und ihre Folgen übernimmt ABUS Security Center keine Haftung. Die Angaben in dieser Installationsanleitung wurden nach bestem Wissen und Gewissen unter Berücksichtigung des jeweiligen Standes der Technik zusammengestellt. Sie werden regelmäßig überprüft und bei Bedarf aktualisiert bzw. korrigiert.

Alle Warenzeichen und Schutzrechte werden anerkannt, Änderungen im Sinne des technischen Fortschritts können ohne Vorankündigungen vorgenommen werden.

2.5. Symbolerklärung

In dieser Installationsanleitung werden die folgenden Symbole verwendet:

Symbol	Signalwort	Bedeutung
	Vorsicht	Weist auf eine Verletzungsgefahr oder Gesundheitsgefährdung durch elektrische Spannung hin
	Wichtig	Weist auf eine mögliche Beschädigung des Geräts/Zubehörs oder auf eine Verletzungs- oder Gesundheitsrisiko hin
	Hinweis	Weist auf wichtige Informationen hin

2. Funktionsprinzip und Leistungsmerkmale

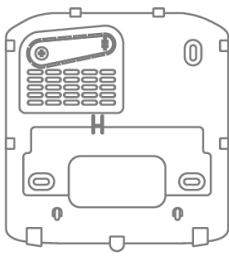
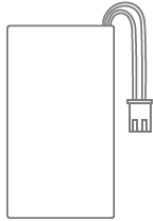
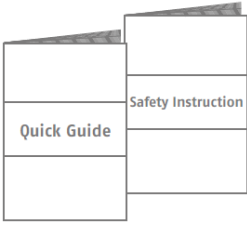
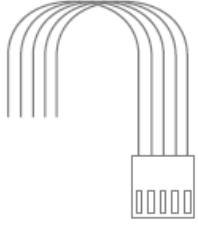
2.1. Produktmerkmale

Das **FUAA85000 Comfion Pro Funk-Sicherheitssystem** ist ein EN-Grad-2-zertifiziertes Einbruchmeldesystem mit Smart Home-Funktionen. Das System kann über die intuitive App oder das ABUS-Cloud-Portal eingerichtet und bedient werden.

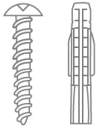
Hauptmerkmale:

- All-in-One Sicherheitssystem: Alarmanlage, Video-NVR (bis 8 Kameras) und Zutrittskontrolle in einem System – reduziert Gerätevielfalt und Installationsaufwand.
- Native wAppLoxx Pro Integration: Direktes Scharf-/Unscharf schalten an der Tür – weniger Fehlalarme, höhere Bedienakzeptanz beim Endkunden.
- Perimeterwarnung mit Außenkomponenten: Frühzeitige Detektion von Eindringlingen – erhöhte Interventionszeit und reduziertes Einbruchrisiko.
- Integrierter Netzwerk-Videorekorder: Zentrale Aufzeichnung und Verwaltung für bis zu 8 Kameras – Videobilder im Alarmfall direkt in der App sichtbar und ohne zusätzlichen NVR-Rekorder realisierbar.
- App-Steuerung & Smart-Home-Szenarien: Zentrale Bedienung aller Komponenten, Szenarien flexibel konfigurierbar – ideal für individuelle Kundenanforderungen.
- Skalierbar und projektstark: Bis zu 160 Funk-Komponenten und 40 Teilbereiche – mit hoher Funkreichweite bis zu 2.600 m im Freifeld für effiziente Planung von kleinen Objekten bis hin zu größeren Projekten.
- Sicherer 868-Funk mit AES128-Bit-Verschlüsselung: Damit ist eine hohe Übertragungssicherheit gewährleistet, der bidirektionale Funk stellt sicher, dass das Funksignal angekommen ist
- EN 50131 Grad 2: Geeignet für versicherungsrelevante Sicherheitsanforderungen und professionelle Projekte.
- 4G-Mobilfunk-Backup: Sichere Alarmübertragung auch bei Netzausfall – erhöhte Systemverfügbarkeit.
- Sabotageschutz: Wandabriss-Kontakt & Systemüberwachung – zuverlässiger Betrieb im Alltag.
- Jamming-Überwachung: Wird ein Störsender erkannt, schlägt Comfion Pro Alarm
- Einen Sicherheitsdienst beauftragen: Leitstellenprotokoll integriert (SIA DC-09)
- Immer alle Informationen zur Hand: Benachrichtigungen wahlweise über SMS, E-Mail oder Push-Nachricht

2.2. Lieferumfang

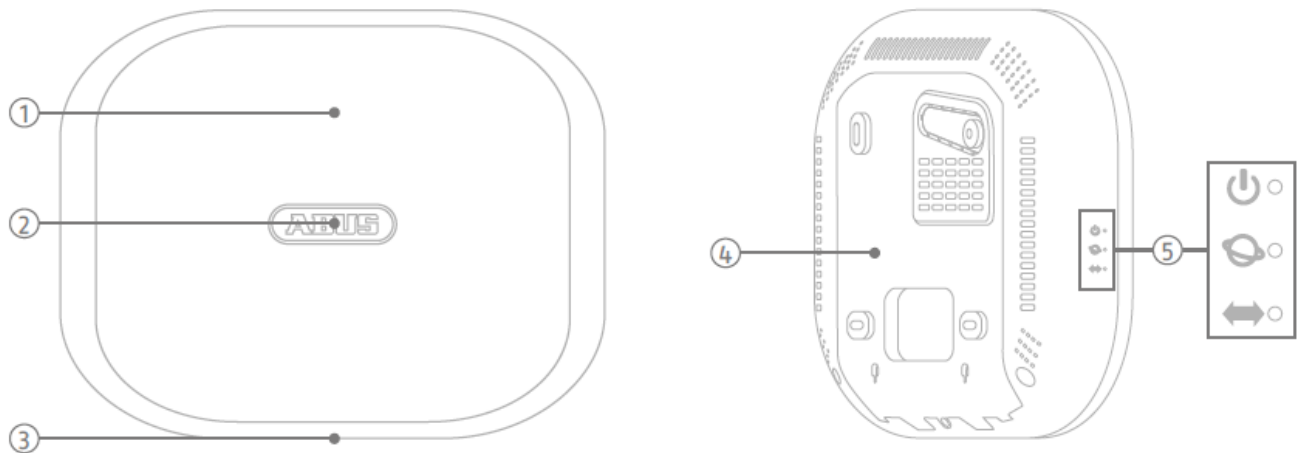
		
1 x Zentrale	1 x Wandhalterung	1 x Akku
		
Kurzanleitung & Sicherheitshinweise	2 x Drahtmelder-Kabel	4 x Schrauben für Festplatte
		
1 x Öffnungswerkzeug		

Benötigt:


4 x Schrauben / Dübel Ø 7.0 mm

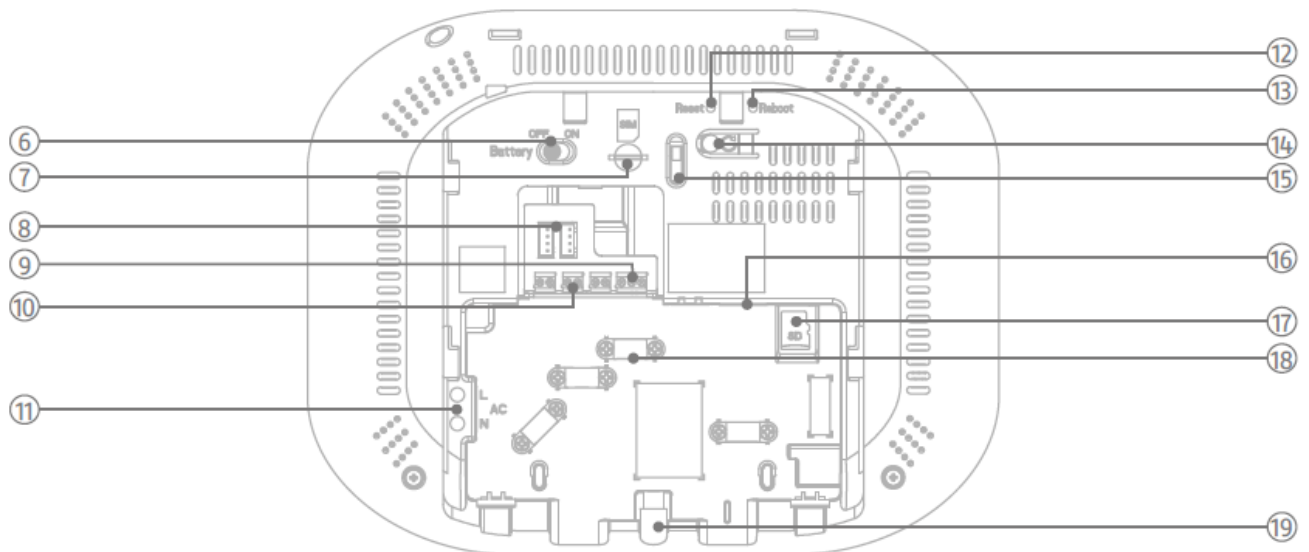
2.3. Gerätebeschreibung

Produktaufbau (Vorder-/ Rückseite)



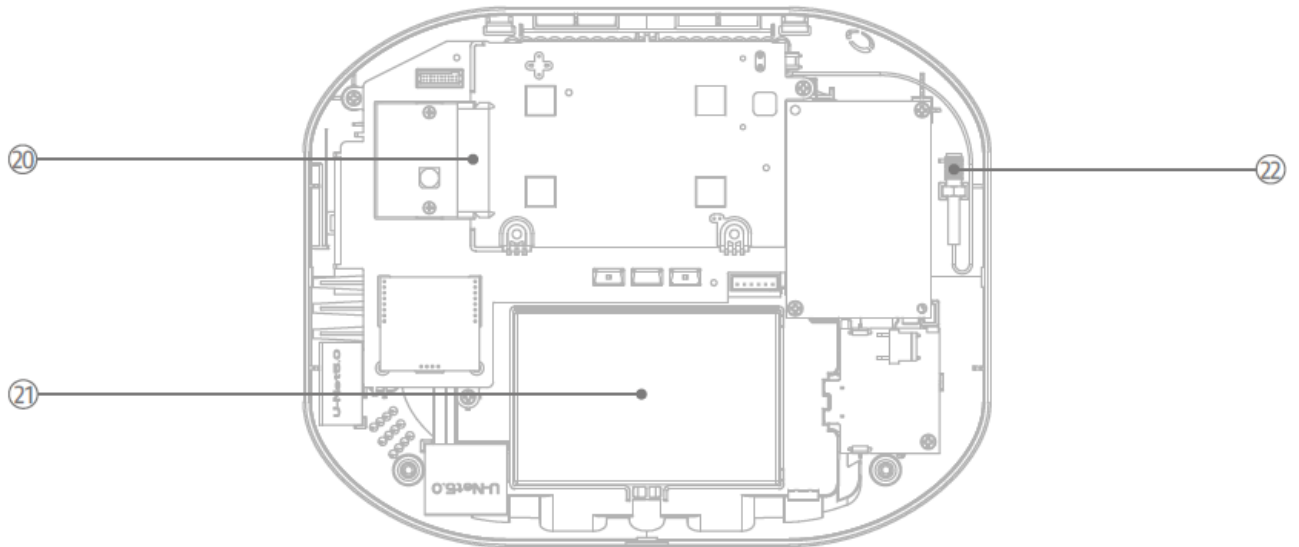
1	Deckel	2	Logo (Alarm-Status)	3	Öffnungsmechanismus
4	Rückplatte	5	Status-LEDs Stromversorgung, Internet, Netzwerk		

Rückseite (geöffnet)



6	Batterie-Schalter	7	SIM-Kartenschacht (Nano-SIM)	8	Drahtmelder-Eingänge
9	Relais-Ausgang	10	BUS-Klemmen	11	AC-Anschlussklemmen (L/N)
12	Reset-Taste	13	Neustart-Taste	14	Netzwerk-Reset
15	Sabotageschalter	16	RJ45-Buchse	17	MicroSD Schacht
18	Zugentlastung	19	Befestigungsschraube		

Vorderseite (geöffnet)



20 SATA-Anschluss für SSD-Festplatte	21 Notstrom-Akku	22 Anschluss Externe Mobilfunkantenne (SMA)
--------------------------------------	------------------	---

LED-Status-Anzeigen

		  	
		Logo (Alarm-Status) Status-LEDs	
Unscharf	Weiß	Power-LED (oben)	
Scharf	Blau	Netzspannung	Grün
Teilscharf	Blau	Batteriebetrieb	Rot
Alarm	Rot (blinken)	Firmware-Update	Gelb (blinken)
Sabotage Zentrale	Rot (blinken)	Internet-LED (mitte)	
Einlernvorgang	Grün (blinken)	Online & Admin registriert	Grün
Wartungsmodus	Violett	Online & Admin nicht registriert	Grün (blinken)
Störung	Orange (blinken)	Offline	Rot
		Netzwerk-LED (unten)	
		LAN	Grün
		3G/4G Mobilfunk	Rot

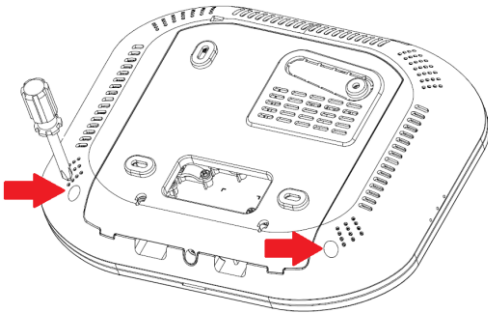
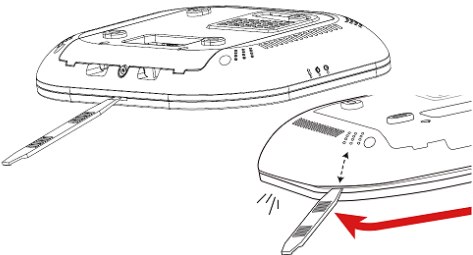
2.4. Technische Daten

Abmessungen (BxHxT)	242 x 190 x 45 mm
Gewicht	950g (mit Backup-Akku)
Betriebstemperatur	-10 °C bis +40 °C
Umweltklasse	II (EN 50131-1 + A3:2020)
Schutz vor Umwelteinwirkungen	IP40 / IK06
Luftfeuchtigkeit	max. 85% RH (Relative Luftfeuchte)
Anschlüsse	L/N Buchse (230 Volt), RJ45 (LAN), SATA-3.0-Anschluss (für 2.5"-SSD), SIM-Kartenschacht (Nano-Sim), Micro-SD Kartenschacht
Ein/Ausgänge	4 Meldergruppen-Eingänge (NC/NO) potenzialfrei (Verdrahtungsart 2-Draht CC, EOL, DEOL) 1 Relaisausgang (NC/COM/NO) max. 30V DC / 1.6A
BUS-Schnittstelle	(GND / +V / B / A) 13,0 V Kabellänge max. 200m
Anzeigen	Status LED (Power, Internet, Kommunikation) ABUS-Logo (Systemstatus)
Tasten	Neustart-Taste, Reset-Taste, Netzwerk-Reset, Akku-Schalter
Funkfrequenz / Modulation	868.0 - 868.6 MHz / GFSK
Leistung, Funk / Reichweite	max. 25 mW (14dBm) / 1000m, Freifeld
Anzahl Funk-Komponenten	160
Anzahl Bereiche	40
Anzahl Benutzer	51
Anzahl Ereignisse	> 10.000
Netzwerkrecorder	Max. 8 Kanal @ 2048 kbps, Bei Nutzung 4 Kanäle @ 4096 kbps Beispiel: 4 Kanäle a 4K (3840 x 2160) + 4 Kanäle a 1080p (1920 x 1080)
Kommunikation	Ethernet 1 GbE LAN SSL/TLS Mobiles Netzwerk (Backup): 3G UMTS / 4G LTE SMS & Sprache: 2G GSM / 4G LTE
AÜA-Kategorie	SP5 (LAN) SP2 (GSM) DP3 (LAN + GSM)
Stromversorgung	Primär: AC 230V / 50Hz Sekundär: LiPo-Akku 7,4V / 6.000mAh
Typ der Stromversorgung	Typ A, Spannungsversorgung konform gemäß EN50131-1+A3:2020 und EN50131-6+A1:2021
Pufferzeit - Batteriebetrieb	> 12 Stunden gemäß EN50131-1+A3:2020 Grad 2
Sabotagesicherheit (Erkennung / Schutz)	ja (1x Wandabriss-Kontakt)
Supervisionszeit	900 - 3.600 s (Voreinstellung: 3.600 s)
Sicherheitsgrad	Grad 2 (EN 50131-1 + A3:2020)
Konformität	Sicherheitsgrad 2 bei ordnungsgemäßer Installation konform gemäß EN 50131-1+A3:2020, EN 50131-3:2009 und EN 50131-5-3:2017
EU-Richtlinien	RED: 2014/53/EU, RoHS: 2011/65/EU + 2015/863 Allgemeine Sicherheit: 2001/95/EG

3. Montage & Inbetriebnahme

3.1. Wandmontage der Zentrale

 Vorsicht	ACHTUNG: VOR DER INSTALLATION DIESER ANLAGE MÜSSEN SIE SICHERSTELLEN, DASS DIE NETZVERSORGUNG DER ALARMZENTRALE GETRENNT UND UNTERBROCHEN IST. (Achten Sie ebenfalls darauf, dass der Batterie-Schalter auf „Off“ steht.) Alle elektrischen Anschlüsse müssen von einem qualifizierten Elektriker ausgeführt werden und den geltenden lokalen Vorschriften entsprechen.
 Vorsicht	ACHTUNG: Wenn das Gerät an das Stromnetz angeschlossen wird, während dort eine Spannung anliegt, liegt die Netzspannung auch an den ummantelten Köpfen der Schraubklemmen des Netzanschlusses an. ACHTUNG: Das Netzkabel zur Alarmzentrale muss mit einer zweipoligen Trennvorrichtung gemäß EN 62368-1 versehen sein. Vorsicht: Wenn Sie die Platine in der Alarmzentrale anfassen, müssen Sie die üblichen Vorsichtsmaßnahmen treffen, um Schäden durch statische Elektrizität zu vermeiden.
 Hinweis	- Montieren Sie die Zentrale auf ca. 1,5m Höhe an die Wand - Halten Sie zu allen Seiten einen Abstand von mindestens 1,5 m zu folgenden Geräten ein: Elektrogeräte, metallische Objekte oder Geräte mit Funkabstrahlung (z.B. Router, Mikrowellen) – da diese die Funkleistung des Systems beeinträchtigen können.

Befestigung der Festplatte / SSD-Datenspeicher und externe Mobilfunkantenne (nicht im Lieferumfang)	
Öffnen Sie den Deckel der Zentrale. Lösen Sie hierfür die 2 Schrauben auf der Rückseite.	
Hebeln Sie den Deckel mithilfe des mitgelieferten Werkzeugs ab.	

Festplatte / SSD-Datenspeicher: (nicht im Lieferumfang) Schließen Sie die 2,5" SSD-Festplatte an den vorgesehenen Steckplatz an. (SATA 3.0) und fixieren den Datenträger mit den mitgelieferten Schrauben.

Externe Mobilfunk-Antenne: (nicht im Lieferumfang) Führen Sie das Anschlusskabel durch die vorbereitete Öffnung und schrauben dieses auf die SMA-Buchse.

Empfohlenes Zubehör bei ABUS:

TVAC41210 - 1 TB 2,5" SSD Datenspeicher SATA WD Red
TVAC41220 - 2 TB 2,5" SSD Datenspeicher SATA WD Red
FUZU85000 - Ext. Mobilfunkantenne für Comfion Pro



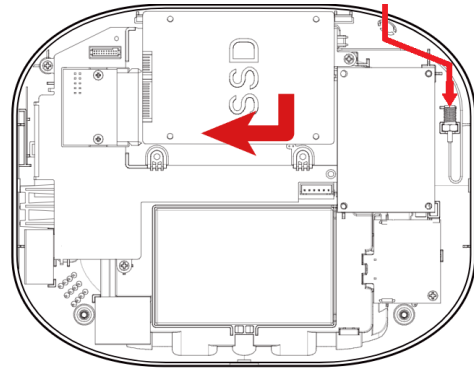
Hinweis

Formatieren Sie die Festplatte vor Einlegen im Format exFAT oder NTFS.

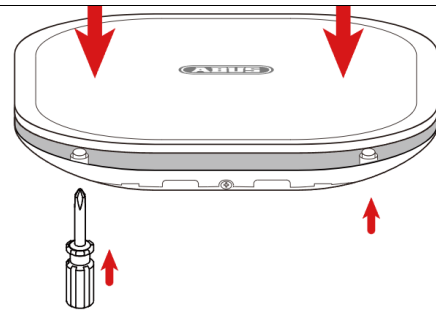


Hinweis

Der 2.5" Festplatten-Steckplatz erlaubt die Verwendung von HDD-Festplatten und SSD-Datenspeichern. Die Anforderungen nach EN 50131 (Notstromzeit) werden bei Verwendung eines SSD-Datenspeichers erfüllt.

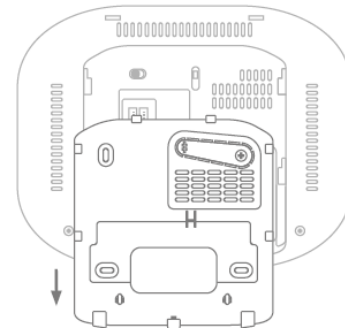


Befestigen Sie den Deckel bis dieser hörbar einrastet und fixieren sie die Schrauben auf der Rückseite.



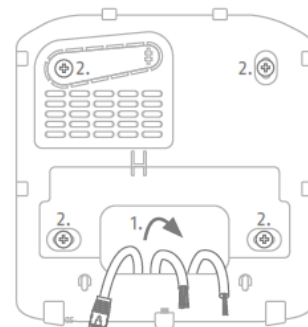
Wandmontage & Verkabelung

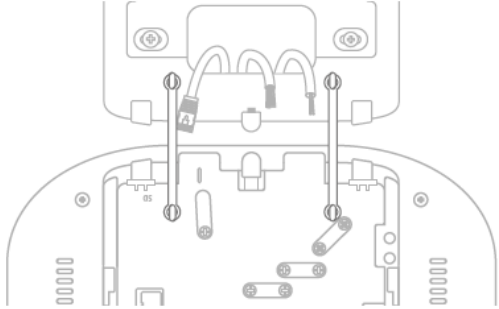
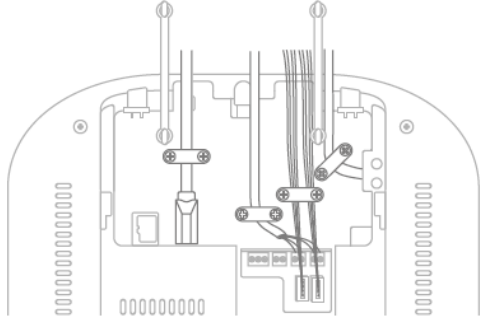
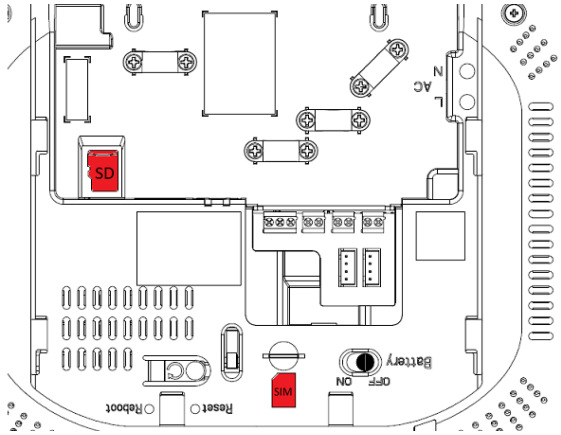
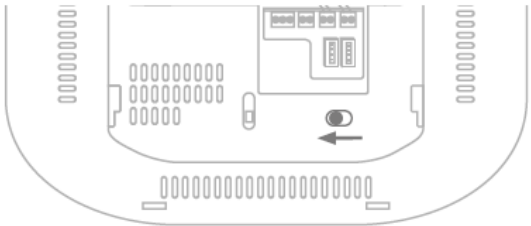
Lösen Sie die Befestigungsschraube (unten Mitte) und ziehen die Rückplatte vom Zentralgehäuse.



Achtung: Achten Sie darauf, dass die Spannungsversorgung (Netzleitung) ausgeschaltet und isoliert ist!

1. Führen Sie alle erforderlichen Anschlussleitungen durch die Kabeldurchführung der Montageplatte der Zentrale.
2. Befestigen Sie anschließend die Montageplatte an der Wand.

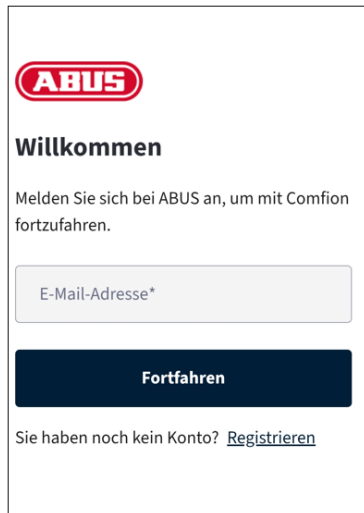
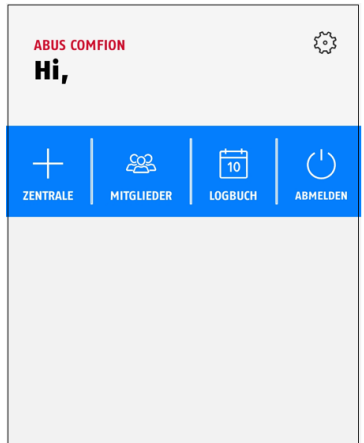


Hängen Sie die Haltersicherungen der Zentrale (2 Haltekabel) in die Vorrichtungen der Rückplatte ein.							
Führen Sie die Anschlussleitungen in die Zentrale ein • Schließen Sie das Netzkabel an die L/N Klemme an. • Schließen Sie das Ethernet Kabel an die RJ45 Buchse an • Schließen Sie gegebenenfalls das Bus-Kabel sowie die verdrahteten Melder usw. an die entsprechenden Klemmen an. • Nähere Details zum Anschluss verdrahteter Melder und Bus-Geräte finden Sie im Kapitel 3.2.5 und 3.2.6 Fixieren Sie alle Anschlussleitungen mit den Zugentlastungen.							
Stecken Sie gegebenenfalls eine Micro-SD Karte (max Kapazität 512 GB) und und/ oder eine SIM-Karte (Nano-SIM) in die vorgesehenen Kartenschächte bis diese hörbar einrasten. (Karten nicht im Lieferumfang)  Hinweis Formatieren Sie Ihre SD-Karte vor dem Einlegen im Format exFAT oder NTFS.							
Schalten Sie jetzt die Spannungsversorgung ein. Die Zentrale führt jetzt den Boot-Vorgang durch.							
Schalten Sie den Batterieschalter auf „ON“ Nach Abschluss des Boot-Vorgangs leuchten die Status-LEDs wie folgt:    <table border="0"> <tr> <td>Power LED:</td> <td>Grün (Netzspannung)</td> </tr> <tr> <td>Internet-LED:</td> <td>Grün (blinken) (Online & Admin nicht registriert)</td> </tr> <tr> <td>Netzwerk-LED:</td> <td>Grün (LAN)</td> </tr> </table>	Power LED:	Grün (Netzspannung)	Internet-LED:	Grün (blinken) (Online & Admin nicht registriert)	Netzwerk-LED:	Grün (LAN)	
Power LED:	Grün (Netzspannung)						
Internet-LED:	Grün (blinken) (Online & Admin nicht registriert)						
Netzwerk-LED:	Grün (LAN)						

3.2. Inbetriebnahme des Systems

3.2.1. Einrichtung via App & Abschluss der Hardware-Vorbereitungen

 Hinweis	Die Erstinbetriebnahme der Comfion Pro Zentrale und damit die Verknüpfung zum Fachpartnerportal und dem dazugehörigen Errichter muss per App stattfinden.
--	--

Laden Sie sich die Comfion App aus Ihrem App-Store auf Ihr Smartphone bzw. Tablet (iOS oder Android) Folgen Sie den Anweisungen in der App bis Sie zur Login-Seite gelangen	
Melden Sie sich mit ihren ABUS Single Sign-On Daten an (Partner-Zugang) Falls Sie keinen Zugang besitzen, erstellen Sie sich unter „Registrieren“ ein kostenloses Konto.	
Nach dem Login sehen Sie die Zentralenübersicht. Fügen Sie über den Plus-Button eine neue Zentrale hinzu.	

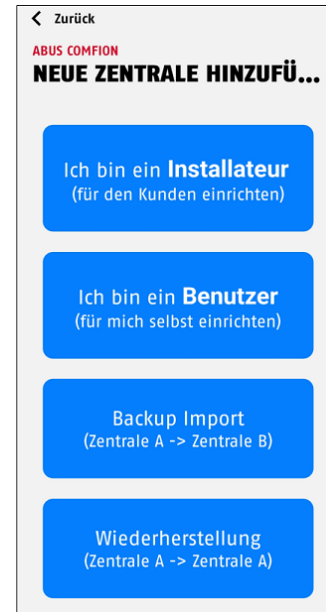
Wählen Sie, wenn Sie die Anlage für einen Kunden in Betrieb nehmen **„Ich bin ein Installateur“**. Dadurch wird ihr Nutzer in der Rolle Installateur angelegt.

Wenn Sie die Anlage für sich selbst installieren, wählen Sie **„Ich bin ein Benutzer“**. Hiermit werden Sie als Rolle Admin mit Installateur- & Admin-Rechten angelegt.



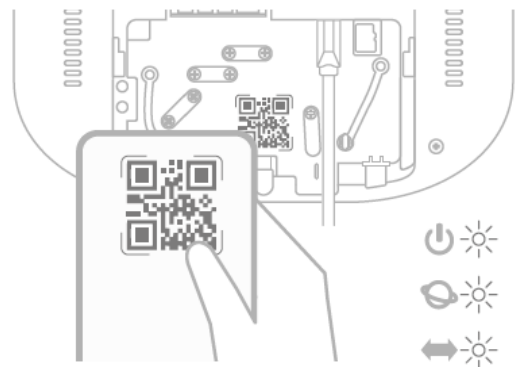
Als Installateur können Sie Benutzer anlegen, verlieren diese Berechtigung allerdings mit Einladen eines Admin-Benutzers (Besitzer). Weitere Details finden Sie in **Kapitel 4.1**. (Benutzerrollen) und **Kapitel 4.2** (Inbetriebnahme)

Weitere Details zum „Backup Import“ und zur „Wiederherstellung“ finden Sie im **Kapitel 6.1.7** (Backup)

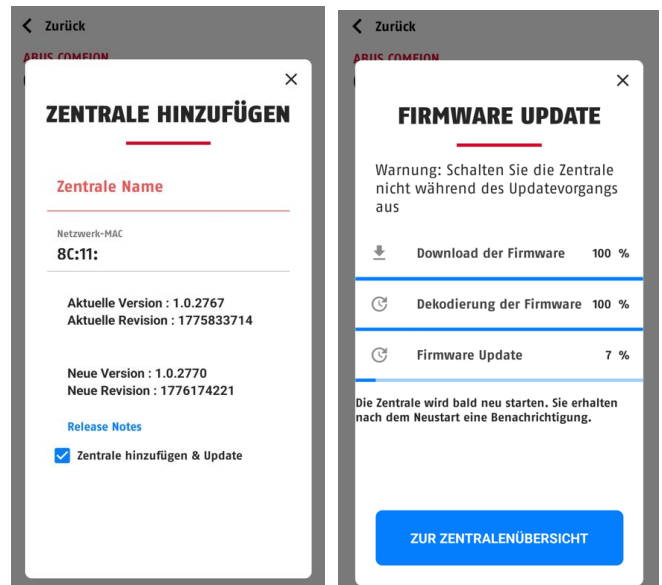


Achten Sie darauf, dass die Zentrale mit dem Internet verbunden ist.

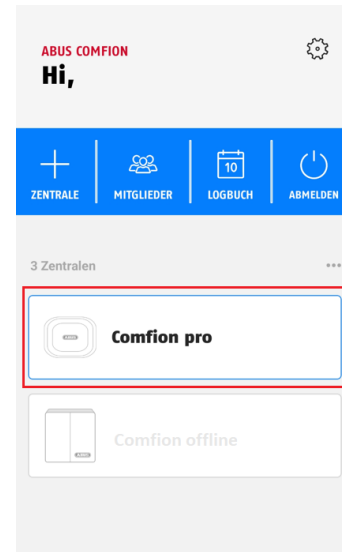
Sobald die Status-LED „Internet“ grün blinkt, können Sie den Pairing Vorgang in der App starten. Scannen Sie hierfür den QR-Code mit der Aufschrift „Pairing-Code“



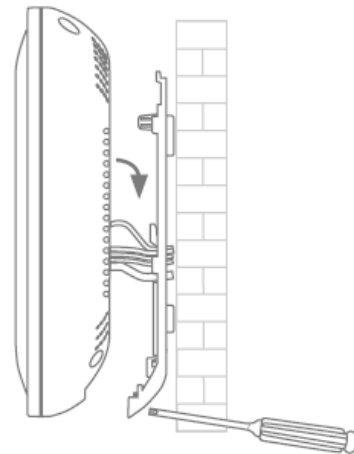
Vergeben Sie einen Zentralenamen und bestätigen Sie diesen. Die Anlage wird nun ein Firmware-Update starten, bevor Sie auf die Anlage zugreifen können. Das Firmware-Update kann einige Minuten dauern und beinhaltet einen Neustart der Zentrale. Während des Updates blinkt die Power-LED gelb.



Nach dem Neustart der Zentrale ist die Zentrale in der Zentralenübersicht nicht mehr ausgegraut und kann durch Klick hierauf aufgerufen werden.



Lösen Sie die Haltesicherung von der Rückplatte und legen die Haltekabel nach innen. Setzen Sie die Zentrale in die Rückplatte ein, schieben Sie sie nach unten und schrauben Sie die Zentrale an der Rückplatte fest.



Hinweis

Nach Installation und Inbetriebnahme löst das Entfernen der Zentrale von der Wandhalterung, sowie das Öffnen des Gehäusedeckels einen Sabotagealarm aus. Führen Sie notwendige Arbeiten an der Hardware nur dann aus, wenn der Wartungsmodus aktiviert ist (*Zentralen-Konfiguration* -> *Sicherheitseinstellungen*)

3.2.2. Dashboard (nach Erst-Anmeldung)

Kopfleiste:

- ☰ Konfiguration & Benutzer-Einstellungen
- Installateur Benutzer-Rolle (nur Installateur)
- 🕒 Firmware-Update (sofern vorhanden)
- 🔔 Panik-Alarm auslösen

Dashboard / Funktionsbereich

- Hotkey-Schaltflächen (sofern eingerichtet)
- Kamera-Vorschaubilder (sofern eingerichtet)
- Übersicht Teilbereiche (Innenbereich, Außenhaut ist voreingestellt & kann um weitere Bereiche erweitert werden siehe: 3.2.3 Bereiche)
 - Klick auf ▼ zeigt zugewiesene Komponenten & deren Status an (sofern eingerichtet)

Navigationsleiste

- Räume (& Komponentenliste) siehe 3.2.4 u. 3.2.5
- Szenarien (Szenen und Automationen) siehe 6.4
- Alarmmodi (Schloss-Symbol) – siehe 3.2.8
- Logbuch (Ereignis-Liste & Filterfunktion)
- Zentralen (Übersicht) – siehe 6.3

Eine fertig konfigurierte Dashboard-Ansicht finden Sie in **Kapitel 6.2 Dashboard**

3.2.3. Bereiche

Bereiche geben Ihnen die Möglichkeit, Ihr zu überwachendes Objekt aufzuteilen und somit auch differenziert scharf- und unscharf schalten zu können. Im Zusammenspiel mit den Alarmmodi können Sie Bereiche gemeinsam oder getrennt schalten.

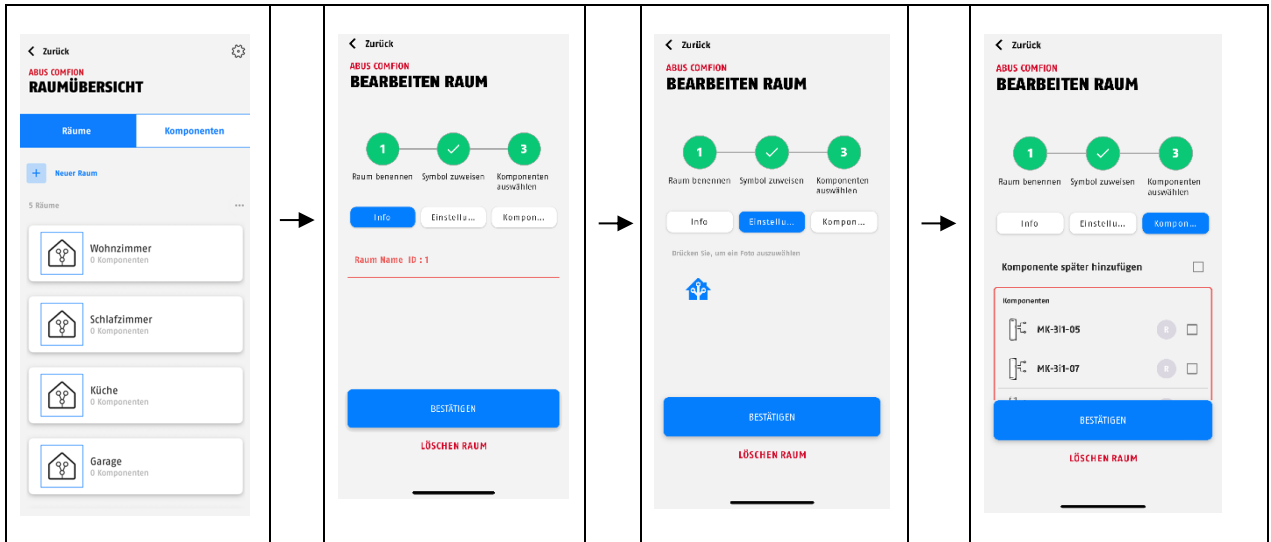
Im Werkzustand verfügt die Anlage über zwei Bereiche – die Außenhaut und der Innenbereich. Sie können diese Bereiche durch einen langen Druck hierauf bearbeiten.

Durch Klick auf den Button „Bereich hinzufügen“ können Sie weitere Bereiche anlegen.

3.2.4. Räume

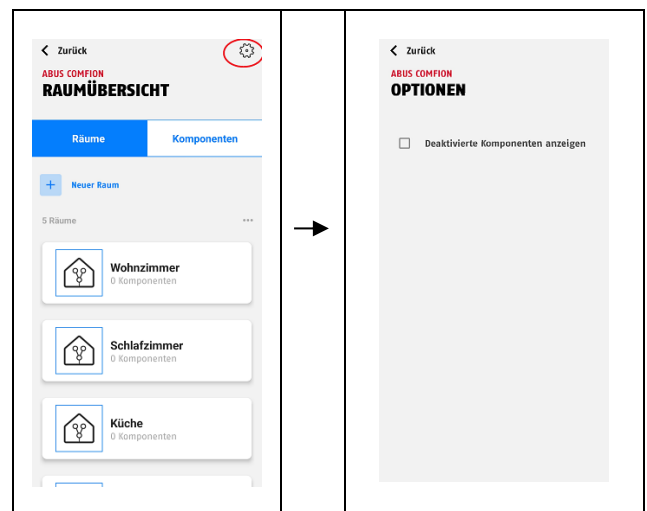
Vom Dashboard aus gelangen Sie über die Navigationsleiste in den Bereich „Räume“ zur Konfiguration von Räumen und Komponenten. Das Comfion Pro Funk-Sicherheitssystem bietet Ihnen die Möglichkeit, Ihre Komponenten Räumen zuzuweisen. Dies dient zur einfacheren Identifikation von Komponenten und hat keine funktionellen Eigenschaften. Räume sind keinen Bereichen zugeordnet, was bedeutet Sie können in einem Raum Komponenten aus verschiedenen Bereichen haben.

Im Werkzustand verfügt die Anlage über einige vordefinierte Räume. Sie können diese Räume frei bearbeiten, oder auch komplett löschen. Sie können diesen Bereich durch einen langen Druck hierauf bearbeiten.



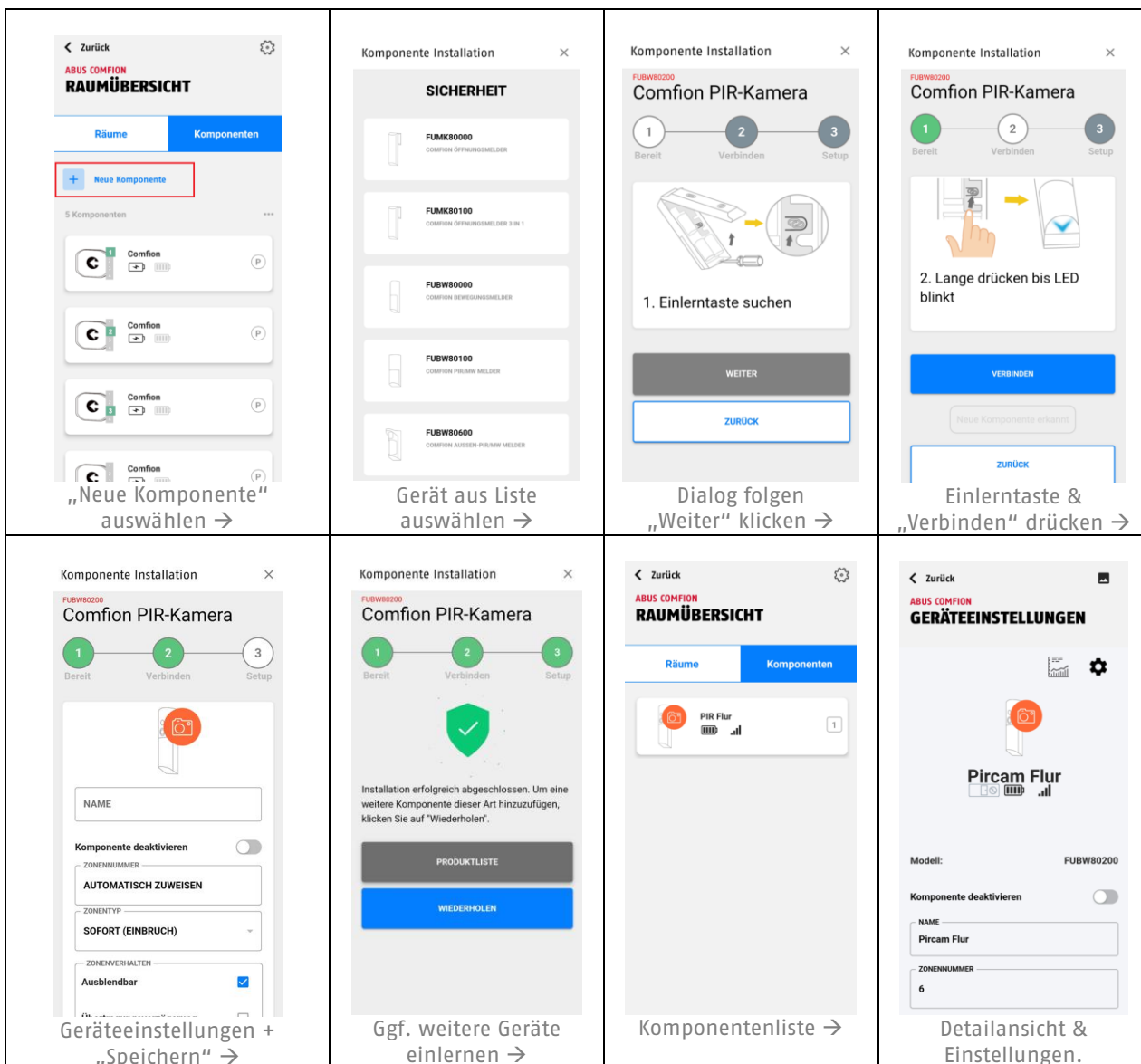
In der Raumübersicht kann über das Zahnradsymbol im rechten oberen Bildrand die Einstellung „Deaktivierte Komponenten anzeigen“ aktiviert oder deaktiviert werden. (deaktiviert ist voreingestellt)

Wenn diese Option aktiviert ist, werden deaktivierte Komponenten im Dashboard unter den Räumen und in der Komponentenliste angezeigt.



3.2.5. Komponenten

Von der Raumübersicht gelangen Sie in die Komponentenansicht. Durch Klick auf „Neue Komponente“ können sie Ihre Comfion-Komponenten dem System hinzufügen.



Durch Klick auf eine bereits eingelernte Komponente können Sie diese bearbeiten und folgende Geräteeinstellungen anpassen:

Komponente deaktivieren	AUS: (Voreinstellung): Gerät normal in Funktion EIN: Gerät wird deaktiviert (keine Funktion)
Name	Namensvergabe der Komponente
Zonenummer	Vergabe der Zonenummer (geschieht automatisch durch System)
Zonentyp	- Eingang -> löst eine Eingangsverzögerung aus, nach Ablauf wird ein Einbruchalarm ausgelöst - Ausgang -> kann während der Ausgangsverzögerung offen sein, funktioniert nach Scharfschaltung wie eine Sofort-Zone - Eingang/Ausgang -> nutzt eine Ein- & Ausgangsverzögerung - Eingang folgend -> Melder reagiert wie eine Sofort-Zone, außer wenn davor eine Eingangsverzögerung ausgelöst wurde. Dies kann in den Sicherheitseinstellungen auf denselben Bereich begrenzt werden. - Sofort (Einbruch) -> löst bei scharfer Anlage einen Einbruchalarm aus - Perimeterwarnung -> Zonentyp für Außenmelder. Löst das Event, samt

	<i>Logeintrag und Benachrichtigung aus. Keine akustische Alarmierung.</i> • Sofort (Überwacht) -> <i>funktioniert bei scharfer Anlage wie die Sofort-Zone; Bei unscharfer Anlage wird bei Auslösung eine Benachrichtigung versendet</i> • 24 Std. Einbruchalarm -> <i>Einbruchalarm unabhängig vom Anlagenzustand</i> • 24 Std. Wasseralarm -> <i>Wasseralarm unabhängig vom Anlagezustand</i> • 24 Std. Feuer -> <i>Feueralarm unabhängig vom Anlagezustand</i> • 24 Std. Sabotage -> <i>Sabotagealarm unabhängig vom Anlagenzustand</i> • Verschlussüberwachung -> <i>Offene Zone verhindert die Scharfschaltung, löst aber keinen Alarm aus</i>
Eingangszeit/Ausgangszeit	• Für Zonentyp Eingang, Ausgang und Eingang/Ausgang kann eine Verzögerungszeit in Sekunden eingestellt werden (5 bis 180 Sekunden) • Voreinstellung 10 s (Eingangsverzögerung) / 30 s (Ausgangsverzögerung)
Zonenverhalten	• Ausblendbar: <i>Wenn die Zone bei Scharfschaltung ausgelöst ist, haben Sie die Möglichkeit diese auszublenden</i> • Übertragungsverzögerung: <i>Wenn dieser Punkt aktiviert wird, wird die Meldung von Zonenalarmen um die programmierte Zeit verzögert.</i> • Auslösung Sirene: <i>Dieser Melder steuert die in den Bereich integrierten Sirenen an</i>
Bereich	• Gerät kann einem oder mehreren Bereichen zugewiesen werden. -> Diese Zuweisung bewirkt in Verbindung mit dem Zonentyp die Auslösung eines Alarms.
Raum	• Gerät kann einem Raum zugewiesen werden. • „Später zuweisen“ heißt, dass das Gerät keinem Raum zugewiesen wurde.
Gehtest starten (Bewegungsmelder)	• Klick auf „Gehtest starten“ startet ein Zeitfenster von 1:00 Minute in dem das Gerät ausgelöst werden soll. • Der Gehtest kann durch Klick auf „Stopp“ abgebrochen werden. • Bei Auslösung startet das Zeitfenster (Stummzeit des Melders) erneut. • Bei Mehrfachsensoren (z.B. PIR + Mikrowelle) können Sensoren einzeln oder zusammen getestet werden.
Signalstärketest starten (Funk-Komponenten)	 Testen Sie die Signalstärke vor Montage der Komponente und verwenden im Zweifelsfall einen Repeater. Eine Übersicht zur Bewertung der Signalstärke finden Sie im Kapitel 6.11 Hinweis • Klicken Sie auf „Signalstärketest starten“ und lösen Sie das Gerät aus. • Bei Mehrfachsensoren (z.B. PIR + Mikrowelle) kann jeder Sensor einzeln getestet werden.
Kamera-Funktionen (nur Kameras)	• MotionAlarm Aus/An (Voreinstellung Aus), „An“ löst einen Alarm aus, sofern die Kamera einem Bereich zugewiesen wurde.
Speichern	• Durch Klick auf „Speichern“ übernehmen Sie Einstellungs-Änderungen.

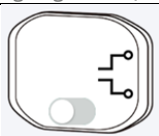
 Hinweis	Ist ein Melder auf den Zonentyp Ausgang oder Ein/Ausgang programmiert, prüft die Anlage bei Scharfschaltung den Melder-Status erst nach Ablauf der Verzögerungszeit. - Ist der Melder nach Ablauf der Zeit nicht bereit, und „Ausblendbar“ ist aktiviert, wird der Melder nach der Verzögerungszeit automatisch ausgeblendet und das System scharf geschaltet. - Ist der Melder nach Ablauf der Zeit nicht bereit, und „Ausblendbar“ ist deaktiviert, wird das System nicht scharf geschaltet.
---	--

 Hinweis	Eine detaillierte Übersicht der Symbole in der Komponentenliste finden Sie in Kapitel 6.7 (Symbolerklärung)
---	---

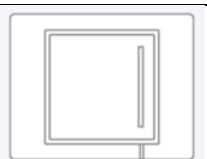
3.2.6. Komponenten-Einstellungen

In den Komponenten-Einstellungen & rechts oberhalb des Geräte-Icons können durch Klick auf das Zahnrad  Detailsinstellungen an der Komponente vorgenommen werden. Weitere Details entnehmen Sie der Installationsanleitung der jeweiligen Komponente. Im Folgenden finden Sie die Einstellungen für die Comfion Pro Zentrale FUAA85000, das Comfion Pro BUS-WLX-Modul BUM080000, und IP-Kameras

Comfion Pro Zentrale FUAA85000

Symbol	Bezeichnung	Einstellmöglichkeit	Erklärung
 (je Eingang d.h. 1, 2, 3, 4)	Draht-Modus	2-Draht CC / EOL / DEOL (Voreinstellung CC)	Verdrahtungsart der Meldergruppen-Eingänge
	NC od. NO	Normally Open / Normally Closed (Voreinstellung: NO)	Ruhezustand des Relais, d.h. geöffnet oder geschlossen
	Logo Display	Immer Aus / Immer An / Aufleuchten (Voreinstellung An)	Schaltet die Logo-Staus Beleuchtung dauerhaft Aus, dauerhaft An, oder bei Statusänderung 10 Sek. An (Aufleuchten)
	Scharf Farbe Unscharf Farbe Teilscharf Farbe	Farb-Matrix	Anpassung der Leuchtfarbe durch Klick auf das Farbsymbol

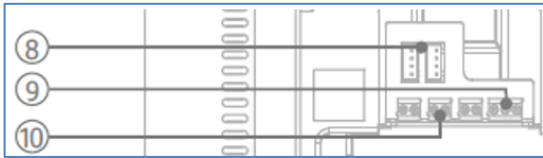
Comfion Pro WLX Pro Modul BUM080000 und WLX Pro Schließmedien

Symbol	Bezeichnung	Einstellmöglichkeit	Erklärung
 (BUS-WLX-Modul)	Auf Werkseinstellungen zurückstellen	Ausführen	Rückstellung des WLX-Pro Funkmodul. Hinweis: alle Schließzylinder u. Wandler müssen danach neu eingelernt werden! (das BUS-WLX-Modul bleibt weiterhin eingelernt!)
 Schließzylinder (Access / Intrusion)	Supervisionszeit	4 – 720 Min (Voreinstellung: 720)	Regelmäßige Überprüfung der Funk-Kommunikation im eingestellten Intervall.
	Zwangsläufigkeit (nur Access)	Aus / An (Voreinstellung: An)	Bei Stellung auf „An“ wird bei scharfgeschalteter Comfion Pro kein Zutritt gewährt.
	Öffnungs-Zeit	6 Sek / 12 Sek (Voreinstellung 6 Sek)	Definiert den eingekoppelten Zeitraum des Zylinders zur Öffnung des Türschließers
 Wandler (Access / Intrusion)	Supervisionszeit	4 – 720 Min (Voreinstellung: 720)	Regelmäßige Überprüfung der Funk-Kommunikation im eingestellten Intervall.
	Zwangsläufigkeit (nur Access)	Aus / An (Voreinstellung: An)	Bei Stellung auf „An“ wird bei scharfgeschalteter Comfion Pro kein Zutritt gewährt.
	Öffnungs-Zeit	6 Sek / 12 Sek (Voreinstellung 6 Sek)	Definiert den eingekoppelten Zeitraum des Zylinders zur Öffnung des Türschließers

IP-Kameras

Symbol	Bezeichnung	Einstellmöglichkeit	Erklärung
 (IP-Kamera)	Kamera Funktion „Motion Alarm“	Aus/An (Voreinstellung: Aus)	Bewegungserkennung zur Alarm-Auslösung verwenden. Hinweis: Es sind weitere Einstellungen u.a. in der Kamera Konfiguration nötig. Siehe Kapitel 3.4.4

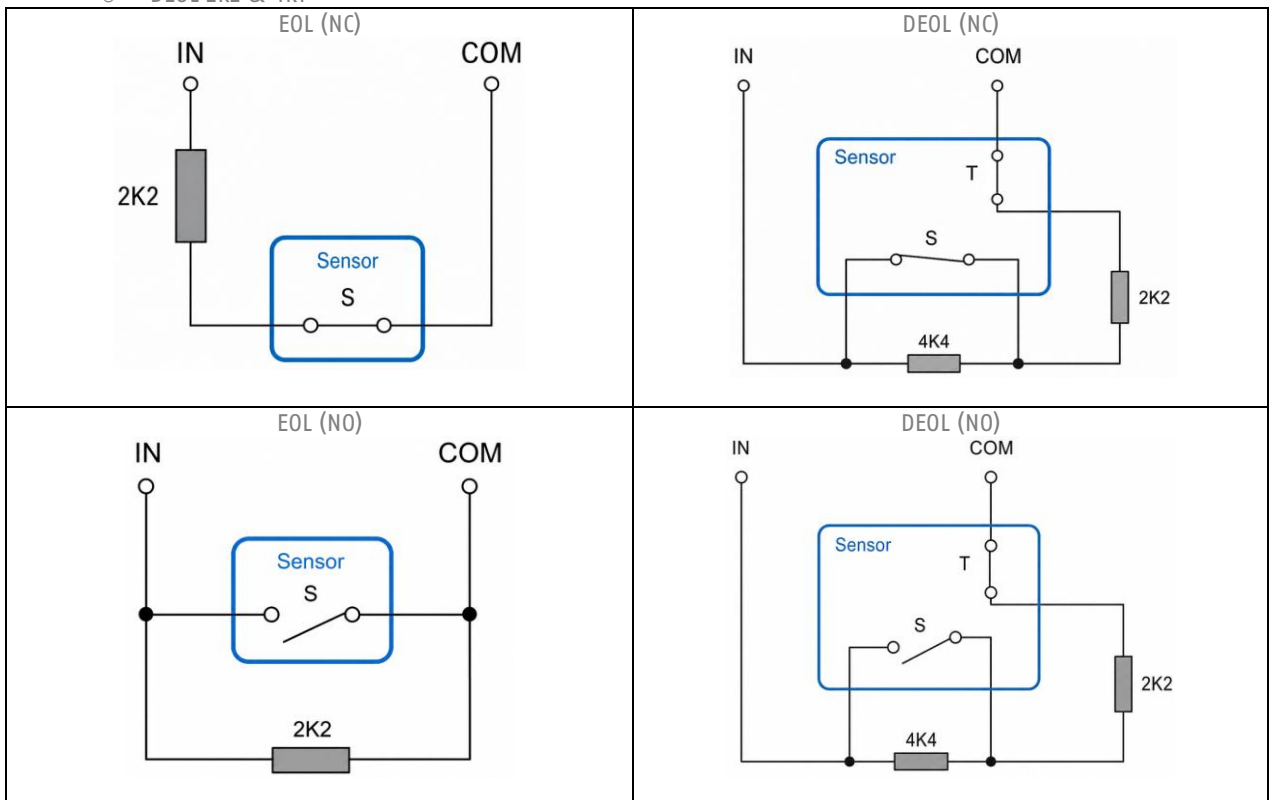
3.2.7. Hinweise zur Verdrahtung (Eingänge/Ausgänge/BUS)



Die Comfion Pro Zentrale verfügt über mehrere Anschlussmöglichkeiten für bis zu 4 verdrahtete Melder (8), einen Relais-Ausgang (9) und eine RS485 BUS-Schnittstelle (10).

Drahtmelder-Eingänge

- Verwenden Sie die mitgelieferten 30cm Adapterkabel mit offenen Kabelenden. Die Kabelpaare sind je Eingang farblich markiert.
- In den Geräteeinstellungen der Comfion App stellen Sie je Eingang den Draht-Modus (2-Draht-CC, EOL oder DEOL) sowie die Ruhestellung NO bzw. NC ein.
- Für die überwachte Widerstandsverdrahtung sind folgende Widerstandswerte fest vorgegeben:
 - EOL: 2k2
 - DEOL 2k2 & 4k7



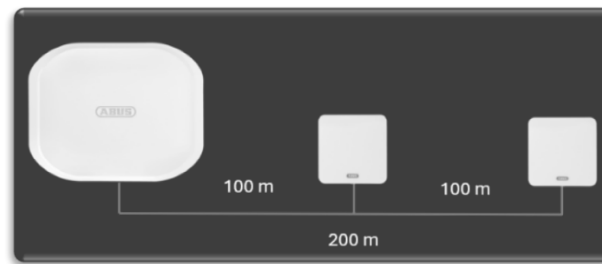
Relais-Ausgang

- Der Relaisausgang ist spannungsfrei. Schließen Sie den Ausgang an Masse und je nach Bedarf an die Klemme NC (Öffner) oder NO (Schließer) an. max. 30V DC & max. 1.6A

RS485 BUS-Schnittstelle

- Die Comfion Pro besitzt eine 4-Draht RS485 BUS Schnittstelle (GND / +V / B / A), 13.0V zum Anschluss von bis zu 2 BUS-Teilnehmern (**Comfion Pro BUS-WLX-Modul BUM080000**)
- Sie können Geräte entweder in Reihe oder Parallelanordnung mit dem Anschluss der Comfion Pro Zentrale verbinden.
- Die maximale Leitungslänge beträgt 200m und kann bei Verwendung von 2 Geräten flexibel aufgeteilt werden:

- Beispiel:



- Kabel-Empfehlung: Twisted-Pair-Kabel (geschirmt u. verdreht) z.B.: RS485/DMX Kabel oder CAT5e bzw. CAT6 Kabel.



Wichtig

Halten Sie bei der Installation der Comfion Pro Zentrale und dem BUS-WLX-Modul sowie zu anderen elektrischen Geräten, Antennen und Metallen einen Mindestabstand von 1.5 Meter ein, um Störungen in der Funk-Kommunikation (z.B. Verzögerungen oder Signalverlust) zu vermeiden!

3.2.8. Alarmmodi

Das Comfion Pro Funk-Sicherheitssystem arbeitet mit sogenannten „Alarmmodi“, welche den Kern des Systems bilden. Es handelt sich hierbei um scharf- und unscharf- schaltbare Verknüpfungen zwischen Bereichen und Benutzern.

In einem Alarmmodus definieren Sie, welcher Benutzer welchen Bereich mit diesem scharf- oder unscharf schaltet. Hiermit lassen sich alle möglichen Szenarien der Scharf- und Unscharfschaltung abbilden.

In der Praxis führt ein Benutzer beim Scharf- oder Unscharf-schalten in Wirklichkeit einen Alarmmodus aus.

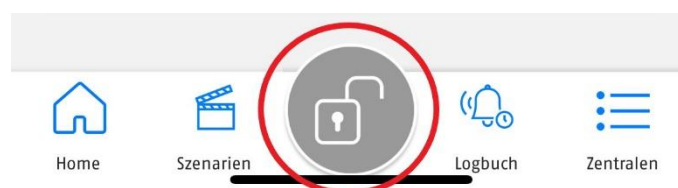


Hinweis

Das Comfion Pro Funk-Sicherheitssystem hat im Werkszustand drei vorkonfigurierte Alarmmodi: „Gesamt Scharf“, „Außenhaut scharf“ und „Gesamt unscharf“.

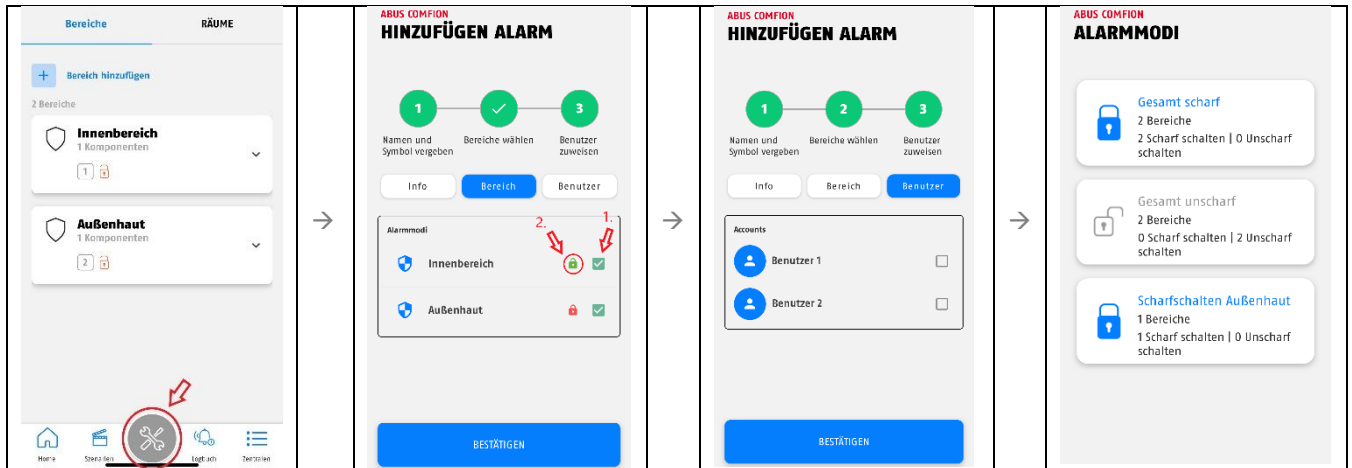
Ausführung eines Alarmmodus

- Der im unteren Bildrand, mittige Button zeigt den aktuellen Status der Anlage (scharf, unscharf, teilscharf oder Wartungsmodus)
- Durch Drücken auf den Button werden Ihnen die vorhandenen Alarmmodi angezeigt und Sie können einen der dort angezeigten Schaltbefehle ausführen.



Alarmmodi erstellen oder bearbeiten

1. Sie öffnen die Verwaltung der Alarmmodi, indem Sie im Dashboard auf den Status Button klicken und daraufhin auf das Einstellungssymbol (Zahnrad) im rechten oberen Bildrand.
2. Klicken Sie anschließend auf „Alarmmodus hinzufügen“ oder bearbeiten Sie einen bestehenden Alarmmodus durch langen Druck auf diesen.
3. Nachdem Sie den Namen für den Alarmmodus vergeben haben, wählen Sie die Bereiche UND die Art der Schaltung aus (Scharf od. Unscharf). Zum Ändern der Art der Schaltung, klicken Sie auf das Symbol.
4. Wählen Sie im nächsten Schritt die Benutzer, die die Berechtigung zur Schaltung dieses Alarmmodus haben sollen.
5. Nach Abschluss erscheint der Alarmmodus in Ihrer Übersicht und kann benutzt werden.



3.3. WLX Pro Installation & Einlernen

Führen Sie die Montage und Verdrahtung des **Comfion Pro BUS-WLX-Modul** wie in der Produkthanleitung und in **Kapitel 3.2.7** beschrieben durch.

 Hinweis	Zur Einrichtung und Konfiguration des Comfion Pro BUS-WLX-Modul und weiterer WLX Pro Schließmedien benötigen Sie die mitgelieferte System-Karte und Reset-Karte. Bewahren Sie diese Karten sorgsam auf!
---	--

- Lernen Sie das Comfion Pro BUS-WLX-Modul als „Neue Komponente“ in das System ein. Gehen Sie wie in **Kapitel 3.2.5** beschrieben vor und folgen den Einlern-Anweisungen.
- Lernen Sie anschließend den WLX Pro Schließzylinder oder WLX Pro Wandler ein.
- Im Einlernvorgang (Schritt 2) werden Sie aufgefordert den WLX Pro Schließzylinder oder WLX Pro Wandler einem Comfion Pro BUS-WLX-Modul zuzuordnen. Wählen Sie das Modul aus, welches am nächsten zum Zylinder/Wandler platziert ist.

 Hinweis	Nach Einlernen des ersten Schließzylinders bzw. Wandlers werden Sie aufgefordert, die beiliegende Reset-Karte einzulernen. Die eingelernte Reset-Karte ist im Comfion System fest als Fallback-Medium hinterlegt und wird benötigt, um einen Zylinder zurückzusetzen. Weitere Details finden Sie im Kapitel 6.1.8 WLX-Informationen und im Kapitel 3.2.6 Komponenten-Einstellungen
--	---

 Wichtig	Folgende Geräte können zurzeit in die Comfion Pro eingelernt werden: - WLX Pro Zylinder (Access/Intrusion) Typ: LA-A, LA-I - WLX Pro Wandler (Access/Intrusion) Typ: WR-A-S-O, WR-I-S-O Der WLX Pro Repeater und weitere Schließmedien werden zurzeit nicht unterstützt.
--	---

- RFID-Tags (NFC-Tags) lernen Sie in den Benutzereinstellungen ein bzw. kann nach Übergabe direkt durch den Besitzer (Administrator) durchgeführt werden. Weitere Details finden Sie im **Kapitel 4.4.1 Zugriffsrechte**.

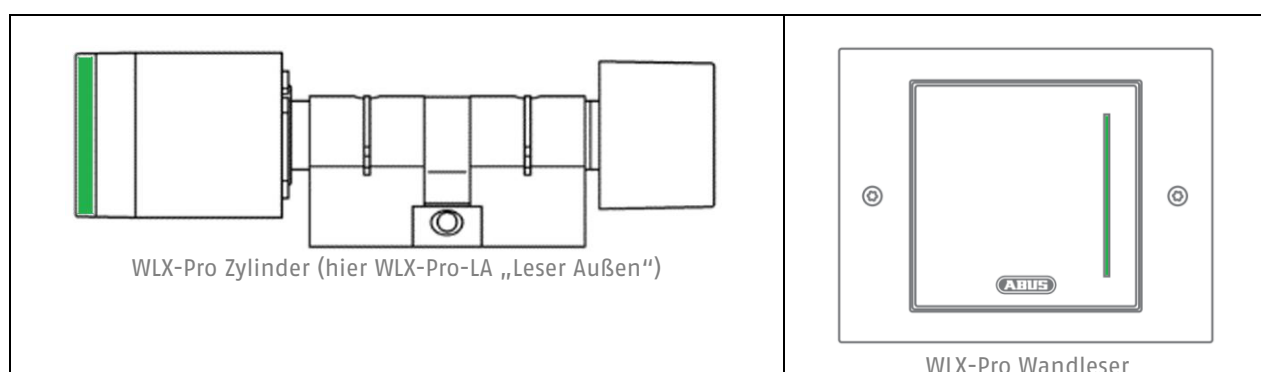
 Wichtig	Wir empfehlen, mindestens einen NFC-Tag als Fallback-Medium einzurichten, damit im Notfall (z.B. Ausfall der Funkverbindung oder längerer Ausfall der Stromversorgung) berechtigten Personen Zutritt gewährt werden kann. Weitere Details finden Sie in im Kapitel 4.4.1 Zugriffsrechte
--	---

3.3.1. Installation, Konfiguration und Benutzung der WLX Pro Zylinder und Wandleser

Details zur Installation von WLX-Pro Schließzylindern / WLX-Pro Wandleser finden Sie in den jeweiligen Installationsanleitungen der Produkte. Diese stehen online auf abus.com im Downloadbereich der Produkt-Seite bereit:

- WLX-Pro-Schließzylinder: <https://abus.com/products/WLX-Pro-LA>
- WLX-Pro-Wandleser: <https://www.abus.com/products/ACSE00026>

Der WLX-Pro Schließzylinder sowie der WLX-Pro Wandleser signalisieren folgende Zustände per LED-Blinkfolge:



Signale		Beschreibung
Inbetriebnahme & Initialisierung		
	1 x grün, 1 x rot, 1 x grün, 1 x rot	Initialisierung nach Batterie-Einlegen
	1 x grün (lang)	Zylinder ist nicht eingelernt (& dauerhaft eingekoppelt)
	2 x rot	Kommunikation mit Außenknopf vorhanden
	2 x grün	Kommunikation mit Comfion Pro BUS WLX Modul vorhanden.
Einlernen/Auslernen/Reset (im Einlernprozess (ab FW 2.01) blinkt der Zylinder zyklisch grün)		
	2 x grün	Einlernen erfolgreich
	3 x rot	Auslernen erfolgreich
	1 x rot	Einlernen fehlgeschlagen
	10 x rot	Systemkarte wurde präsentiert (Einlernen/Auslernmodus), während Blinkfolge Reset-Karte vorhalten setzt das Gerät zurück.
Im Betrieb		
	1 x grün	Durch ein kurzes grünes Blinken wird das Lesen und Senden des Schließmediums 1x grün signalisiert.
	1 x rot	Keine Funkverbindung zum Comfion Pro BUS-WLX-Modul
	1 x rot (lang)	Die Comfion Pro wurde scharfgeschaltet (Quittierung)
	1 x grün (lang)	Die Comfion Pro wurde unscharf geschaltet (Quittierung)
	1 x rot, 2x grün	Funkausfall / berechtigtes Fallback (Vorgang insgesamt 3x wiederholen)

	2 x grün	Zutritt gewährt
	3 x rot	Zutritt verweigert, kein berechtigter Zutritt
	3 x rot, 2 x grün	Batteriewarnung (bis FW 2.07)
	5 x rot, 2 x grün	Batteriewarnung (ab FW 2.09) Zylinder koppelt ca. eine Sekunde verzögert ein
	1 x rot, 2 x grün	Batteriewarnung Stufe 2: keine Signalisierung auf Personentransponder, Fallback kann noch 3x Zutritt gewähren → Fallback Medium nutzen wie bei Funkausfall
	4 x rot	Funkausfall & unberechtigter Fallback-Transponder wurde präsentiert
	6 x rot	- Kein Scharfschalten möglich, oder - Kein Unscharf schalten möglich

3.3.2.WLX Pro Funktionen – Fernöffnung und Büromodus

Fernöffnung

Mithilfe der Fernöffnung (auch Remote-Freigabe) kann der WLX-Pro Schließzylinder für einen festgelegten Zeitraum (maximal 180 Sekunden) eingekoppelt werden. Die Konfiguration erfolgt in der Comfion App (bzw. Webinterface) als Szene bzw. Automation.

- Die Szenen-Konfiguration ergänzt eine Hotkey-Schaltfläche im Dashboard der Comfion App
- Weitere Details zur Konfiguration finden Sie im **Kapitel 6.4 Automationen & Szenen**
- Nach Ausführung der Fernöffnung muss am WLX-Pro Schließzylinder der Außenknopf gedreht werden, um eine Öffnung durchzuführen.

 Hinweis	Bitte unterscheiden: - Die Dauer der Remote-Freigabe ist der Zeitraum, in der der Zylinder eingekoppelt werden kann - Nach Drehen des Außenknopfes wird der Zylinder gemäß definierter Öffnungszeit (6 oder 12 Sekunden) eingekoppelt.
--	---

 Wichtig	Fernöffnung ist nur im unscharf-geschalteten Zustand der Comfion Pro möglich.
--	---

Büromodus (Permanent Zutritt)

Ein Zylinder, bei dem der Büromodus eingeschaltet ist, erlaubt es die Tür ohne NFC-Tag durch Drehen des Zylinderknopfes zu öffnen. Die Konfiguration erfolgt in der Comfion App (bzw. Webinterface) als Szene bzw. Automation.

- Die Szenen-Konfiguration ergänzt eine Hotkey-Schaltfläche im Dashboard der Comfion App (Sie benötigen 2 Szenen um den Büromodus ein-, und auszuschalten)
- Die Automations-Konfiguration ermöglicht das Ein/Ausschalten des Büromodus zum Beispiel durch einen Zeitplan: wenn Zeit x → dann einschalten ... wenn Zeit Y → dann ausschalten
- Weitere Details zur Konfiguration finden Sie im **Kapitel 6.4 Automationen & Szenen**
- Bei aktiviertem Büromodus muss am WLX-Pro Schließzylinder der Außenknopf gedreht werden, um eine Öffnung durchzuführen.

 Wichtig	Öffnung per Büromodus ist nur im unscharf-geschalteten Zustand der Comfion Pro möglich. Ein aktivierter Büromodus wird für die Dauer der Scharfschaltung unterbrochen!
	Programmieren Sie diese Funktion nur, wenn der Betreiber die Auswirkungen kennt und ihnen diese schriftlich bestätigt hat.

3.4. Kameras (NVR)

Mithilfe des Integrationsprotokolls ONVIF lassen sich diverse Kameras aus der ABUS Professional Line in das Comfion Pro Funk- Sicherheitssystem einbinden. Alternativ ist die Einbindung per RTSP möglich. In die Comfion Pro können Sie bis zu 8 Kameras einbinden und diese bei Event, bei scharfer Anlage oder dauerhaft (24/7) aufzeichnen lassen (auf Micro-SD-Karte oder SSD).

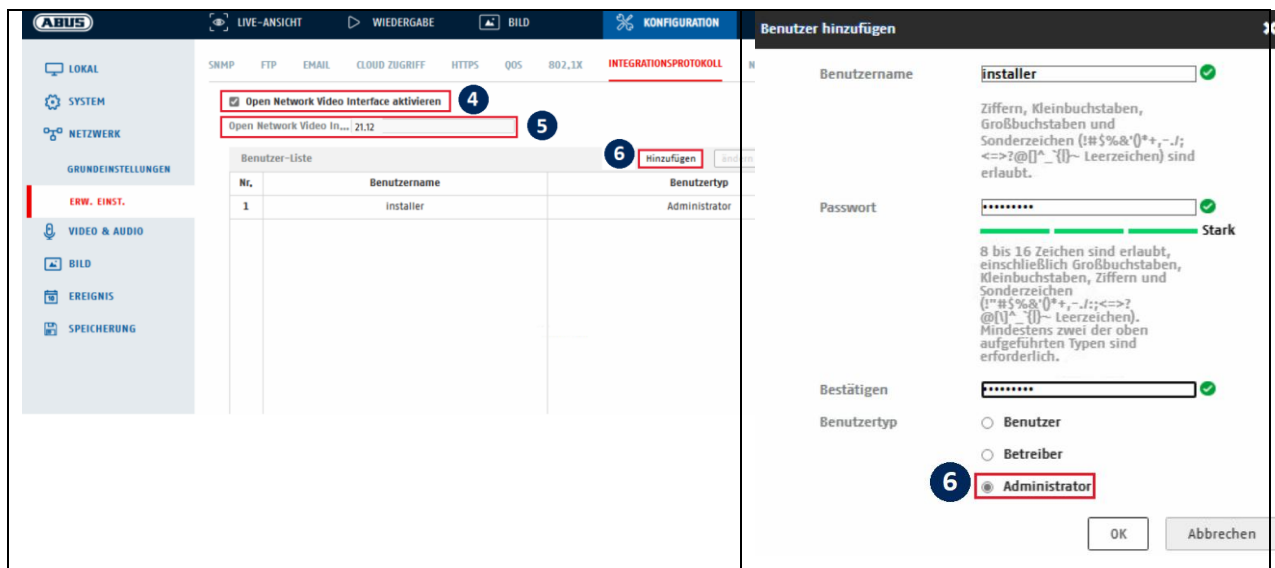
 Hinweis	Zur Daueraufzeichnung (24/7) wird ein SSD-Datenspeicher in der Zentrale benötigt.
--	---

3.4.1. Einbinden von Kameras per ONVIF

Das Comfion Pro System sucht in der Werkseinstellung selbstständig nach ONVIF-Kameras im Netzwerk und fügt diese dem System hinzu. Die automatische Kamerasuche können Sie unter der Kameraübersicht in den Kamera Einstellungen deaktivieren.

Gehen Sie beim Einbinden der Kameras wie folgt vor:

1. Binden Sie die Kamera in das gleiche Netzwerk wie die Comfion Pro ein.
2. Öffnen Sie die Software ABUS IP-Tool und aktivieren die Kamera.
3. Öffnen Sie die Oberfläche der Kamera, loggen sich als Installateur ein und öffnen die Konfiguration.
4. Aktivieren Sie ONVIF in den erweiterten Netzwerkeinstellungen der Kamera unter dem Reiter "Integrationsprotokoll" (Open Network Video Interface)
5. Hier sehen sie auch die ONVIF Version der Kamera & für Comfion Pro wird 21.12 oder höher benötigt. (Bei Bedarf bitte die Firmware der Kamera aktualisieren – diese ist auf abus.com im Downloadbereich des Artikels verfügbar)
6. Darüber hinaus muss hier ein neuer ONVIF-Benutzer hinzugefügt werden. Wählen Sie hier bitte den Benutzertyp „Administrator“ aus.
7. Nehmen Sie die im untenstehenden Hinweissfeld beschriebenen Video-Einstellungen in der Kamera vor
8. Hinterlegen Sie die ONVIF-Benutzerdaten in der Comfion Pro. (Wählen Sie für die Verbindung zur Kamera in der Comfion Pro App & Webinterface den unter (6.) angelegten Benutzer aus.
9. Testen Sie die Kamerafunktionen (Livebild, etc.)



The screenshot shows the ABUS configuration interface. On the left, the 'KONFIGURATION' tab is selected, and the 'INTEGRATIONSPROTOKOLL' sub-tab is active. A red box highlights the 'Open Network Video Interface aktivieren' checkbox, which is checked. Below it, the 'Open Network Video Interface Version' is shown as 21.12. A table lists the current users:

Nr.	Benutzername	Benutzertyp
1	installer	Administrator

On the right, the 'Benutzer hinzufügen' dialog is open. The 'Benutzername' field contains 'installer'. The 'Passwort' field is masked with dots. The 'Bestätigen' field is also masked. The 'Benutzertyp' is set to 'Administrator' (indicated by a radio button and a red box). The 'OK' button is visible at the bottom right.

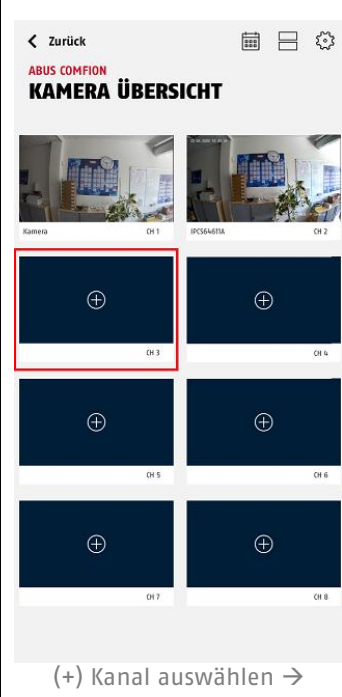
 Hinweis	Folgende Video-Stream-Einstellungen werden je nach Anzahl der eingebundenen Kameras (Kanäle) empfohlen, um auch bei gleichzeitigem Aufrufen und Daueraufzeichnen von 8 Kanälen einen störungsfreien Stream gewährleisten zu können. Primär-Stream: • 1 Kanal: Auflösung 4K; Bitrate: 6Mbps • 8 Kanäle: ➤ 4 x Auflösung: 4K (3840 x 2160); Bitrate: 2048kbps ➤ 4 x Auflösung: 1080p (1920 x 1080; Bitrate: 2048kbps Sekundär-Stream: • 1-8 Kanäle: Auflösung: 360p; Bitrate 512kbps
 Hinweis	• Die maximale Auflösung von 4K (3840 x 2160) je Kanal darf nicht überschritten werden • Die maximale Bitrate darf 8 x 2048kbps nicht überschreiten

3.4.2. Einbinden von Kameras per RTSP

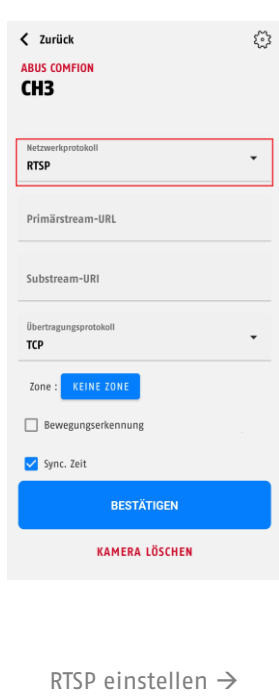
 Hinweis	Die Einbindung via RTSP liefert den Video- und Audio-Stream der Kamera ermöglicht aber keine weitergehende Konfiguration keine PTZ-Steuerung und Bewegungserkennung.
--	---

Zur Einbindung von Kameras via RTSP-Stream führen Sie folgende Schritte aus:

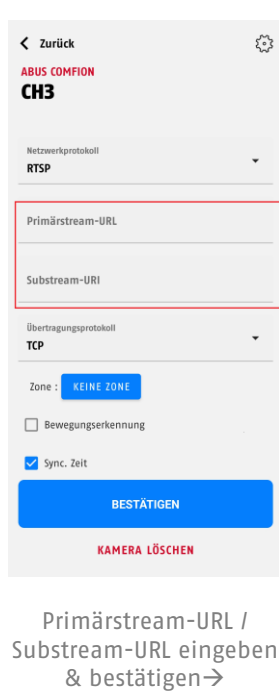
1. Binden Sie die Kamera in das gleiche Netzwerk wie die Comfion Pro ein.
2. Öffnen Sie die Software ABUS IP-Tool und aktivieren die Kamera. Legen Sie ggf. einen Installateur-Account für die Kamera an.
3. Wählen Sie in der Comfion App → Kamera-Übersicht einen (noch freien) Kamerakanal aus (+)
4. Wählen Sie in der Konfiguration unter „Netzwerkprotokoll“ RTSP aus.
5. Fügen Sie die Primärstream und die Substream URL ein. Kompatible ABUS-Kameras verwenden folgende URLs:
 - **Hinweis:** Ersetzen Sie „Benutzername“ und „Passwort“ durch die Zugangsdaten aus Schritt 2
 - Primärstream: `rtsp://Benutzername:Passwort@192.168.0.27/ISAPI/Streaming/channels/101`
 - Sekundärstream: `rtsp://Benutzername:Passwort@192.168.0.27/ISAPI/Streaming/channels/102`



(+) Kanal auswählen →



RTSP einstellen →



Primärstream-URL / Substream-URL eingeben & bestätigen →

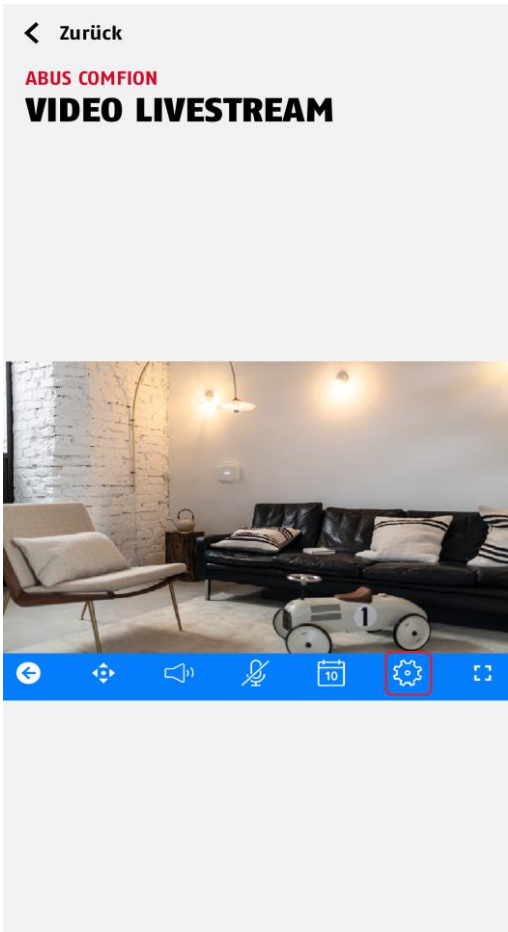
3.4.3. Kamera Einstellungen (global)

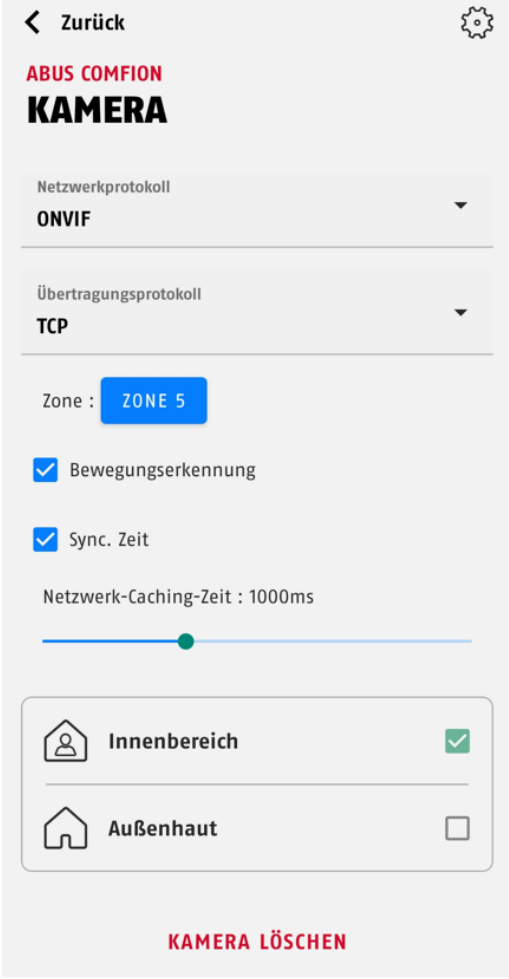
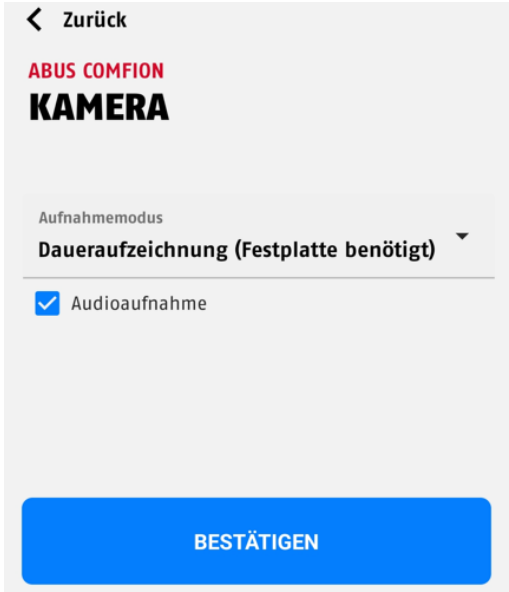
Über die Kamera-Übersicht gelangen Sie durch Klick auf das Zahnrad-Symbol  in die Kamera-Einstellungen. Diese gelten für **alle eingebundenen Kameras gleicherweise**.

Automatische Kamerasuche	AUS (Voreinstellung) / EIN (keine) Automatische Suche nach ONVIF Kameras im gleichen Netzwerk
Datenspeicherung	AUS / EIN & 1 – 365 Tage Aufnahmen werden nach Ablauf der angegebenen Zeit vom Datenträger gelöscht, sofern „EIN“ aktiviert wurde.
Aufnahme Stream Typ	Primärstream (Voreinstellung) / Sekundärstream Streamtyp, der für die Aufzeichnung verwendet wird.

In der Kamera-Detailansicht (Video-Livestream) finden Sie ein weiteres Zahnrad-Symbol  für weitere Konfigurationen **dieser Kamera**. Weitere Details finden Sie in **Kapitel 3.4.4**.

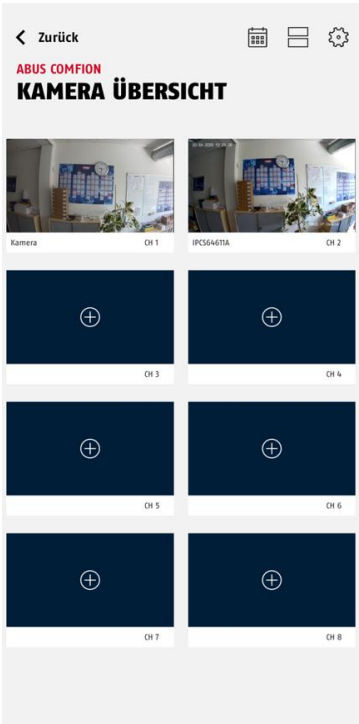
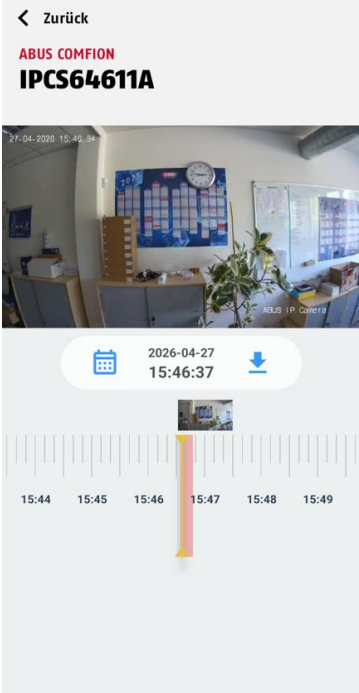
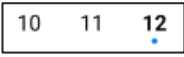
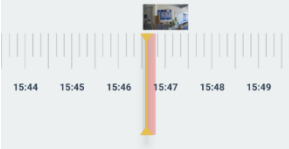
3.4.4. Kamera Einstellungen (einzeln)

	Aus der Kamera Übersicht gelangen Sie durch Klick auf die Kamera-Kachel zum Video-Livestream  zurück zur Kamera-Übersicht Schwenken/Neigen, Lautsprecher, Mikrofon    Weitere Steuerfunktionen & Details entnehmen Sie der Comfion Pro Benutzeranleitung.  Kameraereignisse – weitere Details siehe Kapitel 3.4.5 NVR-Bedienung  Einstellungen für diese Kamera  Wechselt den Betrachtungswinkel Portrait / Landscape Modus
---	---

	Kamera Name, IP-Adresse, Port, Benutzername, Passwort, Netzwerkprotokoll, Übertragungsprotokoll • Siehe 3.4.1 und 3.4.2 Einbinden von Kameras Zone • Sofern die Kamera einem Teilbereich hinzugefügt wurde (hier Innenbereich) wird hier die Zonennummer angezeigt. Bewegungserkennung • Falls aktiviert, wird die Bewegungserkennung der Kamera von der Comfion Pro ausgewertet und kann in Automationen als Auslöseereignis programmiert werden.  Wichtig Die Aktivierung dieser Funktion erfordert, dass Sie in der Direktkonfiguration der Kamera (Webinterface bzw. ABUS-IP-Tool) aktivieren.  Hinweis Um die Bewegungserkennung der Kamera zur Alarmauslösung zu verwenden, muss zusätzlich in den Komponenten-Einstellungen der Kamera. die Funktion „MotionAlarm“ aktiviert werden. Sync.Zeit • Falls aktiviert, übernimmt die Kamera die Zeiteinstellung der Comfion Pro Zentrale Netzwerk-Caching-Zeit • Pufferzeit des Comfion Pro NVR zur Zwischenspeicherung eingehender Videodaten vor Anzeige. Kamera Löschen Entfernt die Kamera vom Kanal-Platz und aus der Komponenten-Liste.
	Klicken Sie auf das Zahnradsymbol in den Kamera-Einstellungen (einzeln) um den Aufnahmemodus einzustellen: Aufnahmemodus • Daueraufzeichnung ○ 24/7 Aufnahme ○ Erfordert Festplatte (z.B. SSD-Datenspeicher) • Aufnahme nur bei aktiviertem System ○ Aufnahme bei Scharfgeschalteter Anlage (bzw. Teilbereich) ○ Erfordert Festplatte (z.B. SSD-Datenspeicher) • Aufnahme nur bei Event ○ Abhängig vom eingestellten Zonentyp der Kamera z.B. Einbruch oder Perimeter ○ Erfordert Micro-SD Karte oder Festplatte • Keine Aufnahme Audioaufnahme • Aufnahme inklusive Audiostream (sofern von Kamera unterstützt)

3.4.5. NVR-Bedienung

Über die Kamera-Übersicht gelangen Sie in die Parallelansicht, aller Kanäle. Sie können sich hier das Livebild aller eingebundenen Kameras anschauen. Über die Kalender-Funktion können Sie sich die vorhandenen Aufnahmen im System nach Datum sortiert anschauen.

	 Kameraereignisse je Kamera-Kanal (Daueraufzeichnung und/oder Ereignisse)   Ansicht der Kamera-Kanäle im Raster oder Zeilen.  Kamera-Einstellungen  Vorschaubild bereits eingelernter Kamera – Klicken wechselt zum Live-Stream der Kamera. Abhängig vom Kamera-Typ sind weitere Funktionen/Einstellungen möglich. (z.B. PTZ, 2WayAudio, etc.)  Freier Kamera-Kanal. Klicken auf „+“ startet den Einlernprozess d.h. durch die Suche nach Kameras im gleichen Netzwerk bzw. manuelles Einbinden.
	Wählen Sie zunächst den Kamerakanal aus um in diese Ansicht zu gelangen.  Suche von Kamera-Aufnahmen im Kalender (Tage mit Ereignissen sind mit einem Punkt markiert)   Download von Kamera-Ereignissen • Startzeit wird im Zeitstrahl festgelegt • Aufnahmedauer 10 Sek. – 30 Min einstellbar  Auswahl Kamera-Ereignisse im Zeitstrahl Eventaufzeichnung → Rot Daueraufzeichnung → Grau

4. Benutzer und Berechtigungsgruppen

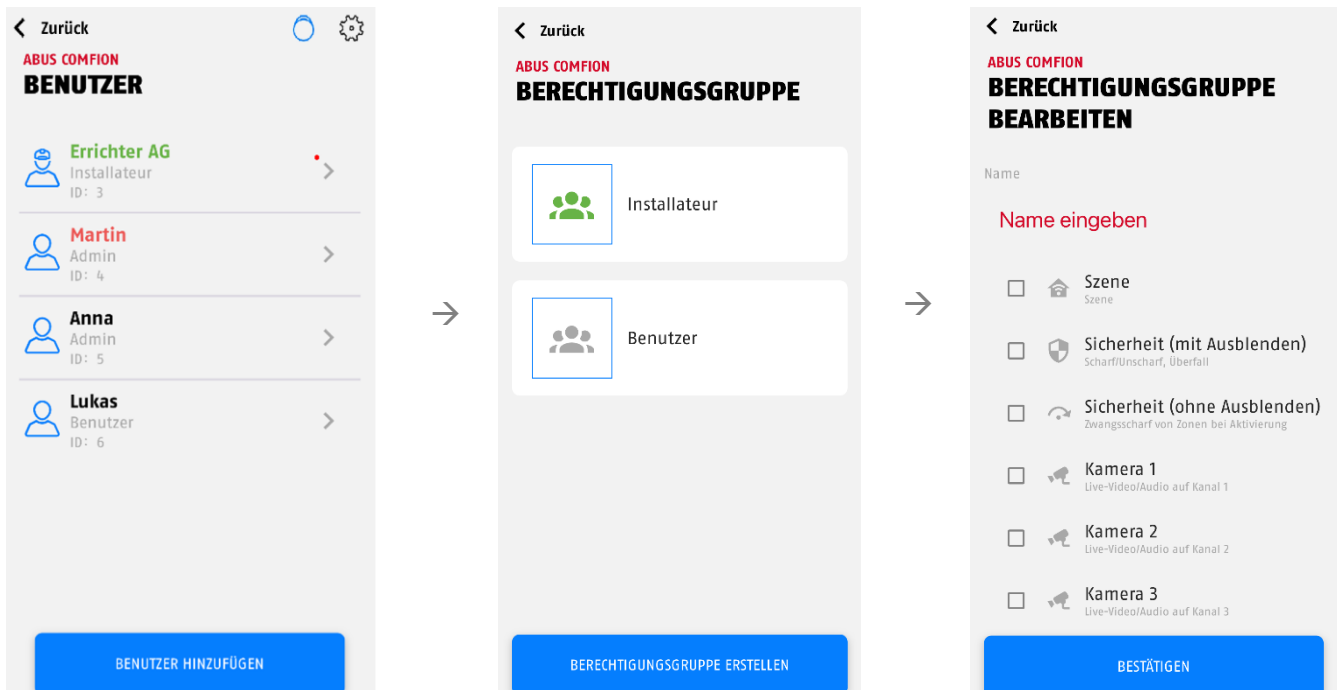
4.1. Erklärung der verschiedenen Rollen

Installateur	Der Installateur hat bei Erstinbetriebnahme alle Benutzerrechte. Nach der Übergabe der Anlage behält der Installateur alle Konfigurationsrechte. Der Besitzer der Anlage kann dem Installateur die Rechte für das Kamera-Livebild nehmen, und ihm den Zugriff auf die Anlage komplett sperren.
Admin	Der Admin der Anlage hat alle Benutzerrechte für die Anlage. Sofern der Installateur den Admin mit Konfigurationsrechten ausstattet, kann der Admin die Rechte eines Installateurs erhalten und so z.B. Automationen und Szenen erstellen und bearbeiten.
Eigene Rolle (Benutzerdefiniert)	Sie haben die Möglichkeit eigene Nicht-Admin-Benutzergruppen zu erstellen und deren Berechtigungen festzulegen (Siehe unten)
Besitzer (Zusatzrolle)	Die Besitzer-Rolle wird automatisch dem ersten an der Anlage bestehenden Admin zugewiesen. Die Besitzer-Rolle kann nicht manuell vergeben werden. Der Besitzer der Anlage hat zusätzlich zu dem Admin-Rechten die Rechte Benutzer hinzuzufügen, einzuladen und zu löschen. Der Besitzer der Anlage ist in der Benutzerliste rot markiert.

Folgende Einstellungsmöglichkeiten gibt es unter dem Installateur-Benutzer:

- Zugriff freigeben: Sperrt/Gibt den Zugriff auf das System sowie Push-Benachrichtigungen
- Haupt-Installateur: Legt fest, mit welchem Installateur-Account die Anlage für die Fernwartung verbunden wird (Facherrichterportal)

Erstellen von Benutzergruppen:



4.2. Inbetriebnahme

Im Werkszustand der Zentrale gibt es aktuell die Berechtigungsgruppen „Installateur“ und „Admin“. Wenn die Anlage durch einen Installateur in Betrieb genommen wird, ist dieser zu Beginn für alle Funktionen in der Zentrale berechtigt.

4.2.1. Übergabe an den Besitzer

Nachdem Sie als Installateur die Einrichtung der Zentrale abgeschlossen haben, muss die Anlage an den Endnutzer übergeben werden. Der erste eingeladene Admin wird **der Besitzer** der Anlage. Dies erkennen Sie daran, dass dieser Nutzer rot markiert wird.

Nach dem Einladen des Besitzers verliert der Installateur die Rechte zum Bearbeiten und Hinzufügen von Nutzern. Weitere Nutzer müssen vom **Besitzer** hinzugefügt werden.

4.3. Einladen/Hinzufügen von Benutzern

Neue Benutzer können nach der Übergabe ausschließlich vom Besitzer eingeladen werden. Zur Auswahl stehen beim Hinzufügen eines neuen Benutzers die folgenden Möglichkeiten:

- Neuen Benutzer einladen
 - Einladung eines Benutzers anhand der E-Mailadresse.
- Wählen von meinen Mitgliedern
 - Einladen eines Mitglieds. Mitglieder können in der Zentralenübersicht zu der persönlichen Mitgliederliste hinzugefügt werden. (Siehe **6.3.2 Mitglieder**)
- Lokalen Benutzer erstellen
 - Erstellen eines lokalen Benutzers ohne Abus Cloud Konto und ohne App-Nutzung. Dem lokalen Benutzer kann eine Fernbedienung, ein Code für das Bedienteil zugewiesen sowie ein NFC-Tag/Karte hinzugefügt werden. Außerdem können Rufnummer & E-Mail für Benachrichtigungen hinterlegt werden.

Des Weiteren kann die Berechtigung des hinzuzufügenden Benutzers gewählt werden. Hierbei kann man zwischen Installateur, Admin und den selbst erstellten Benutzergruppen wählen.

4.4. Bearbeiten von Benutzern

Die Benutzerdaten gliedern sich in 3 Bereiche, d.h. Zugriffsrechte, Benachrichtigungen und Erlaubte Alarmmodi im Betrieb

4.4.1. Zugriffsrechte

Berechtigung:

Pro Benutzer kann hier die Berechtigungsgruppe (Installateur, Admin, Normaler-Benutzer) angepasst werden

PIN-Code:

Eingabe des 4-stelligen PIN-Codes zur Identifikation am Comfion Funk-Bedienteil

 Hinweis	Jeder 4-stellige Code kann nur einmal vergeben werden. Falls der gleiche Code einem zweiten Nutzer zugeordnet wird, erscheint eine Fehlermeldung.
--	---

Zugriff zulassen

In Verbindung mit Eingabe der E-Mail-Adresse und Telefonnummer. Ermöglicht für diesen Benutzer den Zugriff

E-Mail & Telefon (Nur Lokale Benutzer)

Eingabe der E-Mail-Adresse u. Telefonnummer zum Empfang von Benachrichtigungen per E-Mail, SMS

NFC-Tag und Karte

Pro Benutzer können bis zu 2 NFC-Tags / Karten eingelernt und zugeordnet werden.

<
Zurück

ABUS COMFION
BEARBEITEN BENUTZER

✓

Zugriffsrechte

✓

Benachrichtigun
gen

✓

Erlaubte
Alarmmodi im
Betrieb

Info

Einstellu...

Alarm

Benutzername ID : 1
XYZ@abc.com

PIN-Code

NFC-Tag und Karte

WLX_Pro_Tag_1

BESTÄTIGEN

Druck auf „+“ startet den Einlern-Prozess

Druck auf bereits eingelernte Medien öffnet die Einstellungen mit weiteren Konfigurationsmöglichkeiten:

- Aus - (deaktiviert den Tag falls eingeschaltet)
- Zwangsscharf - (Ermöglicht die Scharf-Schaltung bei Störungen)
- Fallback Medium - (falls eingeschaltet wird bei gestörter Funk-Kommunikation zwischen Zylinder/Wall-Reader und dem BUS-WLX-Modul der Zutritt lokal am Zylinder/Wall-Reader geprüft.)
- Name - (Bezeichnung des Tags - der Name erscheint auch im Logbuch bei Zutritts-Ereignis)
- Benutzer - (Zuordnung zu einem eingerichteten Benutzer im Comfion Pro System)

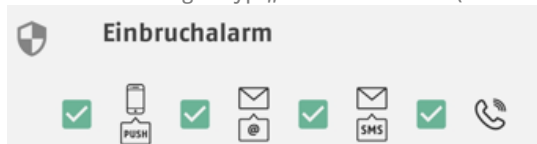
Änderungen müssen durch „Speichern“ bzw. „Bestätigen“ bestätigt werden

4.4.2. Benachrichtigungen

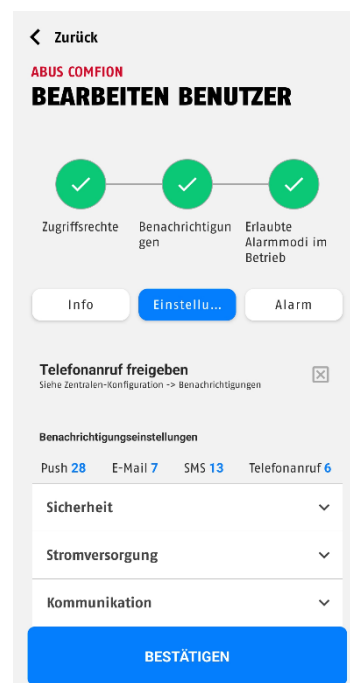
Das Comfion Pro Sicherheitssystem verfügt über folgende Kommunikationswege: E-Mail, Push, SMS, Anruf & Leitstellenaufschaltung

Unter dem Menüpunkt „Benutzer → Bearbeiten Benutzer → Benachrichtigungen“ können Sie bei jedem angelegten Benutzer einzeln wählen, welche Benachrichtigungen je Ereignis versendet werden sollen.

z.B. für den Ereignistyp „Einbruchalarm“ (Push/E-Mail/SMS/Anruf)



 Hinweis	Einige Ereignisse sind auf bestimmte Kommunikationsarten eingeschränkt. Z.B. ist für einige Ereignisse kein Telefonanruf möglich. Push-Benachrichtigungen stehen nur für Comfion App Nutzer zur Verfügung, d.h. kann nicht für lokale Benutzer verwendet werden.
--	--



Die Telefonnummer zur SMS & Telefonanruf, sowie E-Mail-Adresse für Benachrichtigungen werden im Benutzer-Account hinterlegt. Sie können diese jederzeit ändern. Gehen Sie hierzu in Ihre Zentralenübersicht und klicken auf das Zahnrad in der rechten oberen Ecke. Nun können Sie die Benachrichtigungs-Rufnummer, sowie die Benachrichtigungs-E-Mail vergeben.

Für lokale Benutzer erfolgt die Eingabe der E-Mail-Adresse / Telefonnummer in den Benutzereinstellungen (Zugriffsrechte).



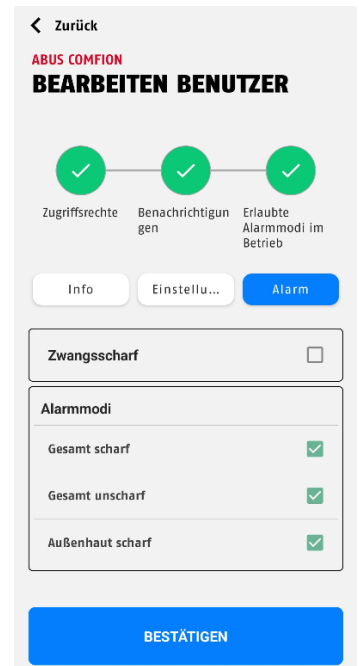
 Hinweis	Bitte geben Sie die Telefonnummer immer mit Ländervorwahl ein z.B. +49.....
--	--

4.4.3. Erlaubte Alarmmodi im Betrieb

Sie legen hier fest ob der Benutzer das System zwangsscharf schalten darf (in diesem Fall erfolgt die Scharfschaltung selbst bei geöffnete/ausgelöster Zone & ohne den Ausblenden-Vorgang) weitere Details finden Sie im **Kapitel: 6.7.3**

Außerdem legen Sie hier die Berechtigung zum Scharf- und Unscharf schalten je Teilbereich fest. Der Benutzer muss mindestens eine Berechtigung besitzen.

Alle Änderungen werden mit Druck auf „Bestätigen“ übernommen.



4.5. Löschen von Benutzern

Es gibt zwei Möglichkeiten, Benutzer aus der Zentrale zu entfernen:

6. Der Besitzer der Anlage (rot markierter Benutzer) kann jeden anderen Benutzer durch Klick auf diesen und den Button „Benutzer löschen“ aus dem System entfernen.
7. Jeder Benutzer kann sich selbst aus der Anlage löschen, indem er in der Zentralenübersicht lange auf die betroffene Zentrale klickt und anschließend die Aufforderung zum Löschen bestätigt.

 Hinweis	Der Besitzer der Anlage kann sich selbst nur durch den zweiten Weg (Zentrale aus Zentralenübersicht löschen) aus dem System entfernen. Nach dem Entfernen des Besitzers fällt die Rolle auf den Installateur zurück. Dieser kann durch Einladen eines neuen Admins diesen als neuen Besitzer kennzeichnen.
--	--

5. Kommunikation

5.1. Mobilfunkmodul

Das Comfion Pro Sicherheitssystem verfügt über ein integriertes Mobilfunkmodul (2G/3G/4G). Über dieses lassen sich SMS verschicken und Anrufe im Alarmfall tätigen. Es bietet außerdem einen Redundanz-Weg für die gesamte Kommunikation des Systems. Das heißt, dass bei Ausfall Ihrer Internetverbindung jegliche Kommunikation mit der Cloud, und somit auch der Fernzugriff sowie die Push-Benachrichtigungen über das Mobilfunkmodul durchgeführt werden.

 Hinweis	Schalten Sie Ihre SIM-Karte vor dem Einlegen in das Mobilfunkmodul Pin-frei. Die PIN können Sie in der Regel in den Einstellungen eines beliebigen Handys abstellen.
--	--

 Hinweis	Verwenden Sie keine SIM-Karten aus dem Ausland für den Dauereinsatz in der Comfion Pro.
--	---

Für den Betrieb des Mobilfunkmodus ist eine SIM-Karte notwendig. Diese SIM-Karte ist frei wählbar (Empfehlung ABUS: Telekom, Vodafone, o2) und muss über die Features verfügen, welche Sie an der Zentrale nutzen möchten. Wenn Sie alle Funktionen nutzen wollen, benötigen Sie eine SIM-Karte mit SMS, einen Sprachtarif sowie Datenvolumen.

 Hinweis	ABUS rät aus Bedenken bzgl. der Verlässlichkeit davon ab, Prepaid-Karten im Comfion Pro Sicherheitssystem zu nutzen. Des Weiteren ist ein Einsatz von Multi-SIMs nicht ratsam, da es zu Verbindungsproblemen führen kann.
 Hinweis	Die SIM-Karte sollte je nach Einsatzzweck über folgende Eigenschaften verfügen: • „SMS over IMS“ – SMS-Versand über das 4G Netz • „Voice over LTE“ – Anruf-Funktion über das 4G Netz

RSRP-Wert (dbm)	Bedeutung	Hinweis
< -80 -80 bis -90 -91 bis -100 -101 bis -110 > -111	Sehr gut Gut Mittel Schwach Sehr schlecht	 RSRP ist die Stärke des Nutzsignals (LTE-Referenzsignal) das vom Mobilfunkmast am Gerät ankommt. Der Installationsort kann die Signalstärke beeinträchtigen z.B. die Entfernung zum Mobilfunkmast oder Dämpfung durch Bausubstanz. Wir empfehlen im Zweifelsfall die Verwendung einer externen Antenne.

Für den SMS-Versand sowie die Anruhfunktion sind im Mobilfunkmodul selbst keine weiteren Einstellungen zu tätigen. Wenn Sie die Redundanz der Netzwerkdienste nutzen möchten, ist es notwendig die APN-Daten der eingesetzten Sim-Karte zu hinterlegen. Den Menüpunkt finden Sie unter „Zentralen-Konfiguration“ → Zahnrad → „Mobilfunkmodul“.

Falls keine SIM-Karte in der Comfion Pro eingesetzt wird, deaktivieren Sie bitte das „Aktivieren“ Feld. In diesem Fall findet keine Prüfung der SIM-Karte und ggf. Fehlermeldung statt.

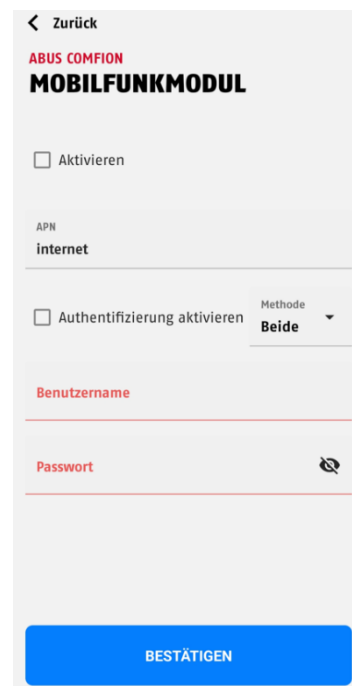
Die APN-Daten Ihres Mobilfunkanbieters liegen Ihrer SIM-Karte bei. Alternativ können Sie diese online abfragen. Die Daten sind nicht SIM-Karten-spezifisch, sondern für jeden Anbieter gleich. Wenn bei den APN-Daten Benutzername & Passwort angegeben sind, setzen Sie den Haken bei „Authentifizierung“.

Beispiel Telekom:

- APN: internet.telekom
- Benutzername: t-mobile
- Passwort: tm

Beispiel Vodafone:

- APN: web.vodafone.de
- Kein Benutzername
- Kein Passwort



5.2. E-Mail

Der E-Mail-Versand der Comfion Pro funktioniert ohne Konfiguration und wird über die Cloud durchgeführt.

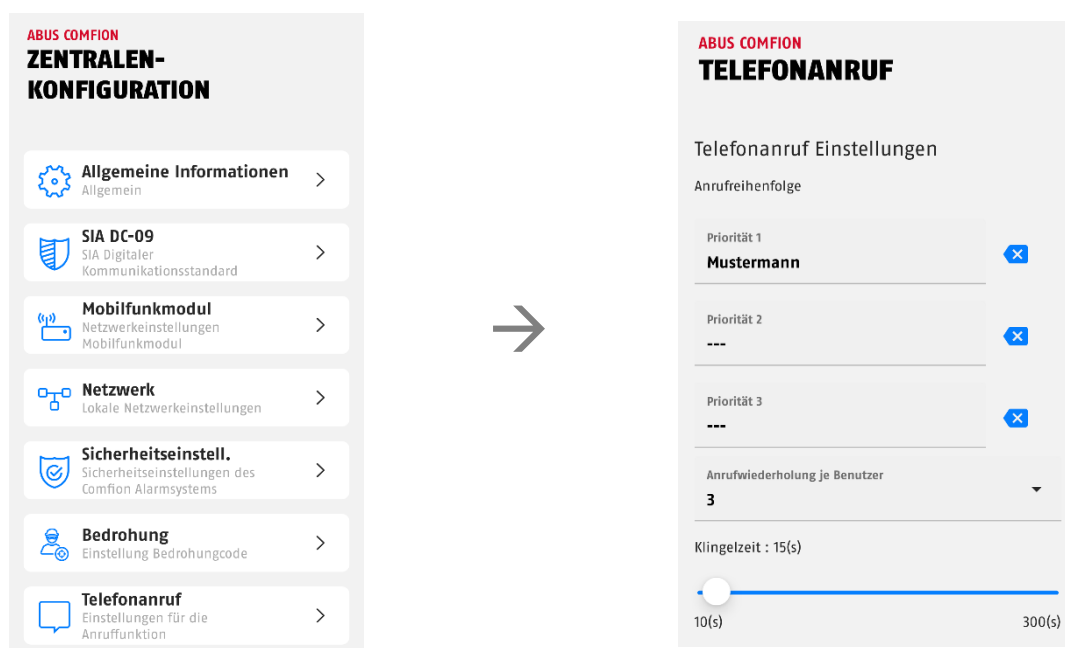
Falls die zu benachrichtigende E-Mail-Adresse von der Account-Mail abweichen soll, können Sie eine Benachrichtigungs-Adresse in Ihrem Account hinterlegen (siehe **4.4.2 Benachrichtigungen**). Wenn Sie keine Benachrichtigungs-E-Mail hinterlegen, werden die E-Mails an Ihre Account-Adresse verschickt.

5.3. Telefonanruf

Das Comfion Pro Sicherheitssystem kann Sie bei einem Alarm anrufen. Die Anlage verfügt über kein Sprachwählgerät, was bedeutet, dass keine Sprachnachricht bei diesem Anruf abgespielt wird. Der Anruf dient lediglich zur Alarmierung und soll helfen, den angerufenen Benutzer über einen Alarm zu informieren. Um was für einen Alarm sich handelt, kann der simultan versendeten Push-Benachrichtigung entnommen werden.

Für die Anruffunktion ist eine eingelegte SIM-Karte mit Anruffunktion notwendig. Weitere Hinweise zum Mobilfunkmodul finden Sie unter **5.1 Mobilfunkmodul**.

- Um Anrufe zu erhalten, muss die Telefonnummer des Empfängers in dem Benutzerkonto hinterlegt werden (siehe 5. Kommunikation).
- Des Weiteren müssen Sie unter „Zentralen-Konfiguration“ – „Telefonanruf“ die Anrufreihenfolge festlegen. Es können maximal 3 Benutzer hintereinander angerufen werden.



 Hinweis	Die Anrufwiederholung je Benutzer ist werkstellig auf 3 gestellt. Das bedeutet, dass jeder Anrufer drei Anrufe bekommt. Der Anruf kann nicht bestätigt werden.
--	---

5.4. SMS

Das Comfion Pro System kann SMS-Nachrichten anhand der Ereignisliste (Siehe **5. Kommunikation**) verschicken. Des Weiteren können Sie sich per Automationen SMS-Nachrichten mit frei definierbarem Text bei beliebigen Ereignissen schicken lassen.

Für die grundsätzliche Versandmöglichkeit von SMS muss lediglich eine SIM-Karte in das Modul eingelegt sein sowie die Benachrichtigungs-Rufnummer im Account hinterlegt sein (Siehe **5. Kommunikation**).

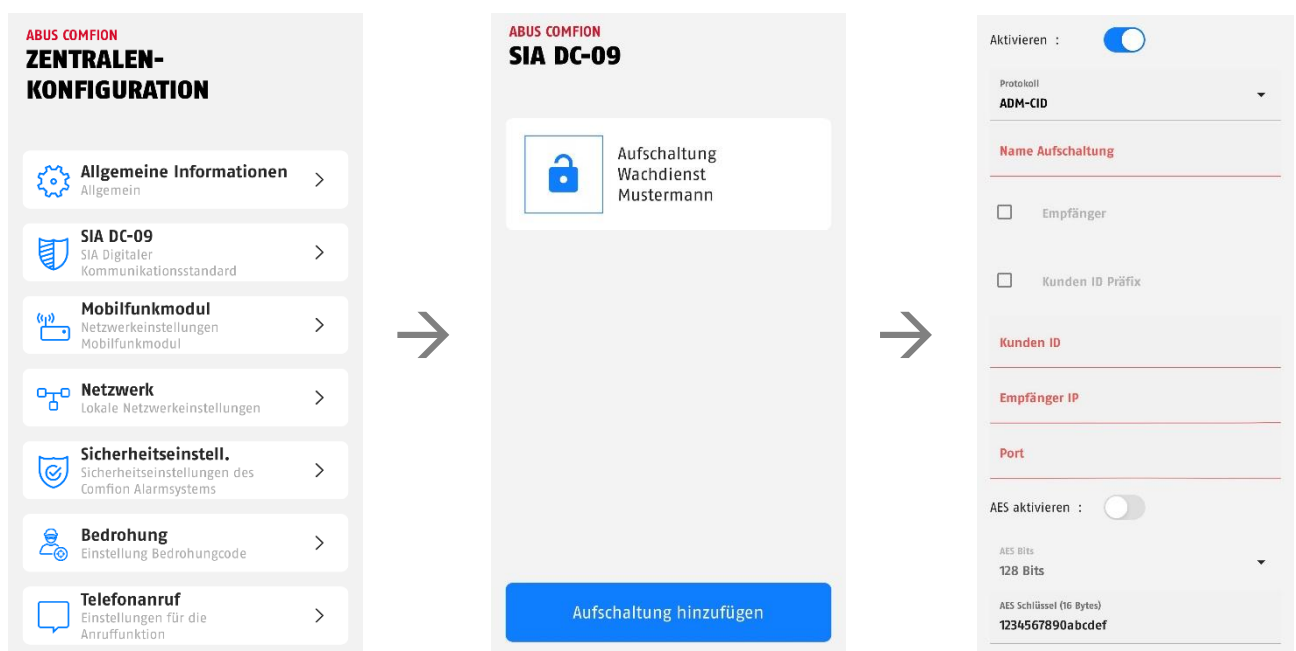
5.5. SIA DC-09 (Leitstellenaufschaltung)

Das Comfion Pro Funk-Sicherheitssystem verfügt über ein digitales Leitstellenwählgerät welches das Protokoll Contact-ID über den Standard SIA DC-09 verschicken kann. Sie können mehrere Aufschaltungen gleichzeitig konfigurieren und somit an verschiedene Wachdienste kommunizieren.

Tragen Sie die von Ihrem Dienstleister erhaltenen Daten in die betroffenen Felder ein. Die beiden ausgegrauten Felder „Empfänger“ sowie „Kunden ID Präfix“ werden in der Regel nicht benötigt und müssen nur aktiviert werden, wenn es explizit von Ihrem Dienstleister gefordert wird.

Im Feld „Statische Testmeldung“ können Sie zwischen folgenden Optionen wählen:

- **DC-09 Leitungsüberwachung** -> Im Leitstellenprotokoll integrierte Supervision (muss von Leitstelle unterstützt werden)
- **CID-Testnachricht 602** -> Übertragung des Contact-ID Codes 602 im eingestellten Intervall
 - **Achtung:** Das eingestellte Intervall bestimmt die Zeit nach dem letzten geschickten Ereignis an die Leitstelle. Wird in der Zwischenzeit ein Ereignis an die Leitstelle übertragen, startet das Intervall erneut.



Über das Zahnrad-Symbol im rechten oberen Bildrand erreichen sie die Erweiterten Einstellungen. In diesem können Sie die statische Testnachricht aktivieren, sowie den Intervall einstellen

 Hinweis	Eine Auflistung der Contact-ID Codes finden Sie im Anhang (Kapitel 11.1)
--	---

6. Allgemeines, Wartung und Hinweise

6.1. Zentralen-Konfiguration

Unter dem Menüpunkt Zentralen-Konfiguration finden Sie zum einen alle wichtigen Informationen zu Ihrer Zentrale und können des Weiteren wichtige Einstellungen zum System vornehmen

Nachdem Sie den Menüpunkt Zentralen-Konfiguration aufgerufen haben, sehen Sie als die folgenden Informationen:

- Zentrale Name → (Eingabefeld)
- Symbol → (Kann durch eigenes Foto ausgetauscht werden)
- Netzwerk → (Anzeige der Art Netzwerkverbindung)
- Mobilfunkstatus → (Drop-Down)
 - Modul Typ → (verbauter Mobilfunkchip)
 - SIM-Karte → (Anzeige ob eingelegt)
 - IMEI → (eindeutige 15-stellige Seriennummer des Mobilfunk-Moduls)
 - Telefonanruf → (Anzeige ob mit eingelegter SIM möglich)
 - LTE-Verbindung → (Anzeige über Verbindungsstatus)
 - Signalstärke (dBm) → (RSRP gemessen in -dbm, (empfohlene Signalstärke siehe **Kapitel 5.1**)
- Stromversorgung → (Anzeige Netzteil od. Akku)
- Firmware → (Per Klick darauf Anzeige der Version u. der Release-Notes)
- Funkmodul → (Anzeige der Firmware des Funkmoduls)
- Artikelnummer

Bestätigen

- Bestätigt die Änderungen in diesem Menü.
- Die Änderungen sind danach ebenfalls in der ABUS-Cloud aktualisiert.
-

Zentrale löschen

- Entfernt Zentrale aus der App und vom ABUS-Cloud Account!

Über das Zahnrad-Symbol rechts oben können Sie weitere Einstellungsmenüs öffnen.

Die Einstellungen zu SIA DC-09, Telefonanruf und dem Mobilfunkmodul finden Sie unter 5. Kommunikation.

6.1.1. Allgemeine Informationen

Unter der Überschrift „Speicher“ werden die Ihnen Informationen zum eingelegten Speichermedium (Festplatte und/oder SD-Karte) angezeigt.

Unter der Überschrift „Datum und Uhrzeit“ werden Ihnen die verwendete Zeitzone sowie der NTP-Server angezeigt. Mithilfe des Buttons „Neustart“ können sie die Zentrale neustarten.

6.1.2. Netzwerk

In diesem Menü können Sie die Netzwerkeinstellungen einsehen und gegebenenfalls anpassen.

Sie haben drei mögliche Methoden als Auswahl:

DHCP (Voreinstellung): Dynamic Host Configuration Protocol ist ein Client/Server-Protokoll, durch welches der Comfion Pro automatisch seine IP-Adresse und andere zugehörige Informationen vom Router zur Verfügung gestellt werden.

PPPoE: Point-to-Point Protocol over Ethernet ist ein Netzwerk-Protokoll, welches die Direktverbindung im internen Netzwerk zur Verfügung stellt. Hierzu ist eine Authentifizierung per Benutzername und Passwort notwendig.

Statisch: Bei der Auswahl „statisch“ werden die Netzwerkdaten der Comfion Pro manuell vergeben. Sprechen Sie dies mit dem Betreiber des Netzwerks ab und vergeben Sie keine IP-Adresse aus dem DHCP-Pool.

 Hinweis	Falsche IP-Einstellungen führen dazu, dass Ihr System keine Verbindung zum Netzwerk herstellen kann, wodurch es für die App unerreichbar wird. Drücken Sie in diesem Fall die „Netzwerk-Rückstellung“-Taste (Nr. 14) auf der Rückseite der Anlage für 6 Sekunden und lassen Sie sie dann los. Die Zentrale wird dann neu starten und ihre Netzwerkeinstellungen wieder auf die Standard-DHCP-Einstellungen zurücksetzen.
--	---

6.1.3. Sicherheitseinstellungen

Wartungsmodus	An/AUS (Voreinstellung AUS)	Der Wartungsmodus dient zur Installation und Wartung des Systems. Während der Wartungsmodus aktiv ist, kann die Anlage keine Alarmer auslösen.
Zonensperre	3x-20x (Voreinstellung 5x)	Wenn eine Zone öfter ausgelöst wird als eingestellt, wird diese Zone nicht weiter auslösen, bis die Alarmer aus dem Alarmverlauf gelöscht werden
Max. Wiederholung der Tastatureingabe	3x-20x (Voreinstellung 5x)	Gibt an nach wie vielen falschen PIN-Eingaben am Bedienteil dieses gesperrt wird
Bedienteil-Timeout	5-180 sek (Voreinstellung 30 sek)	Zeiteinstellung wie lange das Bedienteil nach X falschen Eingaben gesperrt ist
Eingangsverzögerung	5-45 sek (Voreinstellung 10 sek)	Bei scharfer Anlage wird die Eingangsverzögerung am Funk-Bedienteil angezeigt.
Ausgangsverzögerung	5-45 sek (Voreinstellung 30 sek)	Verzögerungszeit, die am Bedienteil angezeigt wird, bevor die Zentrale in den scharfen Zustand wechselt.
Übertragungs- verzögerung	5-180 sek (Voreinstellung 60 sek)	Bei aktivierter Eigenschaft in der Zone wird die Übertragung einer Auslösung um die eingestellte Zeit verzögert.
Stromausfall Verzögerung	0-30 min (Voreinstellung 0 min)	Einstellbare Verzögerung der Meldung eines Spannungsverlusts (12V DC)
Einbruch Sirene aktivieren	An/AUS (Voreinstellung AN)	Sirenenansteuerung bei einem Einbruchalarm
Einbruchalarm Sirenendauer	5-180 sek (Voreinstellung 60 sek)	Dauer der akustischen Signalisierung durch in das System eingebundene Sirenen
Sabotage Sirene aktivieren	An/AUS (Voreinstellung AN)	Sirenenansteuerung bei einem Sabotagealarm
Sabotagealarm Sirenendauer	5-180 sek (Voreinstellung 60 sek)	Dauer der akustischen Signalisierung durch in das System eingebundene Sirenen
Logo-LED anzeigen: Sabotage	An/AUS (Voreinstellung AN)	Zeigt den Alarm-Typ „Sabotage“ visuell am beleuchteten ABUS-Logo an. (Rot-blinken)
Überfall Sirene aktivieren	An/AUS (Voreinstellung AUS)	Sirenenansteuerung bei einem Überfallalarm
Überfallalarm Sirenendauer	5-180 sek (Voreinstellung 60 sek)	Dauer der akustischen Signalisierung durch in das System eingebundene Sirenen
Logo-LED anzeigen: Überfall	An/AUS (Voreinstellung AN)	Zeigt den Alarm-Typ „Überfall“ visuell am beleuchteten ABUS-Logo an. (Rot blinken)
Wasser Sirene aktivieren	An/AUS (Voreinstellung AN)	Sirenenansteuerung bei einem Wasseralarm
Wasseralarm Sirenendauer	5-180 sek (Voreinstellung 60 sek)	Dauer der akustischen Signalisierung durch in das System eingebundene Sirenen
Logo-LED anzeigen: Überschwemmung	An/AUS (Voreinstellung AN)	Zeigt den Alarm-Typ „Überschwemmung“ visuell am beleuchteten ABUS-Logo an. (Rot blinken)
Feuer Sirene aktivieren	An/AUS (Voreinstellung AN)	Sirenenansteuerung bei einem Feualarm
Feualarm Sirenendauer	5-180 sek (Voreinstellung 60 sek)	Dauer der akustischen Signalisierung durch in das System eingebundene Sirenen
Logo-LED anzeigen: Feualarm	An/AUS (Voreinstellung AN)	Zeigt den Alarm-Typ „Feuer“ visuell am beleuchteten ABUS-Logo an. (Rot blinken)
Überfall APP Sirene aktivieren	An/AUS (Voreinstellung AUS)	Sirenenansteuerung bei einem über die App ausgelösten Überfallalarm
Überfall APP Sirenendauer	5-180 sek (Voreinstellung 60 sek)	Dauer der akustischen Signalisierung durch in das System eingebundene Sirenen
Logo-LED anzeigen: Überfall App	An/AUS (Voreinstellung AN)	Zeigt den Alarm-Typ „Überfall-App“ visuell am beleuchteten ABUS-Logo an. (Rot blinken)
Maskierung Sirene aktivieren	An/AUS (Voreinstellung AN)	Sirenenansteuerung bei Maskierung eines Melders (Abdecküberwachung)
Maskierung Sirenendauer	5-180 sek (Voreinstellung 30 sek)	Dauer der akustischen Signalisierung durch in das System eingebundene Sirenen
Logo-LED anzeigen: Maskierung	An/AUS (Voreinstellung AN)	Zeigt den Alarm-Typ „Abdecküberwachung“ visuell am beleuchteten ABUS-Logo an. (Rot blinken)
Ausblenden	An/AUS	Scharfschaltverhinderung eines Netzwerkfehlers

Netzwerkfehler	(Voreinstellung AUS)	deaktivieren
Ausblenden Akkufehler	AN/AUS (Voreinstellung AUS)	Scharfschaltverhinderung eines Akkufehlers deaktivieren
Ausblenden Stromverlust	AN/AUS (Voreinstellung AUS)	Scharfschaltverhinderung eines Stromverlusts (12V DC) deaktivieren
Automatische Rückstellung aktivieren	AN/AUS (Voreinstellung AN)	AN: Die Rückstellung wird bei der Unscharfschaltung durchgeführt. Sobald sich alle ausgelösten Melder wieder im Normalzustand befinden, verschwindet bei Unscharfschaltung die Warnungsübersicht aus dem Dashboard. AUS: Alarmer und Fehler müssen immer manuell zurückgestellt werden.
NFC offener Modus	AN/AUS (Voreinstellung AUS)	AUS: Es können ausschließlich Mifare DESFire Transponder von ABUS verwendet werden, da diese aus Sicherheitsgründen auf die Comfion Applikation überprüft werden. Fremdhersteller-Transponder sowie Mifare Classic Transponder können nicht verwendet werden. AN: Es können alle Mifare Classic & Mifare DESFire Transponder (Einschränkung siehe Hinweisfeld unterhalb) verwendet werden.
Werksreset zulassen	AN/AUS (Voreinstellung AN)	AUS: Die Zentrale kann nicht über den Reset Taster zurückgesetzt werden AN: Die Zentrale kann über den Reset-Taster zurückgesetzt werden.
Sabotageerkennung deaktivieren	AN/AUS (Voreinstellung AUS)	AN: die Sabotageerkennung aller eingelernten Geräte ist deaktiviert.
Eingang-Folgend im gleichen Bereich	AN/AUS (Voreinstellung AUS)	AUS: Eingang folgend Zonen reagieren auf die Eingangsverzögerung unabhängig vom Bereich AN: Eingang folgend Zonen reagieren nur auf die im selben Bereich ausgelöste Eingangsverzögerung.

 Hinweis	Mifare DESFire Transponder von Fremdherstellern funktionieren nur, wenn sie über eine feste UID verfügen. Auf den Transpondern darf kein Random-ID Mechanismus aktiviert sein.
--	--

6.1.4. PIN-Codes

Sie können in diesem Menü den Bedrohungscode und Zwangsscharf-Code verändern. Diese Codes gelten für alle Nutzer der Anlage und sind 3-stellig
Die Codes sind nur verwendbar in Verbindung mit einem Comfion Funk-Bedienteil

 Hinweis	Der Bedrohungs-Code und Zwangsscharf-Code wird zusammen mit dem Benutzercode eingegeben, d.h.: Benutzercode (4-Stellig) → Bedrohungs-/Zwangsscharf-code (3-Stellig) z.B. 1357999
--	--

Bedrohungscode

- Die Eingabe dieses Codes am Comfion Funk Bedienteil ermöglicht die Unscharfschaltung unter Zwang
- Die Comfion Pro wird unscharf geschaltet, allerdings erfolgt eine Kommunikation an die konfigurierten Empfänger.

Zwangsscharf Code

- Siehe **Kapitel 6.7.3**
- Ermöglicht die Scharfschaltung eines (oder mehrere Teilbereiche) bei geöffneten Zonen, ohne Ausblenden-Vorgang.

6.1.5. Benachrichtigungsverzögerungen

Sie können in diesem Menü die Verzögerungen für **Netzwerkausfall-Benachrichtigungen** einstellen.

Verzögerung Server-Benachrichtigung:

Verzögerungszeit bei Ausfall der Cloud-Verbindung. Definiert die Verzögerung z.B. bei Cloud-Problemen, bis eine Benachrichtigung abgesetzt wird. (Voreinstellung = 10 Sek.); (Einstellbar von 10-600 Sek.)

Verzögerung Client-Benachrichtigung:

Verzögerungszeit bei Verlust der Internetverbindung an der Comfion Pro Zentrale. Dieser kann z.B. durch DSL-Ausfall, fehlendem LAN-Kabel oder Spannungsausfall am Router auftreten. (Voreinstellung = 0 Sek.); (Einstellbar von 0-600 Sek.)

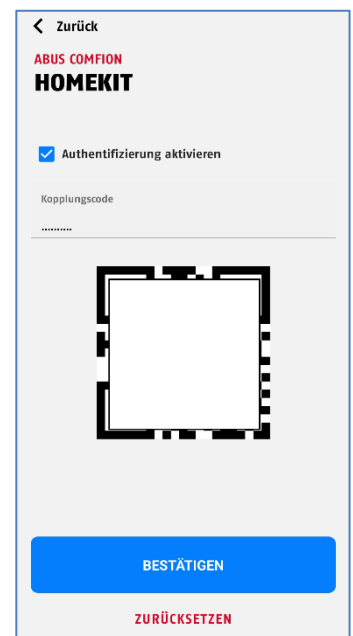
 Hinweis	Abhängig von der Netzwerk Infrastruktur kann es ratsam sein, die Verzögerungszeit leicht zu erhöhen, insbesondere dann, wenn der Router viele IP-Clients verwaltet.
--	---

Mit Klick auf „**Bestätigen**“ werden die Änderungen übernommen.

6.1.6. HomeKit

Fügen Sie in der Apple HomeKit Benutzeroberfläche ein neues Gerät hinzu

- Im Verlauf des Dialogs werden Sie aufgefordert den hier gezeigten QR-Code zu scannen und/oder den 8-stelligen Kopplungs-Code einzugeben.



6.1.7. Backup

 Hinweis	Die Backup-Datei Ihrer Zentrale wird aus Sicherheitsgründen vollverschlüsselt in der Abus Cloud gespeichert.
--	--

Backup erstellen

Im Menü Backup der Zentralen-Konfiguration können Sie manuell ein Backup erstellen sowie das automatische Backup aktivieren. Das automatische Backup wird wöchentlich durchgeführt.

Backup einspielen

 Hinweis	Bitte beachten Sie, dass die neue Zentrale vor dem Backup-Import bereits auf die aktuelle Firmware-Version upgedatet ist.
--	---

Zum Importieren des Backups in eine neue Zentrale gehen Sie bitte wie folgt vor:

1. Trennen Sie Zentrale, von der das Backup stammt, falls noch nicht geschehen vom Netzwerk und schalten Sie sie ab.
2. Gehen Sie in der Zentralenübersicht in der App auf das + Symbol, um eine neue Zentrale hinzuzufügen
3. Wählen Sie „Backup Import“ aus
4. Scannen Sie den QR-Code auf der Rückseite Ihrer neuen Zentrale
5. Wählen Sie die Zentrale aus, von welcher Sie das Backup laden möchten
Hinweis: Nach dem Importieren wird das Backup aus der Cloud gelöscht und die Komponenten funktionieren nicht mehr an der alten Zentrale.
6. Geben Sie den gewünschten Zentralennamen Ihrer neuen Zentrale ein
7. Nach dem Bestätigen wird ein Verifizierungscode an die E-Mail-Adresse des Besitzers der Anlage geschickt. Geben Sie diesen Code in der App ein und klicken Sie auf „Import starten“
8. Der Import wird nun durchgeführt. Sie können Ihre App nun schließen und warten, bis Sie die Push-Mitteilung erhalten, dass die Zentrale online und die Stromversorgung vorhanden ist.

Zum Wiederherstellen einer Konfiguration auf die gleiche Hardware (Zentrale) gehen Sie bitte wie folgt vor:

1. Setzen Sie die betroffene Zentrale auf Werkseinstellungen zurück (Reset-Button für 10 Sekunden betätigen - > siehe 6.5.1)
2. Gehen Sie in der Zentralenübersicht in der App auf das + Symbol, um eine neue Zentrale hinzuzufügen
3. Wählen Sie „Wiederherstellung“ aus
4. Scannen Sie den QR-Code auf der Rückseite Ihrer Zentrale
5. Geben Sie den gewünschten Zentralennamen Ihrer Zentrale ein
6. Der Import wird nun durchgeführt. Sie können Ihre App nun schließen und warten, bis Sie die Push-Mitteilung erhalten, dass die Zentrale online und die Stromversorgung vorhanden ist.

6.1.8. WLX-Informationen

Sie finden hier eine Auflistung der Fallback Berechtigungen inkl. der Reset-Karte

Fallback Berechtigung:

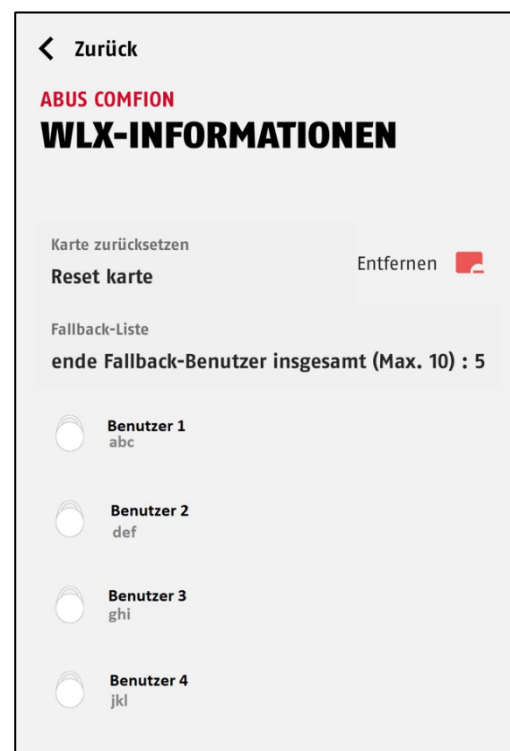
- Die Fallback Berechtigung ist direkt im Zylinder hinterlegt u. erlaubt den Zutritt, wenn keine Funkverbindung zur Comfion Pro Zentrale & BUS-WLX Modul besteht. Im Comfion Pro System können bis zu 10 Fallback Berechtigungen vergeben werden (Die Reset-Karte ist immer ein Fallback-Medium).
- Im Falle einer unterbrochenen Funkverbindung muss das berechtigte Medium drei Mal am wAppLoxx Zylinder präsentiert werden (jeweils die Signalisierung abwarten)
- Die Fallback Berechtigung wird direkt in den NFC-Tag Einstellungen bei dem Benutzer hinterlegt, siehe **Kapitel 4.4** Bearbeiten von Benutzern

Reset Karte

- Die Reset Karte ist im Lieferumfang des Comfion Pro BUS-WLX Modul enthalten.
- Nach dem Einlernen der ersten wAppLoxx Komponente (Zylinder oder Wandlese) wird automatisch der Prozess zum Einlernen der Reset-Karte gestartet.
- Die Reset Karte wird benötigt, um einen Zylinder zurückzusetzen (zusätzlich zur System-Karte)
- Sollte die Reset-Karte verloren gehen, kann diese hier durch „Entfernen“ gelöscht und danach eine neue Reset-Karte eingelernt werden. Nach Entfernen startet der Einlernprozess unmittelbar!

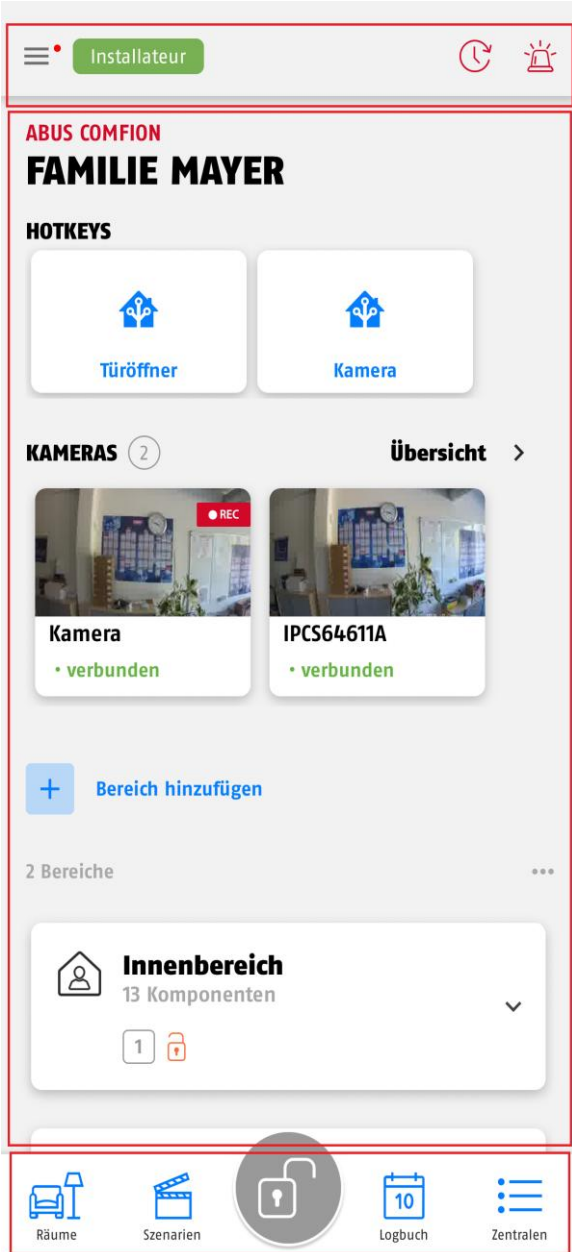
Fallback Liste

- Neben der Reset-Karte erscheinen hier bis zu 9 weitere Tags mit Fallback-Berechtigung.



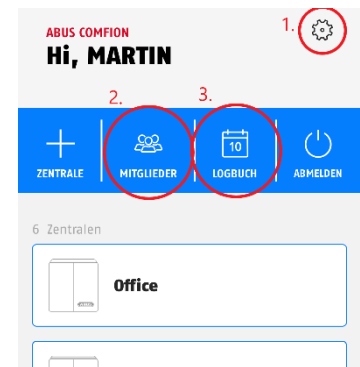
6.2. Dashboard (System eingerichtet)

Über das Dashboard können Sie die Anlage steuern, und auch als Installateur einen Großteil Ihrer Arbeiten durchführen.

	Kopfleiste: •  Konfiguration & Benutze-Einstellungen •  Benutzer-Rolle (nur Installateur) •  Firmware-Update (sofern vorhanden) •  Panik-Alarm Auslösen Dashboard / Funktionsbereich • Hotkey-Schaltflächen ◦ kurzer Tastendruck startet die Szene & Ausführung wird kurz mit  bestätigt ◦ gedrückt halten, um die Szene zu konfigurieren • Kamera-Vorschaubilder ◦ Klick auf Vorschaubild wechselt zum Live-Stream ◦ Klick auf „Übersicht“ wechselt zur Kamera Detail-Seite & weitere Konfiguration • Übersicht Teilbereiche ◦ Klick auf  zeigt zugewiesene Komponenten & deren Status an (sofern eingerichtet) ◦ Klick auf  um die Sortierung der Bereiche anzupassen. Navigationsleiste • Räume (& Komponentenliste) siehe 3.2.4 u. 3.2.5 • Szenarien (Szenen u. Automationen) siehe 6.4 • Alarmmodi (Schloss-Symbol) – siehe 3.2.8 • Logbuch (Ereignis-Liste & Filterfunktion) Zentralen (Übersicht) – siehe 6.3
--	---

6.3. Zentralenübersicht

In der Zentralenübersicht der Anlage können Sie neben dem Hinzufügen von neuen Zentralen die bestehenden Zentralen einsehen und darauf zugreifen, Ihre Account-Informationen bearbeiten (1), Ihre Mitglieder verwalten (2) und den Account-Log einsehen (3).



6.3.1.Account-Informationen

Erreichen Sie in der Zentralenübersicht über das Zahnrad.

Zurück

ABUS COMFION
ACCOUNT INFORMATIONEN

Face/Touch ID aktivieren : ☐

Name

E-Mail

Benachrichtigungssprache
Deutsch

Telefonnummer

Benachrichtigungs-Rufnummer

Benachrichtigungs-E-Mail

Erstellt am
2024-11-12 10:50:51

BESTÄTIGEN

ACCOUNT VERWALTUNG

- Face/Touch ID aktivieren
 - Sichert die App durch Face bzw. Fingerprint
- Account Name (Anzeige in Zentrale & Logbuch)
- Account-E-Mail
- Benachrichtigungssprache
 - Definiert die Sprache für die Push,- E-Mail,- SMS Benachrichtigung, Logbuch, Bereiche und Räume
- Telefonnummer
- Benachrichtigungs-Rufnummer für SMS & Anrufe
- Benachrichtigungs-E-Mail für E-Mail-Versand der Zentrale
- Erstellungszeitpunkt des Accounts
- Bestätigungsbutton zum Speichern der Eingaben
- In-App Lösch-Funktion des ABUS-Accounts

6.3.2. Mitglieder

In der Comfion-App haben Sie die Möglichkeit eine Mitgliederliste zu führen. Dies ist rein optional und wird zum Betrieb der Comfion Pro Systeme nicht benötigt. Durch die Mitgliederliste können Sie beim Hinzufügen/Einladen von neuen Benutzern in einer Zentrale, diese ganz einfach aus Ihren Mitgliedern auswählen.

6.3.3. Account-Logbuch

Im Account-Logbuch werden alle Meldungen von zugriffsberechtigten Anlagen aufgeführt. Wenn der Zugriff auf eine Anlage gesperrt ist, werden Log-Einträge von dieser Zentrale nicht im Account-Log gespeichert.

6.4. Automationen & Szenen

Das Comfion Pro System bietet Ihnen die Möglichkeit bis zu 100 Szenarios zu konfigurieren. Diese Szenen oder Automationen können komplett frei eingestellt werden, was Ihnen eine maximale Flexibilität bietet.

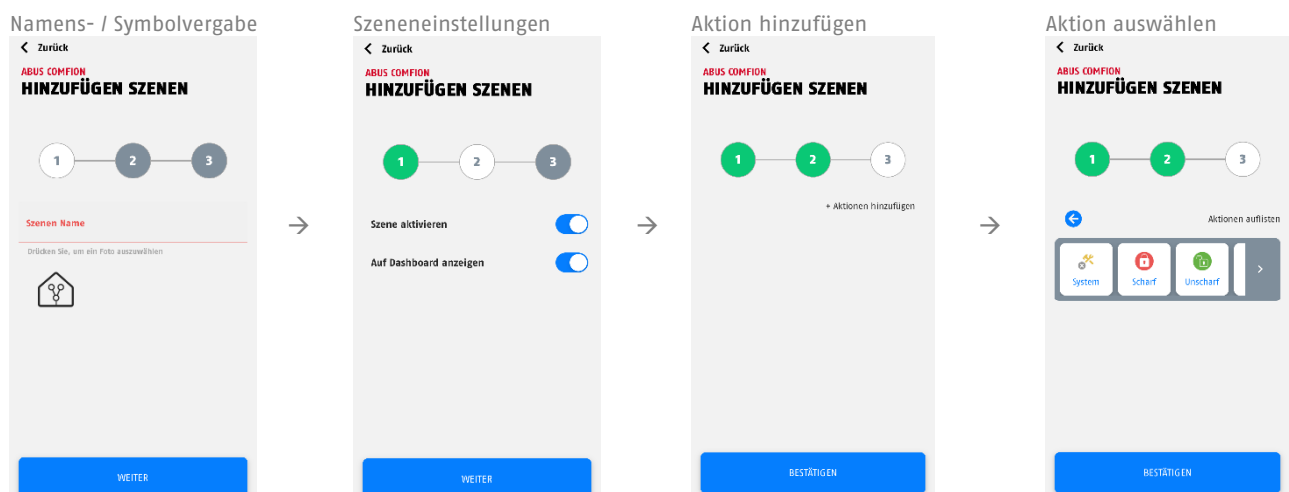
Unter dem Reiter „Szenarien“ können Sie sowohl Szenen als auch Automationen hinzufügen.

 Achtung	Sich gegenseitig widersprechende oder zirkulär aufrufende Automationen dürfen nicht erstellt werden. Hierbei kann es zu schwerwiegenden Funktionsproblemen bei der Zentrale kommen.
---	--

 Hinweis	Achten Sie darauf, dass Sie zwischen zwei Schaltbefehlen für das gleiche Gerät einen Abstand von mindestens 5 Sekunden lassen, um einen reibungsfreien Betrieb sicherstellen zu können.
---	--

Szene = Aktion, welche durch einen Benutzer über die App geschaltet wird (Hotkey). Kann im Dashboard angezeigt werden. Beispiel: Steckdose AN/AUS über App

Beispielkonfiguration einer Szene:



Schritt 1:

- Der Szenen-Name ist ein Pflichtfeld
- Ändern Sie das Symbol durch Klick auf das Icon

Schritt 2:

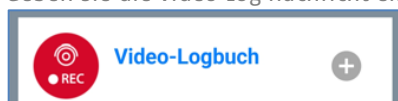
- Legen Sie fest, ob die Szene aktiv oder inaktiv sein soll (inaktiv = Szenen-Name ist ausgegraut)
- Auf Dashboard anzeigen zeigt die Szene im Dashboard im Bereich „Hotkeys“

Schritt 3 (Aktion hinzufügen):

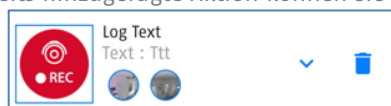
- Wählen Sie die Aktion aus der Liste aus, indem Sie diese anklicken, gegebenenfalls weitere Daten eingeben und abschließend durch Klick auf das „+“ Symbol hinzufügen.

Beispiel: Video-Logbuch:

- Geben Sie die Video Log Nachricht ein, wählen Sie die Kameras aus und drücken dann das „+“ Symbol



- Einige Aktionen können Sie direkt durch Klick auf das „+“ Symbol hinzufügen und danach durch Klick auf das  Symbol weitere Einstellungen ergänzen.
- Eine bereits hinzugefügte Aktion können Sie durch Klick auf die Mülltonne wieder entfernen



- Sie können mehrere Aktionen konfigurieren & diese werden dann nacheinander ausgeführt. Sie können die Reihenfolge der Ausführung ändern, indem Sie auf das Symbol  klicken. Danach können Sie per drag & drop die Aktionen verschieben. Erneuter Druck auf  speichert die Änderung.
- Schließen sie die Konfiguration der Szene am Ende durch „Bestätigen“ ab.

Folgende Aktionen können hinzugefügt werden:

System	Video-Logbuch	Erstellen eines Logbucheintrags mit Log-Nachricht und Ausschnitt der Kameraaufnahme (15 Sek.) bzw. des PIR-Cam Bildes
	Systemneustart	Führt einen Neustart der Comfion Pro Zentrale durch.
	Push-Event Video	Erstellt eine Push-Benachrichtigung mit Nachrichten-Text, Kamerabilder und versendet diese an die ausgewählten Empfänger
	Push-Event Text	Erstellt eine Push-Benachrichtigung mit Nachrichten-Text und versendet diese an die ausgewählten Empfänger
	Verzögerung	Führt die Szene um die angegebene Zeit (Sekunden) verzögert aus bzw. verzögert aufeinanderfolgende Aktionen.
Scharf		Schaltet einen Teilbereich des Systems scharf Hinweis: Nach Hinzufügen dieser Aktion muss noch der Teilbereich festgelegt werden durch Klick auf das Symbol: 
Unscharf		Schaltet einen Teilbereich des Systems unscharf Hinweis: Nach Hinzufügen dieser Aktion muss noch der Teilbereich festgelegt werden durch Klick auf das Symbol: 
Szene		Führt eine bereits konfigurierte Szene aus. Hinweis: Wählen Sie diese Funktion um mehrere Szenen gleichzeitig (oder mit Hilfe der Verzögerung zeitlich versetzt) auszuführen.
Comfion Steckdose	Anschalten	Schaltet die Steckdose an
	Ausschalten	Schaltet die Steckdose aus
	Umschalten	Schaltet die Steckdose um (an → aus, aus → an)
Comfion Relais-Modul	Anschalten	Schaltet das Relaismodul an
	Ausschalten	Schaltet das Relaismodul aus
	Umschalten	Schaltet das Relaismodul um (an → aus, aus → an)
Comfion Jalousie-Modul	Offen	Fährt die Jalousie-Lamellen bis zur Endposition offen & hoch
	Schließen	Fährt die Jalousie-Lamellen bis zur Endposition geschlossen & runter
	Stopp	Stoppt den Offen bzw. Schließen Befehl
	100% nach oben (50% / 1/3 / 25%)	Fährt die Jalousie-Lamellen um den angegebenen Wert hoch
	100% schließen (50% / 1/3 / 25%)	Fährt die Jalousie-Lamellen um den angegebenen Wert runter
	Lamellen öffnen 100% (50% / 1/3 / 25%)	Öffnet die Jalousie-Lamellen um den angegebenen Wert
	Lamellen schließen 100% (50% / 1/3 / 25%)	Schließt die Jalousie-Lamellen um den angegebenen Wert
	Manuelle Steuerung	Individuelle Einstellung der Jalousie-Lamellen. Durch Klick auf das Symbol:  erfolgt Einstellung des Neigungswinkels (5 Stufen) sowie Höhe (10 Stufen) ein.

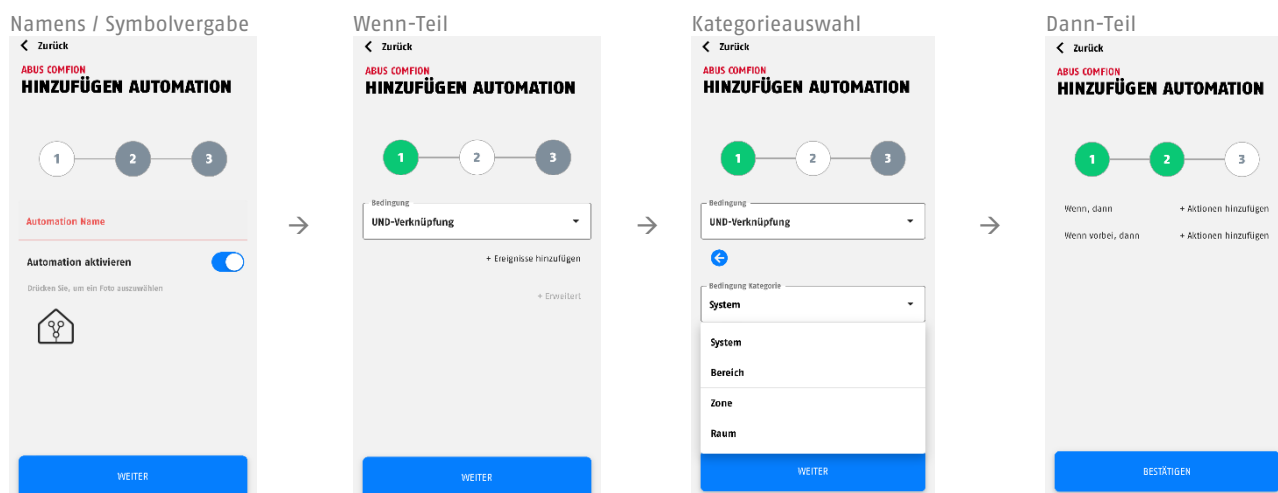
Comfion Pro Zentrale	Ausgang An	Schaltet den Relais-Ausgang der Comfion Pro Zentrale an
	Ausgang Aus	Schaltet den Relais-Ausgang der Comfion Pro Zentrale aus
	Ausgang Umschalten	Schaltet den Relais-Ausgang der Comfion Pro Zentrale um.
Comfion Innensirene	Feuer	Führt die Sprachansage „Feueralarm“ aus
	Alarm	Schaltet den Sirenenton ein (unter v Dauer einstellen max. 180 s)
	Stopp	Schaltet den Sirenenton aus
	Piep (Signalton)	Schaltet den Bestätigungston ein (unter v Anzahl Wiederholungen (max. 30) sowie das Intervall des Piezos (max. 30 s) einstellen
	Fehlgeschlagen	Schaltet den Fehlgeschlagen-Ton ein (unter v Anzahl Wiederholungen (max. 30) sowie das Intervall des Piezos (max. 30 s) einstellen
	Türgong	Schaltet den Tür Gong-Ton ein (unter v Anzahl Wiederholungen (max. 30) sowie das Intervall des Piezos (max. 30 s) einstellen
	Überfall	Führt die Sprachansage „Überfallalarm“ aus
	Wasseralarm	Führt die Sprachansage
Comfion Außensirene	Alarm	Schaltet den Sirenenton ein (unter v Dauer einstellen max. 180 s)
	Stopp	Schaltet den Sirenenton aus
	Piep (Signalton)	Schaltet den Bestätigungston ein (unter v Anzahl Wiederholungen (max. 30) sowie das Intervall des Piezos (max. 30 s) einstellen
	Gong	Schaltet den Gong-Ton ein (unter v Anzahl Wiederholungen (max. 30) sowie das Intervall des Piezos (max. 30 s) einstellen
Comfion Rauchmelder	Alarm Stopp	Schaltet den Alarmton des Comfion Rauchmelders aus. (der Melder löst bei Detektion erneut aus)
WLX-out (Comfion Hybrid-Modul)	Ausgang 1, 2, 3 an	Schaltet den Ausgang 1 bzw. 2 bzw. 3 des Comfion Hybridmoduls an
	Ausgang 1, 2, 3, aus	Schaltet den Ausgang 1 bzw. 2 bzw. 3 des Comfion Hybridmoduls aus
	Ausgang 1, 2, 3 umschalten	Schaltet den Ausgang 1 bzw. 2 bzw. 3 des Comfion Hybridmoduls um
Comfion PIR-Cam / Außen-PIR-Cam	Schnappschuss	Erstellt eine manuelle Bildaufnahme
WLX Pro Zylinder (Access/Intrusion)	Büromodus (Permanenzutritt)	Ergänzt den Büro-Modus (Ermöglicht den Zutritt ohne NRC-Tag) Durch Klick auf das Symbol: v wird ausgewählt, ob der Büromodus „aktiviert“ oder „deaktiviert“ werden soll.
	Remote-Freigabe (Fernöffnung)	Koppelt den Schließzylinder über die App ein und gewährt so Zutritt. Durch Klick auf das Symbol: v legen Sie die Kopplungs-Zeit fest (max. 180 Sek.)
WLX Pro Wand-Leser (Access/Intrusion)	Remote-Freigabe (Fernöffnung)	Steuert den Türöffner (Ausgang an Bridge-Box) über die App ein und gewährt so Zutritt. Durch Klick auf das Symbol: v legen Sie die Impulsdauer fest (6 oder 12 s)
IP-Kamera (IPxxxxxxx)	Gehe zu Preset	Richtet die PTZ-Kamera zu einer vorher definierten Position aus. Durch Klick auf das Symbol: v Auswahl von Position 1, 2, 3 oder 4.

- Klicken sie auf bereits konfigurierte Szenen, um diese erneut zu bearbeiten oder zu löschen.

Automation = besteht immer aus Wenn- und Dann-Teil. Frei konfigurierbar.

Beispiel: Wenn Anlage scharf, Dann Licht aus

Beispielkonfiguration einer Automation:



Schritt 1:

- Tragen Sie den Automations-Namen ein (Pflichtfeld)
- Legen Sie fest, ob die Automation aktiviert oder deaktiviert ist
- Ändern Sie das Symbol durch Klick auf das Icon

Schritt 2: (Wenn Ereignis festlegen)

- Wählen Sie zwischen einer Und-Verknüpfung bzw. einer Oder-Verknüpfung.
 - Bei der Und-Verknüpfung müssen ALLE Bedingungen erfüllt sein, dass die Aktion ausgeführt wird. Bei der Oder-Verknüpfung muss mindestens EINE Bedingung erfüllt sein, dass die Aktion ausgeführt wird.
- Wählen Sie das „Wenn“ Ereignis aus.
 - Es können mehrere Ereignisse eingerichtet werden, die entweder ALLE (Und-Verknüpfung) oder mindestens EINE (oder-Verknüpfung) erfüllt sein müssen.
- Folgende Wenn Ereignisse können ausgewählt werden:
 - System -> Hier finden Sie Systemereignisse wie ein Stromausfall, aber auch den Zeitplan
 - Regel -> Bestehende Automationen können in eine Automation eingebunden werden ...
 - Bereich -> Hier sind Bereichs-Ereignisse wie Scharf/Unscharf, Einbruch, Bereit zum Scharfschalten uvm. zu finden
 - Zone -> Hier sind alle Zonen-Bezogenen Ereignisse zu finden (z.B. Zone Einbruch)
 - Raum -> Hier sind alle Komponenten und die damit verbunden Ereignisse zu finden (z.B. Öffnungsmelder Kontakt geöffnet oder Wandtaster Taste gedrückt)
- Wählen Sie ergänzend unter „Erweitert“ aus, ...
 - ... wie lange die eingestellten Bedingungen zutreffen müssen, bis die Aktion ausgeführt wird. Nur wenn die Bedingungen für den Zeitraum der eingestellten Zeit zutreffen und sich nicht mehr verändern, wird die Aktion ausgeführt.
 - Beispiel: Wenn Tür offen für 30 Sekunden, Dann... Push-Benachrichtigung verschicken.

Schritt 3: (Dann Ereignis festlegen)

- Die „Wenn, dann“ -> Aktion wird ausgeführt, wenn die im Wenn-Teil bestimmten Bedingungen zutreffen
 - Die hier konfigurierbaren Aktionen entsprechen denen im Szenen-Konfigurator (Schritt 3)
- „Wenn vorbei, dann“ -> Aktion wird ausgeführt, wenn die im Wenn-Teil bestimmten Bedingungen NICHT mehr zutreffen

Bearbeiten einer Szene/Automation

Zum Bearbeiten halten Sie das Symbol der Szene/Automation für etwas 2 Sekunden gedrückt und lassen es wieder los

Löschen einer Szene/Automation

Sie können eine Szene/Automation löschen, indem Sie in den Bearbeitungsmodus gehen (siehe „Bearbeiten einer Szene/Automation“) und anschließend auf den Button „Szene/Automation löschen“ im unteren Bildrand klicken.

6.5. Resets



6.5.1. Werksreset

Um die Zentrale auf Werkseinstellungen zurückzusetzen, halten Sie die Reset-Taste (Taste 12 siehe 2.3 *Gerätebeschreibung*) für >10 Sekunden gedrückt und lassen sie wieder los. Die LEDs der Zentrale werden sich nach wenigen Sekunden ausschalten und die Zentrale führt einen Neustart durch. Nach dem Neustart befindet sich die Zentrale auf Werkseinstellungen und kann neu eingerichtet werden.

6.5.2. Neustart (Reboot)

Halten Sie die Reboot-Taste (Taste 13) für 2 Sekunden gedrückt. Die LEDs der Zentrale schalten sich kurz aus. Die Zentrale führt einen Neustart durch.



Hinweis

Bei dem hier beschriebenen Neustart wird die Stromversorgung nicht unterbrochen. Falls z.B. im Rahmen eines Neustart-Vorgangs die Zentrale manuell von der Stromversorgung getrennt wird, führt die Zentrale nach Abschluss des Neustart-Vorgangs eine Prüfung aller angeschlossenen Geräte durch & diese Prüfung führt zu vielen Logbuch Einträgen.

6.5.3. User-Reset

Um die Benutzer der Anlage zurückzusetzen, bzw. alle Benutzer von der Anlage zu löschen, drücken Sie die Netzwerk-Reset-Taste (Nr. 14) 5x innerhalb von 5 Sekunden. Nach einigen Sekunden wechselt die Internet-LED kurzzeitig auf Rot. Sie sollten auf den verbundenen Geräten eine Push-Mitteilung erhalten, dass die betroffene Zentrale entfernt wurde.

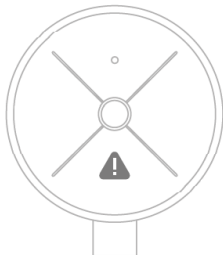
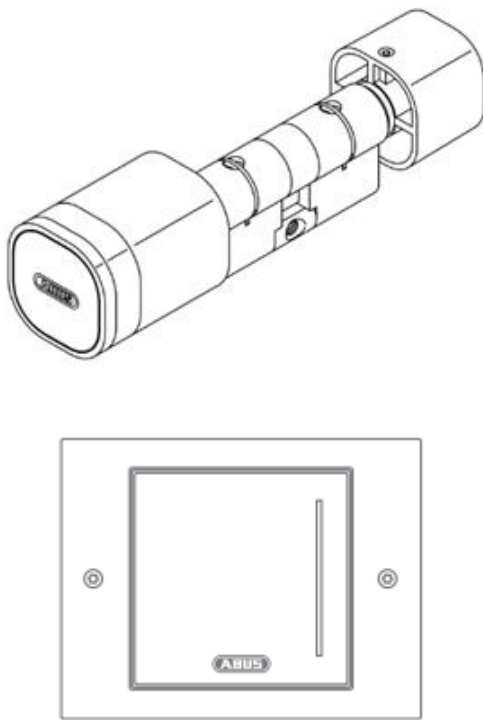
Wenn alle LEDs wieder grün leuchten (Internet LED kann grün blinken), können Sie die Anlage über das +-Symbol in Ihrer App wieder neu hinzufügen.

6.5.4. Netzwerk-Reset

Falls Sie Ihre Anlage im Netzwerk aufgrund falscher IP-Einstellungen nicht mehr erreichen können, ist es möglich die Zentrale auf DHCP zurückzustellen. Halten Sie hierfür die Netzwerk-Rückstellung Taste auf der Rückseite der Zentrale (Nr. 14) für 6 Sekunden gedrückt. Nach einigen Minuten sollte die Anlage wieder erreichbar sein.

6.6. Bedienung

6.6.1. Scharf- / Unscharfschaltung

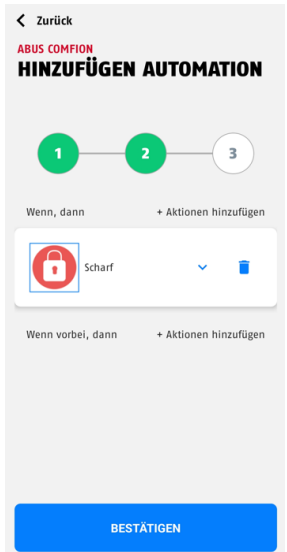
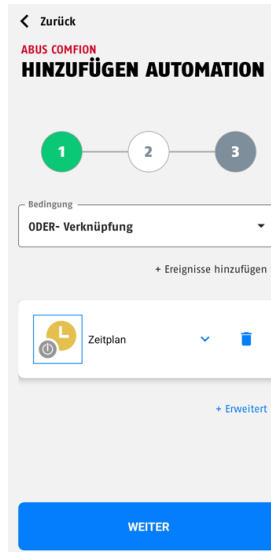
APP: Die Scharf-/Unscharfschaltung kann in der App durch die Ausführung der Alarmmodi durchgeführt werden. Klicken Sie hierzu im Dashboard auf den mittigen Button im unteren Bildrand (Schloss-Symbol) und wählen Sie anschließend die Aktion aus (z.B. Gesamt scharf).	
BEDIENTEIL: Sie können das System über ein Funk-Bedienteil scharf- und unscharf schalten. Geben Sie hierzu Ihren Benutzercode ein bzw. halten den NFC-Tag vor das Bedienteil und klicken anschließend auf die auszuführende Aktionsfläche (Schloss-Tasten). Genauere Informationen finden Sie im User-Guide oder in der Anleitung des Bedienteils	
FERNBEDIENUNG: Sie können die Tasten Ihrer Funk-Fernbedienung mit den Alarmmodi belegen und hiermit durch einen Tastendruck die jeweilige Aktion ausführen. Die Einstellung finden Sie unter der Fernbedienung.	
WLX-Pro Zylinder / WLX Pro Wall-Reader: erfolgt direkt am Leser Scharf-Schalten: • RFID-Tag am Leser präsentieren • Innerhalb der Öffnungs-Zeit ggf. verriegeln und den RFID-Tag erneut präsentieren • Scharf erfolgreich: Rote LED 1 x lang • nicht erfolgreich: Rote LED 6 x Unscharf-Schalten: • RFID-Tag am Leser präsentieren • Nach erfolgreichem Unscharf-Schalten koppelt der Zylinder ein und Grüne LED blinkt 1 x lang • Nicht erfolgreich: Rote LED blinkt 6x  Hinweis Bei unterbrochener Funkverbindung wird nach dem dritten erfolglosen Lesevorgang die Fallback-Funktion ausgeführt. Weitere Details siehe Kapitel 6.1.8	

AUTOMATION: Über eine Automation können Sie die Scharfschaltung oder Unscharfschaltung der Anlage an Bedingungen knüpfen. Hiermit kann beispielsweise nach einem Zeitplan, oder beim Ansteuern eines Drahteingangs geschaltet werden.



Achtung

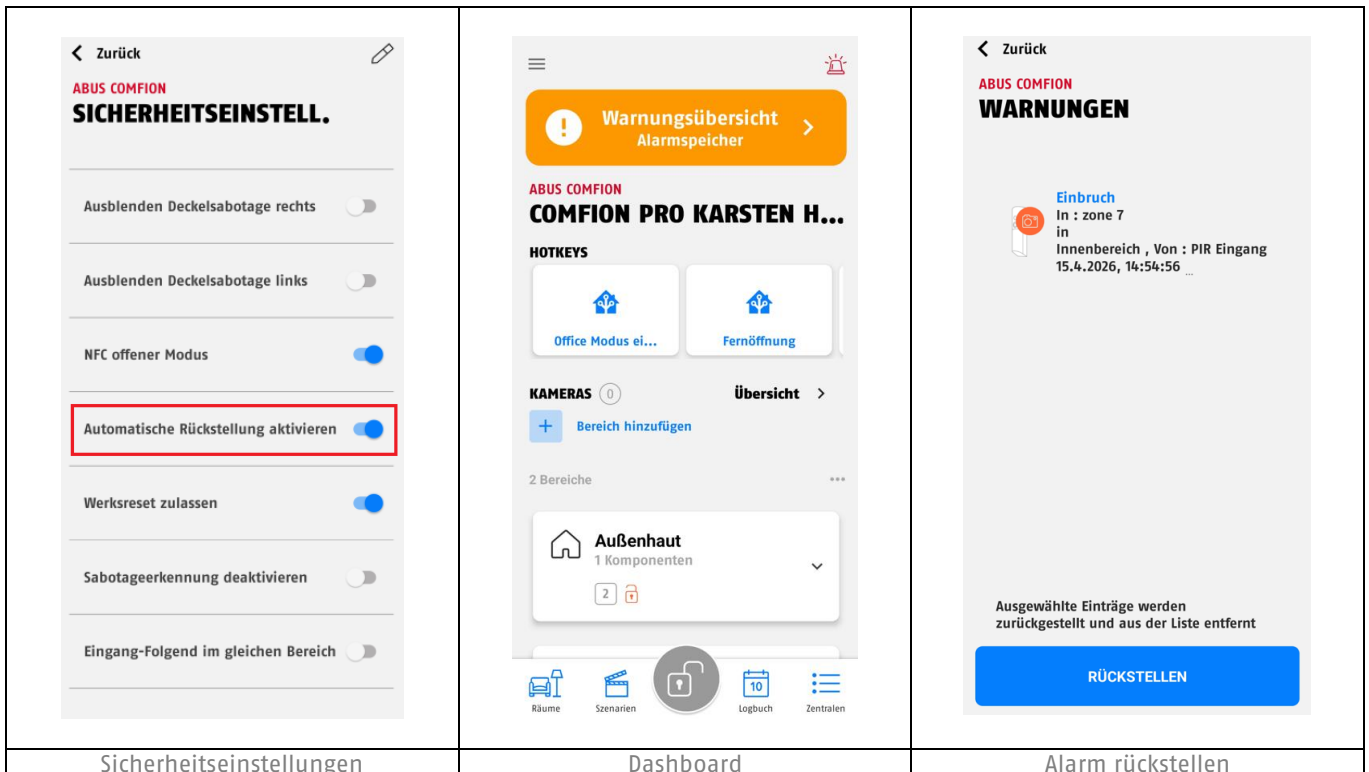
Nach EN 50131 darf die Unscharfschaltung nur durch berechtigte Personen erfolgen. Eine zeitgesteuerte Scharfschaltung darf nur unter Einhaltung der Zwangsläufigkeit (z.B. Benutzer muss das Gebäude verlassen und die Tür verriegeln bevor geschärft werden kann) und im störungsfreien Zustand der Anlage erfolgen. Der Scharfschalt Vorgang sollte in diesem Fall akustisch u./o. optisch angekündigt werden.



6.6.2. Rückstellung von Alarmen

Die Rückstellung des Comfion Pro Systems kann je nach Einstellung über folgende Wege erfolgen:

- Bei aktivierter Option „Automatische Rückstellung aktivieren“ (Unter Zentralen-Konfig. – Sicherheitseinstellungen) setzt die Zentrale bei der Unscharfschaltung, wenn die betroffenen Melder geschlossen sind, automatisch den Alarm zurück.
- Bei deaktivierter Option „Automatische Rückstellung“ (Unter Zentralen-Konfig. – Sicherheitseinstellungen) wird nach einem Alarm die Meldung im oberen Bildrand der App angezeigt und muss manuell vom Nutzer zurückgestellt werden.



Sicherheitseinstellungen

Dashboard

Alarm rückstellen

6.6.3. Zwangsscharf

Durch die Funktion „Zwangsscharf“ kann die Zentrale trotz einer ausgelösten/offenen Zone scharfgeschaltet werden. Die betroffene Zone wird hierbei ohne weiteres Zutun ausgeblendet. Es ist kein weiteres manuelles Ausblenden des Melders notwendig.



Hinweis

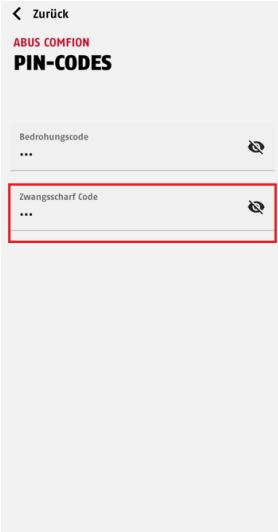
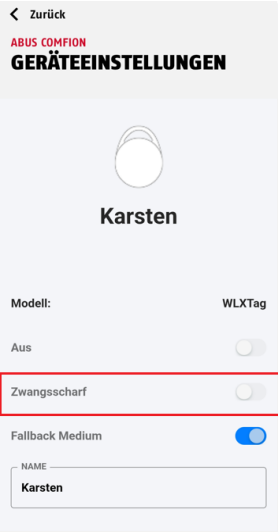
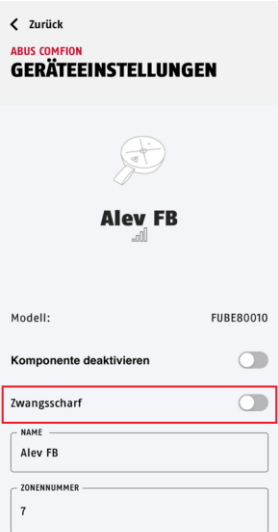
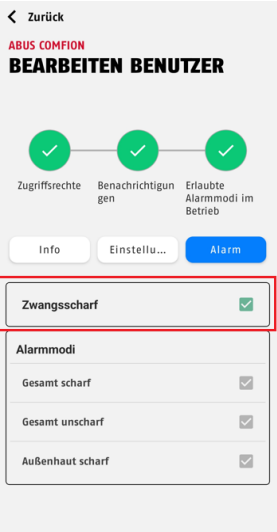
Bitte beachten Sie, dass die Funktion Zwangsscharf nur dann ausgeführt werden kann, wenn die ausgelöste/offene Zone das Zonenverhalten „**Ausblendbar**“ besitzt.

Für die Zwangsscharfschaltung **über das Bedienteil** kann unter der Zentralen-Konfiguration unter „PIN-Codes“ (siehe **Kapitel 6.1.4**) der Zwangsscharfcode festgelegt werden. Dieser 3-stellige Code wird hinter dem 4-stelligen Benutzercode eingegeben, um über das Bedienteil zwangsscharf zu schalten.

Zudem kann einem **Transponder** die Eigenschaft Zwangsscharf zugewiesen werden, um mit diesem zu schalten.

Für die Zwangsscharfschaltung **über die Funk-Fernbedienung** kann unter den Einstellungen der Fernbedienung der Haken bei „Zwangsscharf“ gesetzt werden.

Für die Zwangsscharfschaltung **über die App** kann unter jedem Benutzer im Reiter „Alarm“ der Haken bei „Zwangsscharf“ gesetzt werden.

			
Bedienteil & Zwangsscharfcode	Transponder-Einstellungen	Fernbedienung	Benutzereinstellungen Alarm

6.7. Symbolerklärung

Stromversorgung	
	Ladezustand Batterie (bzw. Akku) 100% / 75% / 50% / 25% / Batterie Leer
	Links: externe Spannungsversorgung (DC oder AC) angeschlossen Rechts: Notstromversorgung (Akku) im Standby
Funksignal	
	4 Balken = Excellent 3 Balken = Sehr gut 2 Balken = moderat 1 Balken = schlecht
	Funkverbindung unterbrochen. Erfolgt nach Ausfall des Supervisionssignals der jeweiligen Komponente d.h. nach > 1 Std. (kann bei einzelnen Komponenten abweichen)
Geräteverhalten	
	Komponente ausgelöst (z.B. Öffnungsmelder geöffnet, Erschütterungsmelder ausgelöst, Rauchmelder ausgelöst, Wassermelder ausgelöst)
	Bewegung erkannt (PIR-Bewegungsmelder / Mikrowelle-Bewegungsmelder)
	Gerät ausgelöst (z.B. Sirene angesteuert, Tastendruck)
	Zone geschlossen (z.B. Öffnungsmelder geschlossen)
	Zone geöffnet (z.B. Öffnungsmelder geöffnet) → Erscheint zusätzlich zum Symbol „Komponente ausgelöst“

Störungen	
	Sabotage erkannt (z.B. Gehäuse geöffnet oder Gerät von Montagefläche entfernt) Alternativsymbol: 
	Kabelbruch erkannt (z.B. 3in1 Melder)
Aktions-Icons (ein Druck auf das Icon löst die beschriebene Aktion aus)	
	Gerätestatus AUS (z.B. Funksteckdose ausgeschaltet) → Druck auf das Symbol schaltet das Gerät EIN
	Gerätestatus EIN (z.B. Funksteckdose eingeschaltet) → Druck auf das Symbol schaltet das Gerät AUS
	PIR-Kamera 1. Aufnahme Erstellen (Druck auf Symbol löst die manuelle Aufnahme aus) 2. Aufnahme wird erstellt 3. Aufnahme wird an Zentralen-Speicher übertragen.
WLX-Icons (Zutrittskontrolle)	
	Zutritt gewährt Anzeige erfolgt für die Zeit, in welcher der Zylinder eingekoppelt ist (6/12 sek)
	Permanent Zutritt ist aktiviert (Büromodus eingeschaltet)  Hinweis Der Permanent Zutritt ist eine Konfiguration in der Zentrale. Zur Ausführung muss der Zylinder zunächst aufgeweckt (d.h. gedreht) werden und eine Funkverbindung zur Zentrale aufbauen. Im Anschluss wird der Zutritt gewährt.
	Teilbereich scharfgeschaltet Die Teilbereiche denen der Zylinder / Wall-Reader zugeordnet ist, sind scharf geschaltet

6.8. ABUS-Cloud

Das Comfion Pro Funk-Sicherheitssystem verbindet sich bei der Erstinbetriebnahme mit der Abus Cloud. Die Anlage wird zudem im Abus Cloud Facherrichter-Account des Installateurs hinterlegt. Sollte dies nicht gewünscht sein, kann unter dem jeweiligen Benutzer in der Anlage der Haken bei „Haupt-Installateur“ entfernt werden, bzw. auch bei einem anderen Installateur gesetzt werden.

6.9. Hinweise zur Festplatte / SSD-Datenspeicher

- Die Schrauben zur Befestigung der Festplatte dürfen nur per Hand festgezogen werden
- Die Akkulaufzeit der Zentrale wird durch die eingebaute Festplatte und dessen Stromverbrauch, sowie der Anzahl der angeschlossenen BUS-Teilnehmer beeinflusst.
 - Die gemäß EN 50131 geforderte Notstromzeit für Einbruchmeldezentralen nach EN Grad 2 ist durch den Einsatz eines SSD-Datenspeichers und den Anschluss von bis zu 2 BUM080000 WLX Pro Modulen am Comfion Pro BUS sichergestellt!
- Die in der Comfion Pro verbaute Festplatte muss im Format exFAT oder NTFS formatiert sein
- Tauschen Sie die Festplatte/SSD-Datenspeicher nur im spannungslosen Zustand der Zentrale

6.10. Wartung und Instandhaltung durch Errichter

Testen Sie bei der routinemäßigen Wartung, dass das System ordnungsgemäß funktioniert:

- Überprüfen Sie die Comfion Pro auf offensichtliche Anzeichen von Schäden an dem Gehäuse, Wandhalterung oder der Frontabdeckung.
- Überprüfen Sie die Wirkung des Sabotageschalters
- Überprüfen Sie den Zustand der Notstrom-Akkus
- Reinigen Sie die das Gehäuse
 - Zum Reinigen wischen Sie bitte die Oberfläche mit einem trockenen, weichen Tuch ab.
 - Benutzen Sie kein Wasser, keine Lösungsmittel und keine Reinigungsmittel.
- Kontrollieren Sie die Signalstärke und den Batterie-/ Akkuzustand aller Komponenten
- Ersetzen Sie die Batterien bzw. Akkus wie in den Anweisungen des Herstellers empfohlen
- Testen Sie jede Komponente.
- Reinigen Sie vorsichtig die Linsen aller PIR-Melder und Kameras mit einem sauberen, trockenen, weichen Tuch.
 - Benutzen Sie kein Wasser, keine Lösungsmittel und keine Reinigungsmittel.
- Führen Sie einen Gehtest aller Melder durch.
- Testen Sie alle Signalgeber
- Testen Sie die Kommunikation.

 Hinweis	ABUS empfiehlt einen Wechsel des Zentralen Akkus nach maximal 3 Jahren. Bei längerer Laufzeit kann ein plötzlicher Leistungsabfall nicht ausgeschlossen werden.
--	---

So wechseln Sie den Akku der Zentrale:

- Setzen Sie die Zentrale in den Wartungsmodus (Sicherheitseinstellungen)
- Entfernen Sie die Zentrale von der Wandhalterung
- Schalten Sie den Akku-Schalter auf „AUS“
- Öffnen Sie die Frontabdeckung durch Lösen der Rückseitigen Schrauben und Aufhebeln der Abdeckung (Weitere Details finden Sie in **Kapitel 3.1** Wandmontage der Zentrale)
- Trennen Sie die Spannungsversorgung sowie den alten Akku von der Zentrale
- Warten Sie 30 Sekunden
- Schließen Sie den neuen Akku sowie die Spannungsversorgung wieder an
- Schließen Sie den Deckel der Anlage und verlassen anschließend wieder den Wartungsmodus

6.11. Tabelle Funk-Signalstärken

Die folgende Tabelle beschreibt die Bedeutung der in dBm angezeigten Signalwerte der Comfion-Funk-Komponenten.

RSSI-Wert (dBm)	Bedeutung	Anzeige an Komponente
≤ -100	Schlecht	0 Balken
≤ -96	OK	1 Balken
≤ -91	Gut	2 Balken
≤ -86	Sehr gut	3 Balken
> -86	Exzellent	4 Balken

7. Gewährleistung

- ABUS-Produkte sind mit größter Sorgfalt konzipiert, hergestellt und nach geltenden Vorschriften geprüft.
- Die Gewährleistung erstreckt sich ausschließlich auf Mängel, die auf Material- oder Herstellungsfehler zum Verkaufszeitpunkt zurückzuführen sind. Falls nachweislich ein Material- oder Herstellungsfehler vorliegt, wird das Modul nach Ermessen des Gewährleistungsgebers repariert oder ersetzt.
- Die Gewährleistung endet in diesen Fällen mit dem Ablauf der ursprünglichen Gewährleistungszeit von 2 Jahren. Weitergehende Ansprüche sind ausdrücklich ausgeschlossen.
- ABUS haftet nicht für Mängel und Schäden, die durch äußere Einwirkungen (z.B. durch Transport, Gewalteinwirkung, Fehlbedienung), unsachgemäße Anwendung, normalen Verschleiß oder durch Nichtbeachtung dieser Anleitung sowie der Pflege-Hinweise entstanden sind.
- Bei Geltendmachung eines Gewährleistungsanspruches ist dem zu beanstandendes Produkt der originale Kaufbeleg mit Kaufdatum und eine kurze schriftliche Fehlerbeschreibung beizufügen.
- Sollten Sie an dem Produkt einen Mangel feststellen, der beim Verkauf bereits vorhanden war, wenden Sie sich innerhalb der ersten zwei Jahre bitte direkt an Ihren Verkäufer.

8. Entsorgungshinweise



Entsorgen Sie das Gerät gemäß der Elektro- und Elektronik-Altgeräte EU Richtlinie 2012/19/EU – WEEE (Waste Electrical and Electronic Equipment). Bei Rückfragen wenden Sie sich an die für die Entsorgung zuständige kommunale Behörde. Informationen zu Rücknahmestellen für Ihre Altgeräte erhalten Sie z.B. bei der örtlichen Gemeinde- bzw. Stadtverwaltung, den örtlichen Müllentsorgungsunternehmen oder bei Ihrem Händler.

9. Konformität

9.1. EU-Konformitätserklärung

Hiermit erklärt ABUS Security Center GmbH & Co. KG, dass der Funkanlagentyp FUAA85000 der Richtlinie 2014/53/EU und 2011/65/EU entspricht. Der vollständige Text der EU-Konformitätserklärung ist unter der folgenden Internetadresse verfügbar: abus.com > Artikelsuche > FUAA85000 > Downloads

9.2. Konformität nach EN 50131

Das Sicherheitssystem FUAA85000 ist zertifiziert nach Sicherheitsgrad 2 bei ordnungsgemäßer Installation konform gemäß EN 50131-1+A3:2020, EN 50131-3:2009, EN 50131-10:2014, EN 50136-1+A1:2018, EN 50136-2:2013 und EN 50131-5-3:2017.

10. Anhang

10.1. Contact-ID Codetabelle

Code	Code-Klasse	Zusatzdaten	Typ	Beschreibung
111	Feuer Alarm	Zone	Rauch	Ein Rauchmelder hat einen 24 Stunden Feueralarm ausgelöst
120	Panik Alarm	Zone	Panik	Am Bedienteil wurde Panik Alarm ausgelöst
121	Panik Alarm	Benutzer	Bedrohung	Ein Benutzer hat den Bedrohungscode eingegeben
130	Einbruch Alarm	Zone	Einbruch	Eine Einbruch-Zone wurde bei scharfgeschalteter Anlage ausgelöst
131	Einbruch Alarm	Zone	Perimeter	Eine Perimeter-Zone löst einen Voralarm aus
133	Einbruch Alarm	Zone	24 Std. Zone	Eine 24 Stunden Einbruchalarm-Zone wurde ausgelöst
134	Einbruch Alarm	Zone	Ein-/Ausgang	Eine Eingangs/Ausgangs-Zone wurde bei scharfgeschalteter Anlage ausgelöst
135	Einbruch Alarm	Zone	Sofort Überwacht Zone	Eine Sofort (Überwacht) Zone wurde bei scharfgeschalteter Anlage ausgelöst
137	Einbruch Alarm	Zone	Sabotage	Zentralen-Sabotage wurde ausgelöst
139	Einbruch Alarm	Zone	Glasbruch	Einbruch durch eine Zone bestätigt
154	24 Stunden Technischer Alarm	Zone	Wasseralarm	Wassermelder meldet Fehler
301	System Störung	Zone	Ausfall AC-Netzspannung	Verlust der Netzspannung der Zentrale oder Erweiterungsmodul bei entschärfter Anlage
302	System Störung	Zone	Akku-Störung	Leerer Pufferakku der Zentrale im unscharfen Zustand
305	System Störung	Zone	Reset	Das System wurde zurückgesetzt und neu gestartet
306	System Störung	Zone	Neustart	Das System hat einen Neustart durchgeführt
308	System Störung	Zone	Abschalten	Das System wurde heruntergefahren und hat den Betrieb eingestellt
311	System Störung	Zone	Akku fehlt /außer Betrieb	Die Pufferbatterie der Zentrale fehlt oder ist vollständig entladen
338	Peripherie Störung	Zone	Bedienteil gesperrt	das Bedienteil ist aufgrund mehrmaliger falscher Codeingabe gesperrt
344	Peripherie Störung	Zone	Jamming Erkennung	Der Funk-Empfänger hat ein Störsignal (Jamming) erkannt.
350	Kommunikation Störung	Zone	Komm.-Fehler	Das System hat einen Kommunikationsfehler festgestellt.
381	Melder Störung	Zone	Supervision	Die angegebene Zone hat sich im Supervisionsintervall nicht gemeldet.
383	Melder Störung	Zone	Sabotage	Es wurde Sabotage an der betreffenden Zone ausgelöst
384	Melder Störung	Zone	Batterie schwach	Es wurde leere Batterie an der betreffenden Zone ausgelöst
393	Melder Störung	Zone	Störung Wartung	Die betreffende Zone hat eine Störung gemeldet
400	Schärfen/Entschärfen/Fernzugriff	Benutzer	Scharf/Unscharf	der betreffende Benutzer hat das System via Fernbedienung scharf bzw. unscharf geschaltet
401	Schärfen/Entschärfen/Fernzugriff	Benutzer	Scharf/Unscharf via Benutzer	der betreffende Benutzer hat das System via Smartphone APP scharf bzw. unscharf geschaltet
406	Schärfen/Entschärfen/Fernzugriff	Benutzer	Zurücksetzen	der betreffende Benutzer hat den zuvor ausgelösten Alarm zurückgesetzt
407	Schärfen/Entschärfen/Fernzugriff	Benutzer	Scharf/Unscharf via Bedienteil	der betreffende Benutzer hat das System durch ein Funk-Bedienteil scharf bzw. unscharf geschaltet

443	Schärfen/Entschärfen/ Fernzugriff	Benutzer	Schärfen mit Ausblenden	der betreffende Benutzer hat das System durch Ausblenden von Störungen scharf geschaltet
454	Schärfen/Entschärfen/ Fernzugriff	Benutzer	Schärfen fehlgeschlagen	Das System konnte nach Ausgangsverzögerung nicht scharfgeschaltet werden
461	Schärfen/Entschärfen/ Fernzugriff	Zone	Falsche Codeeingabe	Am Bedienteil wurde ein falscher Code eingegeben.
570	Ausblenden	Zone	Zone ausblenden	die betreffende Zone wurde ausgeblendet
572	Ausblenden	Zone	24 Std. Zone ausblenden	die betreffende 24 Std. Zone wurde ausgeblendet
602	Test	-	Periodische Testmeldung	Es wurde eine periodische Testmeldung an die Leitstelle übertragen.

ABUS I Security Center GmbH & Co. KG
abus.com

Linker Kreuthweg 5
86444 Affing
Germany

Tel: +49 82 07 959 90-0



Security Tech Germany

FUAA85000

INSTALLATION MANUAL

Comfion Pro Wireless Security system



1.	Updates	5
1.1.	Instructions	5
1.2.	Comfion Pro Firmware & Release Notes	5
2.	General	6
2.1.	Introduction	6
2.2.	Intended use / Legal notices	6
2.3.	Customer Service / Customer Support	6
2.4.	Legal Notice	6
2.5.	Explanation of symbols	7
3.	Operating principle and performance features	7
3.1.	product features	7
3.2.	Contents	8
3.3.	Device description	9
3.4.	Technical specifications	11
4.	Installation & commissioning	12
4.1.	Wall mounting of the control panel	12
4.2.	Commissioning of the system	14
4.2.1.	Setup via the app & finalising hardware preparations	15
4.2.2.	Dashboard (after initial login)	18
4.2.3.	Areas	18
4.2.4.	Rooms	19
4.2.5.	Components	20
4.2.6.	Component settings	22
4.2.7.	Wiring instructions (inputs/outputs/BUS)	23
4.2.8.	Alarm modes	24
4.3.	WLX Pro Installation & Programming	25
4.3.1.	Installation, configuration and use of WLX Pro cylinders and wall readers	26
4.3.2.	WLX Pro functions – remote opening and office mode	27
4.4.	Cameras (NVR)	28
4.4.1.	Integrating cameras via ONVIF	28
4.4.2.	Integrating cameras via RTSP	29
4.4.3.	Camera settings (global)	30
4.4.4.	Camera settings (individual)	30
4.4.5.	NVR operation	32

5. Users and permission groups	33
5.1. Explanation of the different roles	33
5.2. Commissioning	34
5.2.1. Handover to the owner	34
5.3. Inviting/adding users	34
5.4. Editing users	34
5.4.1. Access rights	34
5.4.2. Notifications	35
5.4.3. Permitted alarm modes in operation	36
5.5. Deleting users	36
6. Communication	36
6.1. Modem (Mobile module)	36
6.2. Email	37
6.3. Telephone call	37
6.4. SMS	38
6.5. SIA DC-09 (Control Centre Connection)	39
7. General, Maintenance and Notes	40
7.1. Control panel configuration	40
7.1.1. General information	40
7.1.2. Network	40
7.1.3. Security settings	41
7.1.4. PIN codes	42
7.1.5. Notification delays	42
7.1.6. HomeKit	43
7.1.7. Backup	43
7.1.8. WLX Information	44
7.2. Dashboard (System set up)	45
7.3. Control Centre overview	46
7.3.1. Account information	46
7.3.2. Members	46
7.3.3. Account Log	46
7.4. Automations & Scenes	47
7.5. Resets	50
7.5.1. Factory reset	50
7.5.2. Reboot	50

7.5.3.	User reset	51
7.5.4.	Network reset	51
7.6.	Operation	52
7.6.1.	Arming / Disarming	52
7.6.2.	Resetting alarms	53
7.6.3.	Forced arming	54
7.7.	Key to symbols	55
7.8.	ABUS Cloud	57
7.9.	Notes on the hard drive / SSD data storage	57
7.10.	maintenance and servicing by the installer	57
7.11.	Table of wireless signal strengths	58
8.	Warranty	58
9.	Disposal instructions	58
10.	Conformity	58
10.1.	EU Declaration of Conformity	58
10.2.	Conformity to EN 50131	58
11.	Appendix	59
11.1.	Contact-ID Code Table	59

1. Updates

1.1. Instructions

Version	Date Publication	Changes
1.0	12 May 2026	Initial version
1.1	13 May 2026	Additions: - New: Chapter 1 Updates (previously Chapter 7) - Chapter 3.2.6: Addition: IP cameras & MotionAlarm - New: Chapter 3.3 WLX Pro Installation & Pairing - New: Chapter 3.4.3 Camera settings (global) - New: Chapter 3.4.4 Camera settings (individual) - New: Chapter 3.3.2 Integrating cameras via RTSP - New: Chapter 10.1 Contact-ID Code Table - Chapter 6.6.1: Arming/Disarming WLX Pro Cylinder & Wallreader added
1.2	30 June 2026	Additions: - Added English, French, Dutch language version - Added release notes for Comfion Pro Firmware 1.0.2945

1.2. Comfion Pro Firmware & Release Notes

Firmware version	APP Version	Date Release	Changes
1.0.2864	2.1.96	12 May 2026	Initial version
1.0.2945	2.1.134	30 June 2026	Changes: - Adjustment of FUBE80100 default values to increase battery life - Adjustment of FUBE80100 wake-up time to increase battery life - Adjustment of various log entries (addition of user, area, etc.) - Adjustment of hybrid module preconfiguration when used with wAppLoxx - Improvements to H.265 video stream - Security adjustments - String- and Design Adjustments Bug Fixes: - Inevitability of WLX Access components - Permission message "Access to Gallery" upon app launch - Correction of security settings— gateway tamper

You can find the release notes for the latest firmware update in your Comfion app or via the following link:

<https://l.ead.me/bgjCEA>

2. General

2.1. Introduction

Thank you for choosing the **Comfion Pro wireless security system**, a product from ABUS Security Center (also referred to as "ABUS" for short).

This manual contains essential descriptions, technical data, overviews and further information on the planning, commissioning and operation of the **Comfion Pro wireless security system**.

The products/systems described here may only be installed and maintained by persons qualified for the respective task. Qualified personnel for the installation and maintenance of the system are generally trained ABUS specialist partners.

2.2. Intended use / Legal notices

Responsibility for the legally compliant use of the product lies with the purchaser or customer and the end user. In accordance with the manufacturer's liability for its products as defined in the Product Liability Act, the above information must be observed and passed on to operators and users. Failure to comply releases ABUS Security Center from legal liability.

Use that is not in accordance with the agreement or is unusual, repair work or modifications not expressly approved by ABUS, and improper servicing may lead to malfunctions and must be avoided. Any modifications not expressly approved by ABUS will result in the loss of liability, warranty and separately agreed guarantee claims.

Architects, building services engineers and other advisory bodies are required to obtain all necessary product information from ABUS in order to comply with the information and instruction obligations under the Product Liability Act. Specialist retailers and installers are required to observe the instructions in the ABUS documentation and, where applicable, to pass these on to their customers.

Further information can be found at www.abus.com on the general website or, for dealers and installers, in the partner portal at <https://partner-asc.abus.com/>

2.3. Customer Service / Customer Support

Our support team is available to assist you: support@abus-sc.com

General information on the **Comfion Pro wireless security system** can be found on our homepage at: <https://www.abus.com/de/Privat/Alarmsysteme/Comfion-Funk-System>

2.4. Legal Notice

This edition will cease to be valid upon the publication of a newer installation guide.

All rights reserved. Without the written consent of the publisher, these installation instructions may not be reproduced in any form, in whole or in part, or duplicated or processed using electronic, mechanical or chemical processes.

ABUS Security Center accepts no liability for technical or printing errors and their consequences. The information in these installation instructions has been compiled to the best of our knowledge and belief, taking into account the current state of the art. It is reviewed regularly and updated or corrected as necessary.

All trademarks and intellectual property rights are acknowledged; changes in the interests of technical progress may be made without prior notice.

2.5. Explanation of symbols

The following symbols are used in these installation instructions:

Symbol	Signal word	Meaning
	Caution	Indicates a risk of injury or a health hazard due to electrical voltage
	Important	Indicates possible damage to the device/accessories or a risk of injury or health hazard
	Note	Indicates important information

3. Operating principle and performance features

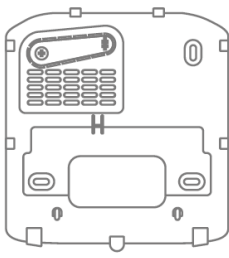
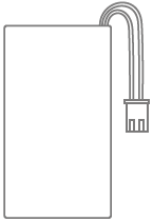
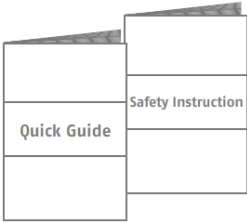
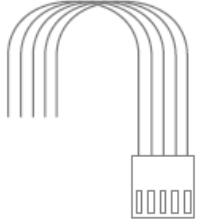
3.1. product features

The **FUAA85000 Comfion Pro wireless security system** is an EN Grade 2-certified burglar alarm system with home-automation functions. The system can be set up and operated via the intuitive app or the ABUS Cloud Portal.

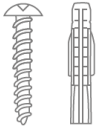
Key features:

- All-in-one security system: Alarm system, video NVR (up to 8 cameras) and access control in a single system – reduces the number of devices and installation effort.
- Native wAppLoxx Pro integration: Direct arming/disarming at the door – fewer false alarms, greater user acceptance among end customers.
- Perimeter alert with outdoor components: Early detection of intruders – increased response time and reduced risk of burglary.
- Integrated network video recorder: Centralised recording and management for up to 8 cameras – video images visible directly in the app in the event of an alarm and achievable without an additional NVR recorder.
- App control & smart home scenarios: Centralised operation of all components, scenarios flexibly configurable – ideal for individual customer requirements.
- Scalable and suitable for large-scale projects: Up to 160 wireless components and 40 sub-zones – with a long wireless range of up to 2,600 m in open space for efficient planning of everything from small properties to larger projects.
- Secure 868 MHz radio with AES 128-bit encryption: This ensures a high level of transmission security, whilst the bidirectional radio ensures that the radio signal has been received
- EN 50131 Grade 2: Suitable for insurance-related security requirements and professional projects.
- 4G mobile network backup: Secure alarm transmission even in the event of a power cut – increased system availability.
- Tamper protection: Wall breach contact & system monitoring – reliable operation in everyday use.
- Jamming monitoring: If a jammer is detected, Comfion Pro triggers an alarm
- Hire a security service: Integrated control centre log (SIA DC-09)
- All information always at your fingertips: notifications via SMS, email or push notification

3.2. Contents

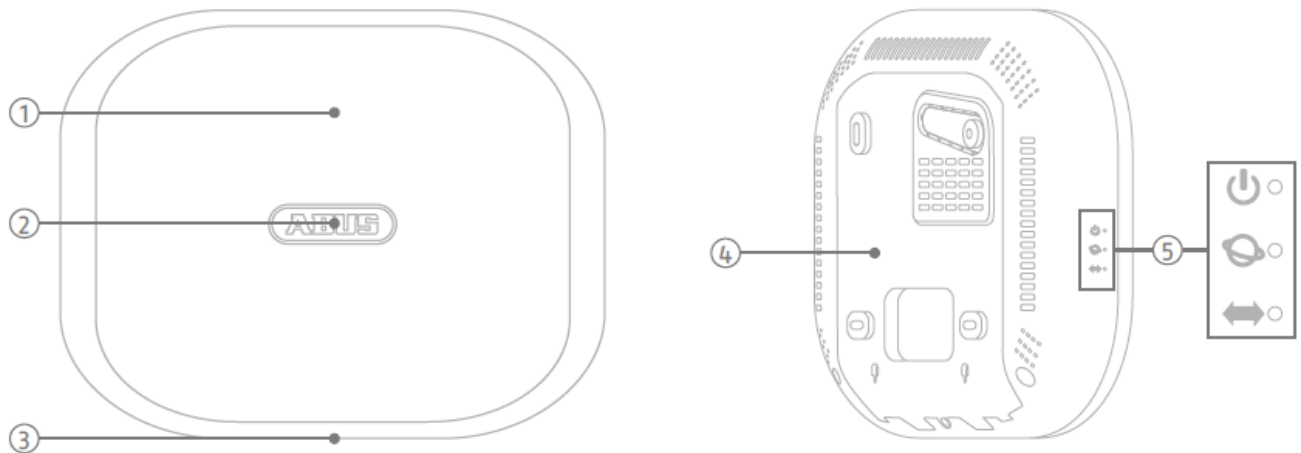
		
1 x Control panel	1 x wall mount	1 x battery
		
Quick Guide & Safety Instructions	2 x wired detector cables	4 x screws for SSD hard drive
		
1 x opening tool		

Required:


4 x screws / wall plugs Ø 7.0 mm

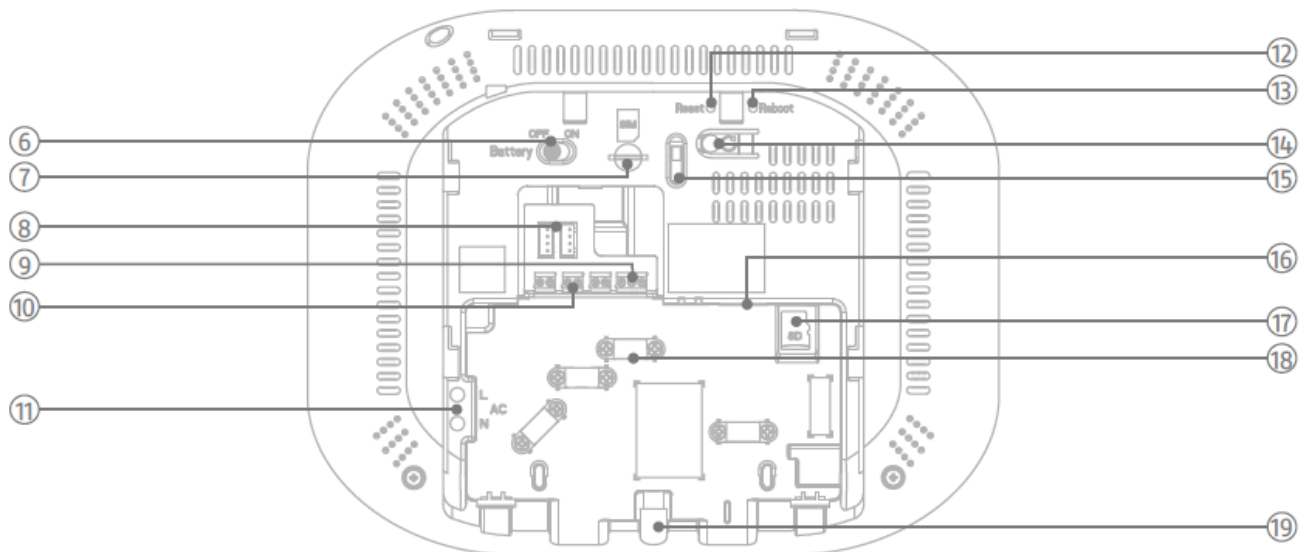
3.3. Device description

Product structure (front/back)



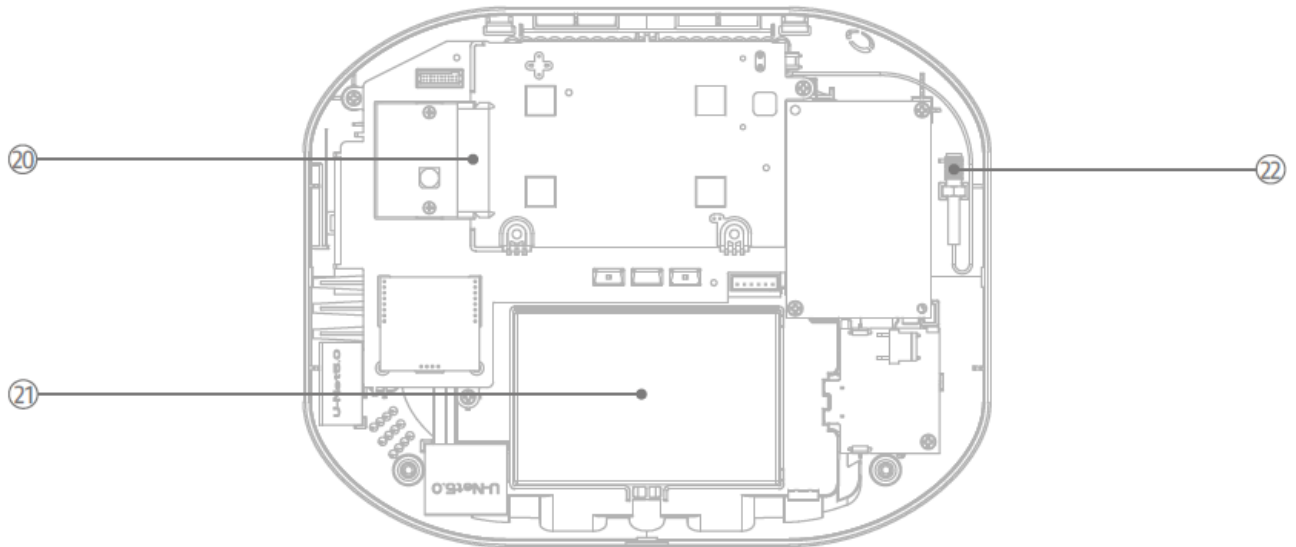
1 Cover	2 Logo (alarm status)	3 Opening mechanism
4 Back panel	5 Status LEDs: Power, Internet, Network	

Rear (open)



6 Battery switch	7 SIM card slot (Nano-SIM)	8 Wired sensor inputs
9 Relay output	10 BUS terminals	11 AC connection terminals (L/N)
12 Reset button	13 Restart button	14 Network reset
15 Tamper switch	16 RJ45 socket	17 MicroSD slot
18 Strain relief	19 Mounting screw	

Front panel (open)



20 SATA connector for SSD	21 Emergency power battery	22 External mobile phone antenna connection (SMA)
---------------------------	----------------------------	---

LED status indicators

		  	
		Logo (alarm status) Status LEDs	
Disarmed	White	Power LED (top)	
Armed	Blue	Mains voltage	Green
Partially armed	Blue	Battery operation	Red
Alarm	Red (flashing)	Firmware update	Yellow (flashing)
Sabotage control panel	Red (flashing)	Internet LED (centre)	
Programming process	Green (flashing)	Online & Admin registered	Green
Maintenance mode	Purple	Online & Admin not registered	Green (flashing)
Fault	Orange (flashing)	Offline	Red
		Network LED (bottom)	
		LAN	Green
		3G/4G mobile	Red

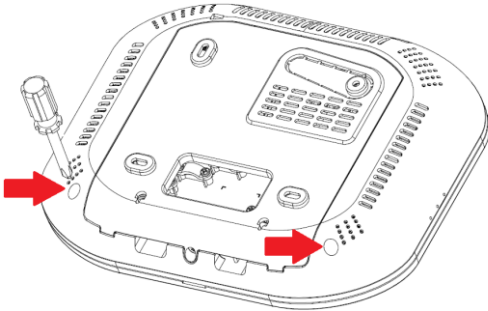
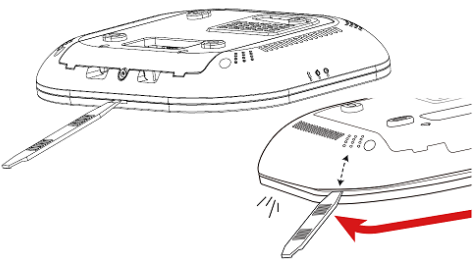
3.4. Technical specifications

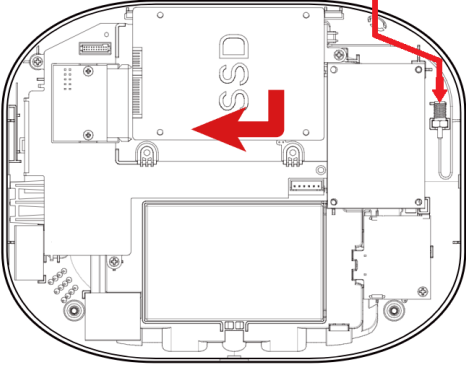
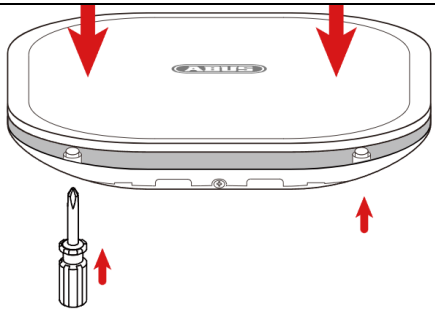
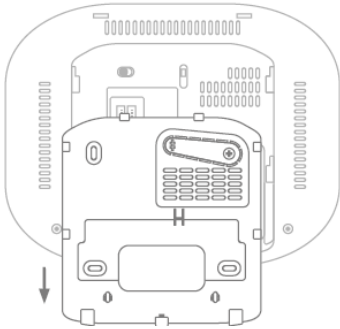
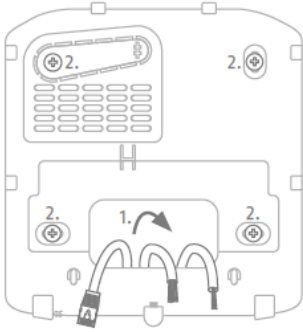
Dimensions (WxHxD)	242 x 190 x 45 mm
Weight	950g (with backup battery)
Operating temperature	-10 °C to +40 °C
Environmental class	II (EN 50131-1 + A3:2020)
Protection against environmental influences	IP40 / IK06
Humidity	max. 85% RH (relative humidity)
Connections	L/N socket (230 V), RJ45 (LAN), SATA 3.0 port (for 2.5" SSD), SIM card slot (Nano-SIM), Micro-SD card slot
Inputs/Outputs	4 contact group inputs (NC/NO), potential-free (wiring type: 2-wire CC, EOL, DEOL) 1 relay output (NC/COM/NO) max. 30V DC / 1.6A
BUS interface	(GND / +V / B / A) 13.0 V Cable length max. 200 m
Indicators	Status LED (Power, Internet, Communication) ABUS logo (system status)
Buttons	Restart button, Reset button, Network reset, Battery switch
Radio frequency / Modulation	868.0 – 868.6 MHz / GFSK
Power, radio / range	max. 25 mW (14 dBm) / 1000 m, open field
Number of radio components	160
Number of zones	40
Number of users	51
Number of events	> 10,000
Network recorder	Max. 8 channels @ 2048 kbps, when using 4 channels @ 4096 kbps Example: 4 channels at 4K (3840 x 2160) + 4 channels at 1080p (1920 x 1080)
Communication	Ethernet 1 GbE LAN SSL/TLS Mobile network (backup): 3G UMTS / 4G LTE SMS & voice: 2G GSM / 4G LTE
AÜA category	SP5 (LAN) SP2 (GSM) DP3 (LAN + GSM)
Power supply	Primary: AC 230V / 50Hz Secondary: LiPo battery 7.4V / 6,000mAh
Power supply type	Type A, power supply compliant with EN50131-1+A3:2020 and EN50131-6+A1:2021
Backup time – battery operation	> 12 hours in accordance with EN50131-1+A3:2020 Grade 2
Tamper protection (detection / protection)	Yes (1x wall tear-off contact)
Supervision time	900 – 3,600 s (default setting: 3,600 s)
Security grade	Grade 2 (EN 50131-1 + A3:2020)
Conformity	Security Grade 2 when properly installed, compliant with EN 50131-1+A3:2020, EN 50131-3:2009 and EN 50131-5-3:2017
EU Directives	RED: 2014/53/EU, RoHS: 2011/65/EU + 2015/863 General safety: 2001/95/EC

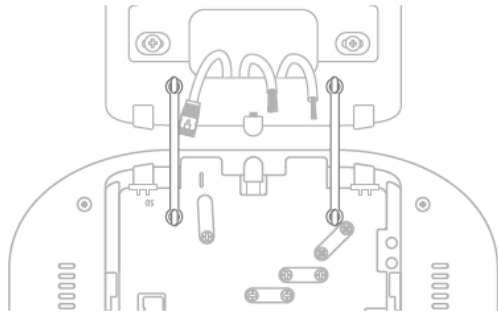
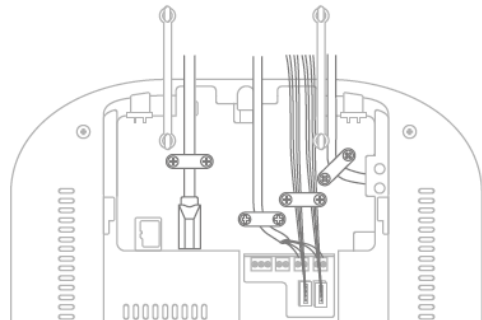
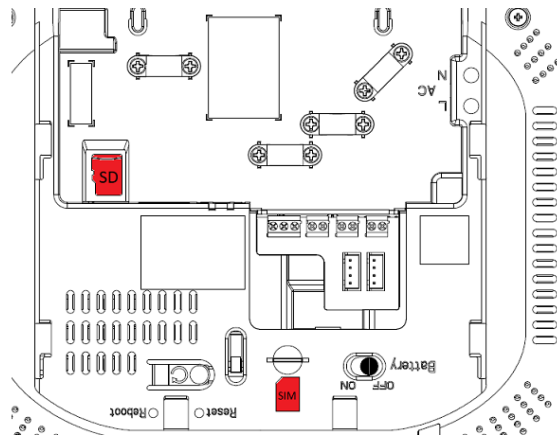
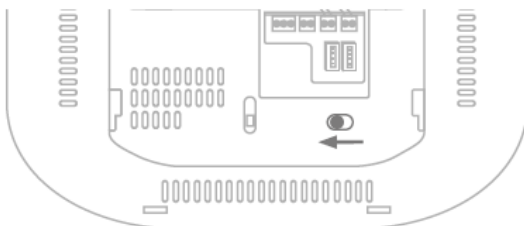
4. Installation & commissioning

4.1. Wall mounting of the control panel

 Caution	ATTENTION: BEFORE INSTALLING THIS SYSTEM, YOU MUST ENSURE THAT THE POWER SUPPLY TO THE ALARM CONTROL PANEL IS DISCONNECTED AND SWITCHED OFF. (Also ensure that the battery switch is set to "Off".) All electrical connections must be carried out by a qualified electrician and comply with applicable local regulations.
 Caution	CAUTION: If the device is connected to the mains whilst live, the mains voltage will also be present at the insulated terminals of the mains connection screw terminals. CAUTION: The mains cable to the alarm control panel must be fitted with a two-pole isolating device in accordance with EN 62368-1. Caution: When handling the circuit board in the alarm control panel, you must take the usual precautions to prevent damage caused by static electricity.
 Note	- Mount the control panel on the wall at a height of approx. 1.5 m - Maintain a distance of at least 1.5 m on all sides from the following devices: electrical appliances, metallic objects or devices emitting radio waves (e.g. routers, microwaves) – as these may impair the system's radio performance.

Fitting the hard drive / SSD data storage and external mobile phone antenna (not included)	
Open the cover of the control unit. To do this, loosen the 2 screws on the back.	
Lever the cover off using the tool provided.	

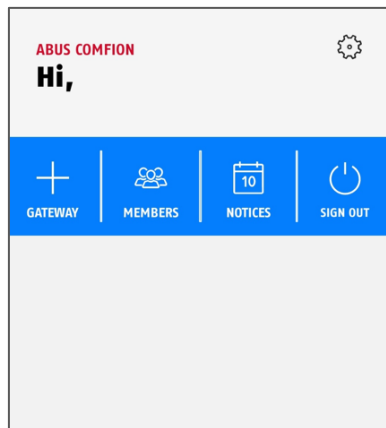
Hard drive / SSD storage: (not included) Connect the 2.5" SSD to the designated slot (SATA 3.0) and secure it using the screws provided. External mobile phone antenna: (not included) Feed the connection cable through the prepared opening and screw it onto the SMA socket. Recommended accessories from ABUS: TVAC41210 - 1 TB 2.5" SSD data storage SATA WD Red TVAC41220 - 2 TB 2.5" SSD storage drive SATA WD Red FUZU85000 - External mobile phone antenna for Comfion Pro Format the hard drive to exFAT or NTFS before insertion. Note The 2.5" hard drive slot allows the use of HDD hard drives and SSD data storage devices. The requirements of EN 50131 (emergency power duration) are met when using an SSD data storage device.	
Secure the cover until it clicks audibly into place and tighten the screws on the rear.	
Wall mounting & cabling	
Loosen the fixing screw (bottom centre) and pull the back plate away from the control unit housing.	
Caution: Ensure that the power supply (mains cable) is switched off and isolated! 1. Feed all necessary connection cables through the cable entry on the control unit's mounting plate. 2. Then secure the mounting plate to the wall.	

Hook the control unit's retaining clips (2 retaining cables) into the fittings on the back plate.										
Feed the connection cables into the control unit • Connect the mains cable to the L/N terminal. • Connect the Ethernet cable to the RJ45 socket • If necessary, connect the bus cable and the wired detectors etc. to the appropriate terminals. • Further details on connecting wired detectors and bus devices can be found in sections 3.2.5 and 3.2.6 Secure all connection cables with the strain reliefs.										
If required, insert a micro SD card (max. capacity 512 GB) and/or a SIM card (nano-SIM) into the designated card slots until they click audibly into place. (Cards not included)  Note Format your SD card to exFAT or NTFS before inserting it.										
Now switch on the power supply. The control unit will now perform the boot process.										
Set the battery switch to "ON" Once the boot process is complete, the status LEDs will light up as follows: <table><tr><td></td><td>Power LED:</td><td>Green (mains power)</td></tr><tr><td></td><td>Internet LED:</td><td>Green (flashing) (Online & Admin not registered)</td></tr><tr><td></td><td>Network LED:</td><td>Green (LAN)</td></tr></table>		Power LED:	Green (mains power)		Internet LED:	Green (flashing) (Online & Admin not registered)		Network LED:	Green (LAN)	
	Power LED:	Green (mains power)								
	Internet LED:	Green (flashing) (Online & Admin not registered)								
	Network LED:	Green (LAN)								

4.2. Commissioning of the system

4.2.1. Setup via the app & finalising hardware preparations

 Note	The initial setup of the Comfion Pro control centre, and thus the connection to the specialist partner portal and the associated installer, must be carried out via the app.
---	---

Download the Comfion app from your app store onto your smartphone or tablet (iOS or Android) Follow the instructions in the app until you reach the login page	
Log in using your ABUS Single Sign-On credentials (partner access) If you do not have access, create a free account under "Register".	Sign up'." data-bbox="594 404 836 605"/>
After logging in, you will see the control panel overview. Use the "+ Gateway" button to add a new control panel.	

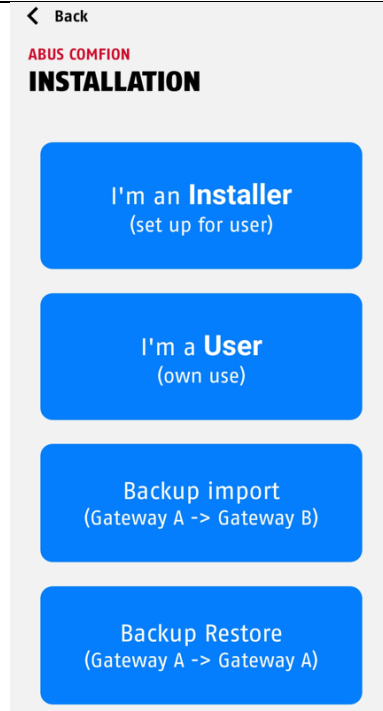
If you are commissioning the system for a customer, select **"I'm an installer"**. This will create your user in the role of installer.

If you are installing the system for yourself, select **"I am a user"**. This will setup your account in the Admin role with installer and admin rights.



As an installer, you can create users, but you lose this permission once you invite an admin user (owner). Further details can be found in **Chapter 4.1.** (User roles) and **Chapter 4.2** (Commissioning)

Further details on "Backup Import" and "Restore" can be found in **Chapter 6.1.7** (Backup)

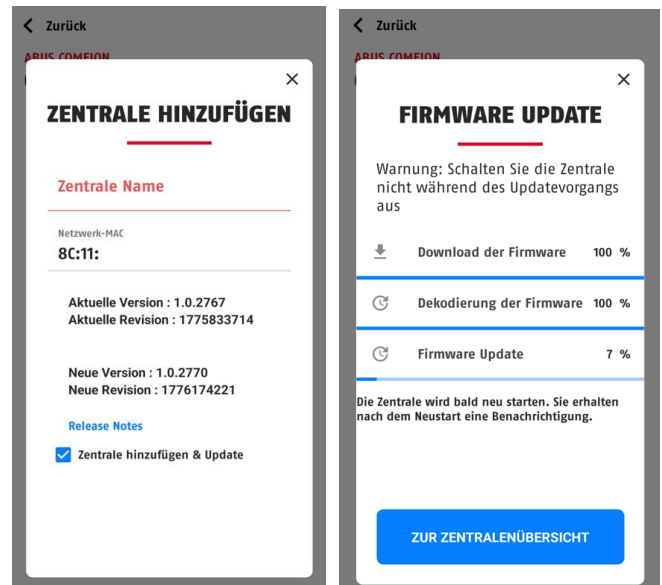


Ensure that the control unit is connected to the internet.

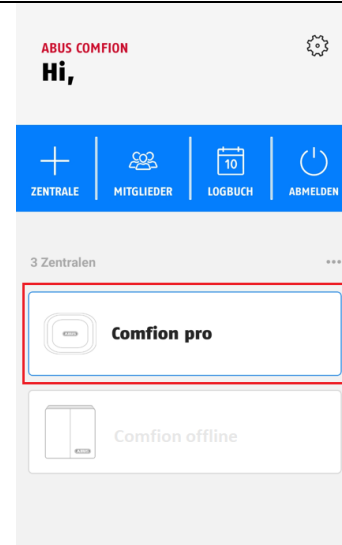
As soon as the 'Internet' status LED flashes green, you can start the pairing process in the app. To do this, scan the QR code labelled "Pairing Code"



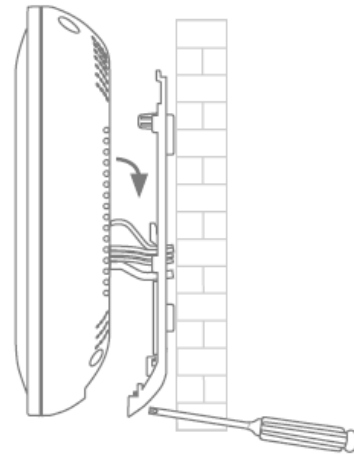
Enter a hub name and confirm it. The system will now start a firmware update before you can access it. The firmware update may take a few minutes and involves restarting the hub. During the update, the Power LED flashes yellow.



Once the control unit has restarted, it will no longer be greyed out in the control unit overview and can be accessed by clicking on it.



Release the retaining clip from the backplate and tuck the retaining cables inwards. Insert the control unit into the backplate, push it down and screw the control unit securely to the backplate.



After installation and commissioning, removing the control panel from the wall mount or opening the housing cover will trigger a tamper alarm. Only carry out necessary work on the hardware when maintenance mode is activated (*Control Panel Configuration -> Security Settings*)

4.2.2. Dashboard (after initial login)

Header bar:

- Configuration & User Settings
- Installateur User role (installers only)
- Firmware update (if available)
- Trigger panic alarm

Dashboard / Function Area

- Hotkey buttons (if configured)
- Camera preview images (if configured)
- Overview of sub-areas (indoor area; the outer shell is preset and can be expanded to include further areas – see: 3.2.3 Areas)
 - Clicking on '▼' displays assigned components and their status (if configured)

Navigation bar

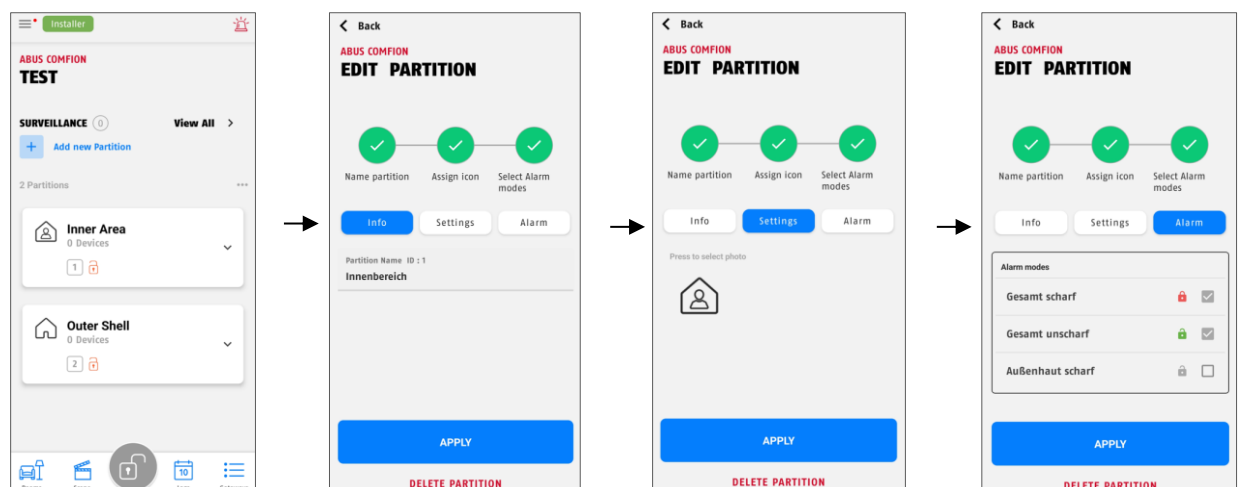
- Rooms (& component list) see 3.2.4 and 3.2.5
- Scenarios (scenes and automations) see 6.4
- Alarm modes (lock icon) – see 3.2.8
- Logbook (event list & filter function)
- Control centres (overview) – see 6.3

A fully configured dashboard view can be found in **Chapter 6.2 Dashboard**

4.2.3. Areas

Zones allow you to divide the property you wish to monitor and thus arm and disarm specific areas individually. In conjunction with the alarm modes, you can arm or disarm zones together or separately.

By default, the system has two zones – the perimeter and the interior. You can edit these zones by pressing and holding on them.

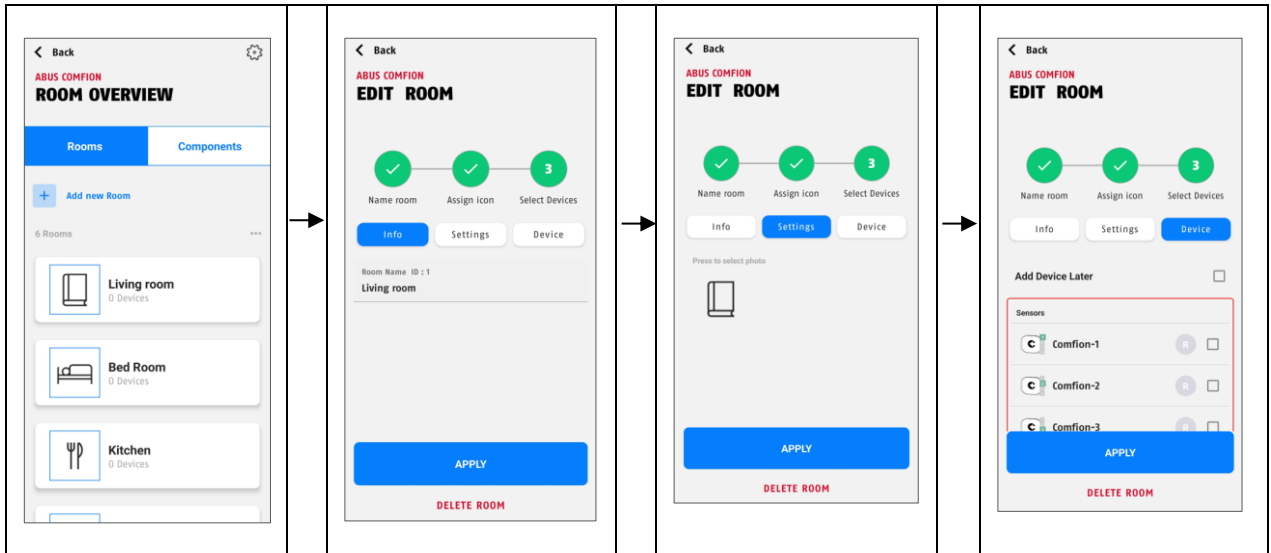


You can create further zones by clicking the “Add zone” button.

4.2.4. Rooms

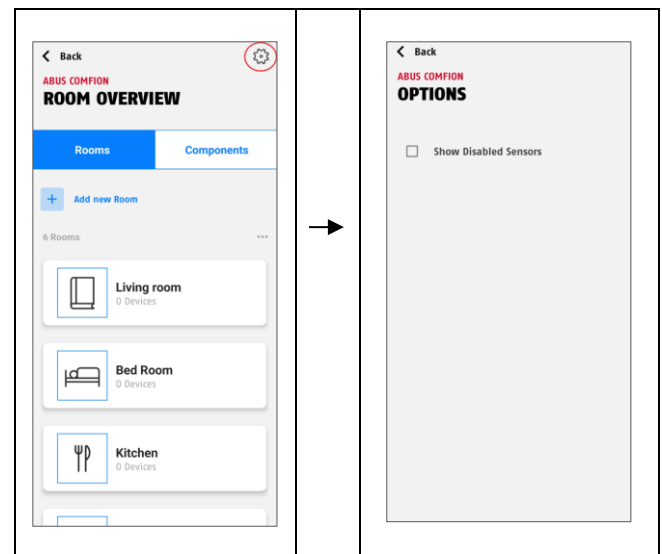
From the dashboard, you can access the 'Rooms' section via the navigation bar to configure rooms and components. The Comfion Pro wireless security system allows you to assign your components to rooms. This is intended to simplify the identification of components and has no functional purpose. Rooms are not assigned to zones, which means you can have components from different zones within a single room.

The system comes with a number of predefined rooms as standard. You can edit these rooms as you wish, or delete them entirely. You can edit this section by pressing and holding on it.



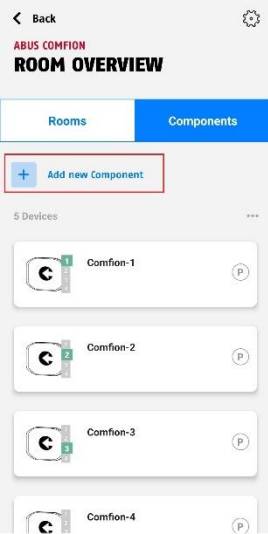
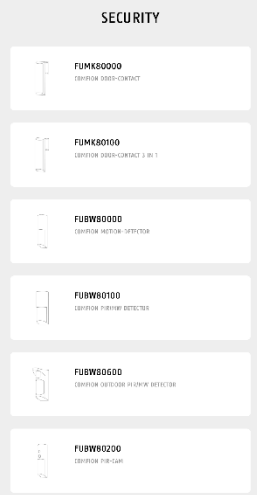
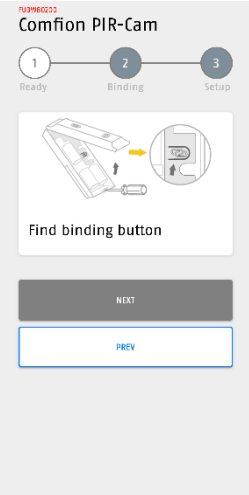
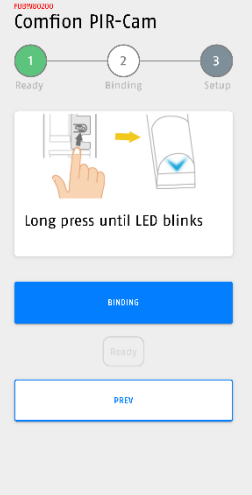
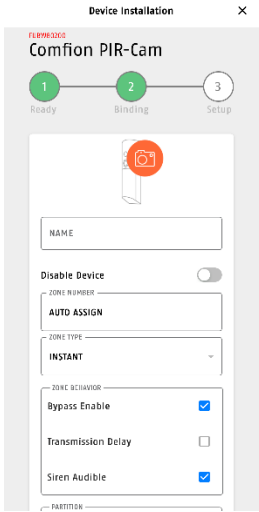
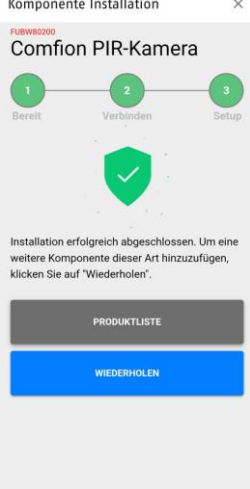
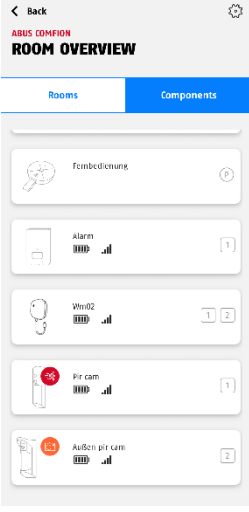
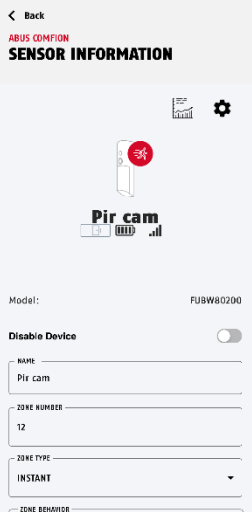
In the room overview, you can enable or disable the 'Show deactivated components' setting via the cog icon in the top-right corner of the screen. (Disabled is the default setting)

If this option is enabled, deactivated components are displayed in the dashboard under the rooms and in the component list.



4.2.5. Components

From the room overview, you can access the component view. By clicking on 'New component', you can add your Comfion components to the system.

 Select "New Component" →	 Select device from list →	 Follow the dialogue Click "Next" →	 Press the programming button & "Connect" →
 Device settings + "Save" →	 Programme any further devices if necessary →	 Component list →	 Detailed view & settings.

By clicking on a component that has already been programmed, you can edit it and adjust the following device settings:

Deactivate component	OFF: (default): Device functioning normally ON: Device is deactivated (no function)
Name	Assign a name to the component
Zone number	Assignment of zone number (done automatically by the system)
Zone type	- Input -> triggers an entry delay; once the delay has elapsed, a intrusion alarm is triggered - Output -> can be open during the exit delay; functions as an instant zone after arming - Input/Output -> uses an entry and exit delay - Entry followed -> The detector reacts like a instant zone, unless an entry

	<i>delay has been triggered beforehand. This can be restricted to the same area in the security settings.</i> • Instant (Intrusion) -> <i>triggers an intrusion alarm when the system is armed</i> • Perimeter warning -> <i>Zone type for outdoor detectors. Triggers the event, including a ' ' log entry and notification. No audible alarm.</i> • Immediate (Monitored) -> <i>functions like the Immediate Zone when the system is armed; when the system is disarmed, a notification is sent upon triggering</i> • 24-hour intrusion alarm -> <i>Intrusion alarm regardless of system status</i> • 24-hour water alarm -> <i>Water alarm regardless of system status</i> • 24-hour fire -> <i>Fire alarm regardless of system status</i> • 24-hour tamper -> <i>Tamper alarm regardless of system status</i> • Door/Window Monitoring -> <i>An open zone prevents the system from arming, but does not trigger an alarm</i>
Arming time/Disarming time	• For zone types Entry, Exit and Entry/Exit, a delay time can be set in seconds (5 to 180 seconds) • Default setting 10 s (entry delay) / 30 s (exit delay)
Zone behaviour	• Mute: <i>If the zone is triggered during arming, you have the option to mute it</i> • Transmission delay: <i>If this option is enabled, the transmission of zone alarm messages is delayed by the programmed time.</i> • Siren activation: <i>This detector controls the sirens integrated into the area</i>
Area	• A device can be assigned to one or more zones. -> This assignment, in conjunction with the zone type, triggers an alarm.
Room	• A device can be assigned to a room. • 'Assign later' means that the device has not been assigned to a room.
Start walk test (motion detector)	• Clicking on "Start walk test" initiates a 1-minute time window during which the device is to be triggered. • The walk test can be cancelled by clicking "Stop". • When triggered, the time window (detector's mute period) restarts. • For multi-sensor devices (e.g. PIR + microwave), sensors can be tested individually or together.
Start signal strength test (Wireless components)	 Note Test the signal strength before installing the component and, if in doubt, use a repeater. You will find an overview of how to assess signal strength in section 6.11 • Click on "Start signal strength test" and trigger the device. • For multi-sensor units (e.g. PIR + microwave), each sensor can be tested individually.
Camera functions (cameras only)	• MotionAlarm Off/On (default Off); "On" triggers an alarm provided the camera has been assigned to an area.
Save	• Click "Save" to apply the changes to your settings.

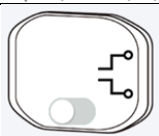
 Note	If a detector is programmed to the zone type Output or Input/Output, the system checks the detector status only after the delay time has elapsed when arming. - If the detector is not ready after the time has elapsed and "Muteable" is enabled, the detector is automatically muted after the delay time and the system is armed. - If the detector is not ready after the time has elapsed and "Muteable" is deactivated, the system is not armed.
--	--

 Note	A detailed overview of the symbols in the component list can be found in Chapter 6.7 (Symbol Explanation)
--	---

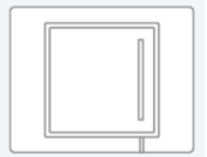
4.2.6. Component settings

In the component settings & to the right above the device icon, you can access detailed settings for the component by clicking on the cogwheel . For further details, please refer to the installation instructions for the respective component. Below you will find the settings for the Comfion Pro Control Unit FUA85000, the Comfion Pro BUS-WLX Module BUM080000, and IP cameras

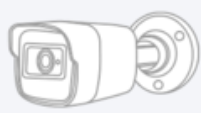
Comfion Pro Control Unit FUA85000

Icon	Description	Setting option	Explanation
 (per input, i.e. 1, 2, 3, 4)	Connection type	2-wire CC / EOL / DEOL (default setting CC)	Wiring type of the detector group inputs
	NC or NO	Normally Open / Normally Closed (Default setting: NO)	Relay default state, i.e. open or closed
	Logo display	Always Off / Always On / Illuminated (Default: On)	Sets the logo status lighting to permanently off, permanently on, or on for 10 seconds when the status changes (illuminates)
	Armed colour Disarmed Colour Partial armed colour	Colour matrix	Adjust the light colour by clicking on the colour icon

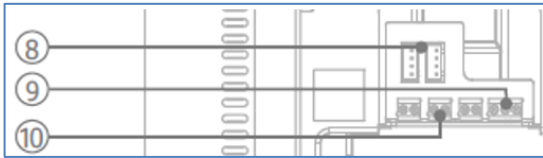
Comfion Pro WLX Pro Module BUM080000 and WLX Pro access media

Symbol	Description	Setting option	Explanation
 (BUS-WLX module)	Reset to factory default	Execute	Reset the WLX-Pro wireless module. Note: all lock cylinders and wall readers must then be reprogrammed! (The BUS-WLX module remains programmed!)
 Lock cylinders (Access / Intrusion)	Supervision time	4 – 720 min (default setting: 720)	Regular monitoring of radio communication at the set interval.
	Observe inevitability (Access only)	Off / On (Default: On)	When set to "On", access is not granted when Comfion Pro is armed.
	Grant time	6 sec / 12 sec (Default setting 6 sec)	Defines the time period during which the cylinder is engaged to open the door closer
 Wall reader (Access / Intrusion)	Supervision time	4 – 720 min (Default: 720)	Regular checking of radio communication at the set interval.
	Observe inevitability (Access only)	Off / On (Default: On)	When set to "On", access is not granted when Comfion Pro is armed.
	Grant time	6 sec / 12 sec (Default setting 6 sec)	Defines the time period during which the cylinder is engaged to open the door closer

IP cameras

Symbol	Description	Setting option	Explanation
 (IP camera)	Camera function "Motion Alarm"	Off/On (Default: Off)	Use motion detection to trigger an alarm. Note: Further settings are required, including in the camera configuration. See Section 3.4.4

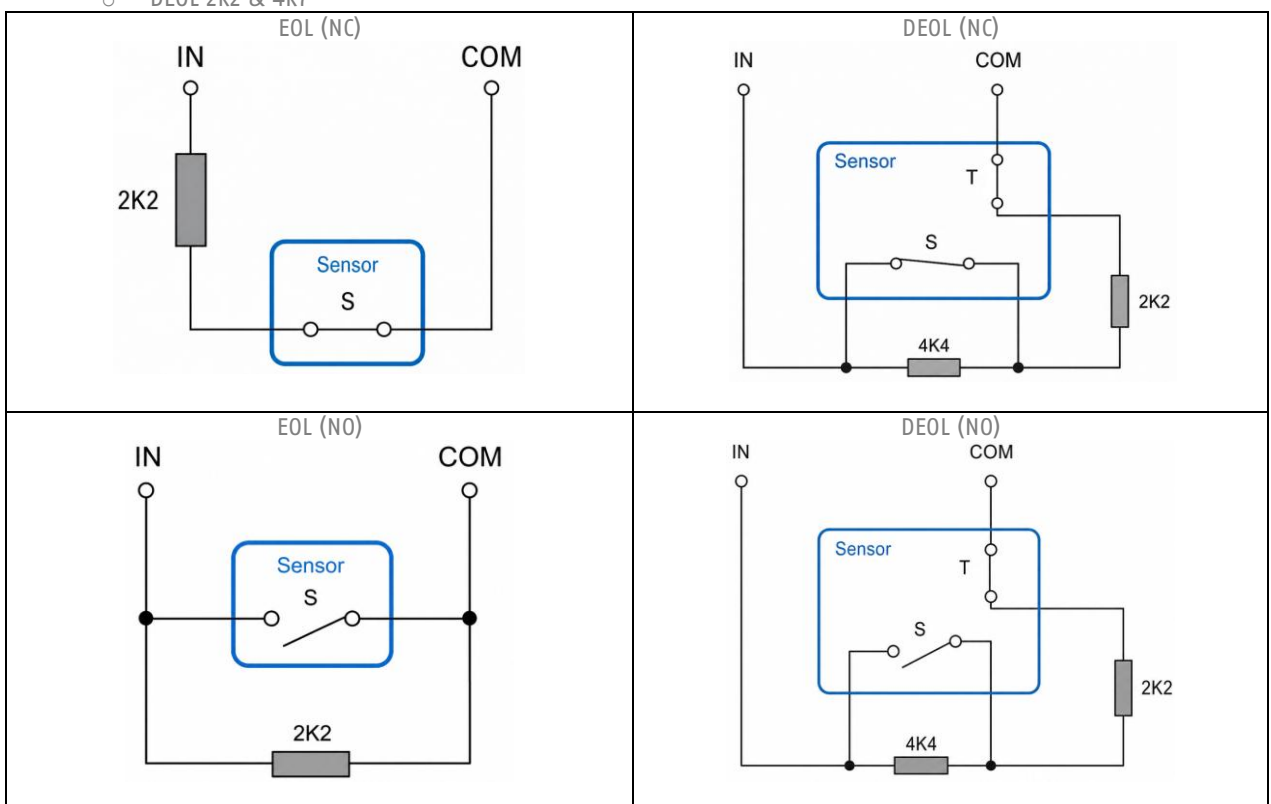
4.2.7. Wiring instructions (inputs/outputs/BUS)



The Comfion Pro control panel has several connection options for up to 4 wired detectors (8), a relay output (9) and an RS485 BUS interface (10).

Wired detector inputs

- Use the supplied 30 cm adapter cables with open cable ends. The cable pairs are colour-coded for each input.
- In the device settings of the Comfion app, set the wire mode (2-wire CC, EOL or DEOL) and the default position (NO or NC) for each input.
- The following resistance values are fixed for the monitored resistance wiring:
 - EOL: 2k2
 - DEOL 2k2 & 4k7



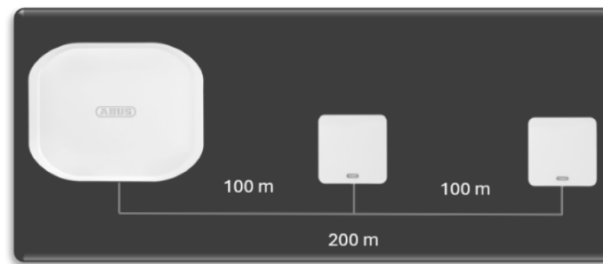
Relay output

- The relay output is voltage-free. Connect the output to earth and, as required, to the NC (normally closed) or NO (normally open) terminal. Max. 30V DC & max. 1.6A

RS485 BUS interface

- The Comfion Pro features a 4-wire RS485 BUS interface (GND / +V / B / A), 13.0V, for connecting up to 2 BUS devices (**Comfion Pro BUS-WLX module BUM080000**)
- You can connect devices to the Comfion Pro control unit either in series or in parallel.
- The maximum cable length is 200 m and can be divided flexibly when using two devices:

- Example:



- Cable recommendation: Twisted-pair cable (shielded and twisted), e.g. RS485/DMX cable or CAT5e or CAT6 cable.



Important

When installing the Comfion Pro control unit and the BUS-WLX module, as well as other electrical devices, antennas and metal objects, maintain a minimum distance of 1.5 metres to avoid interference in wireless communication (e.g. delays or signal loss)!

4.2.8. Alarm modes

The Comfion Pro wireless security system operates using so-called 'alarm modes', which form the core of the system. These are armable and disarmable links between zones and users.

In an alarm mode, you define which user arms or disarms which area. This allows you to map out all possible scenarios for arming and disarming.

In practice, when a user arms or disarms the system, they are actually executing an alarm mode.

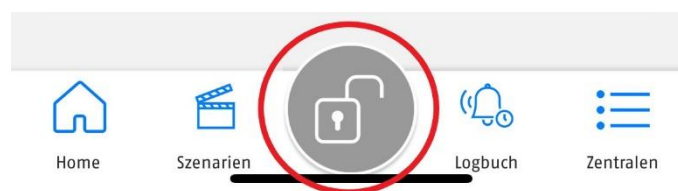


Note

The Comfion Pro wireless security system has three pre-configured alarm modes as standard: 'All Armed', 'Perimeter Armed' and 'All Disarmed'.

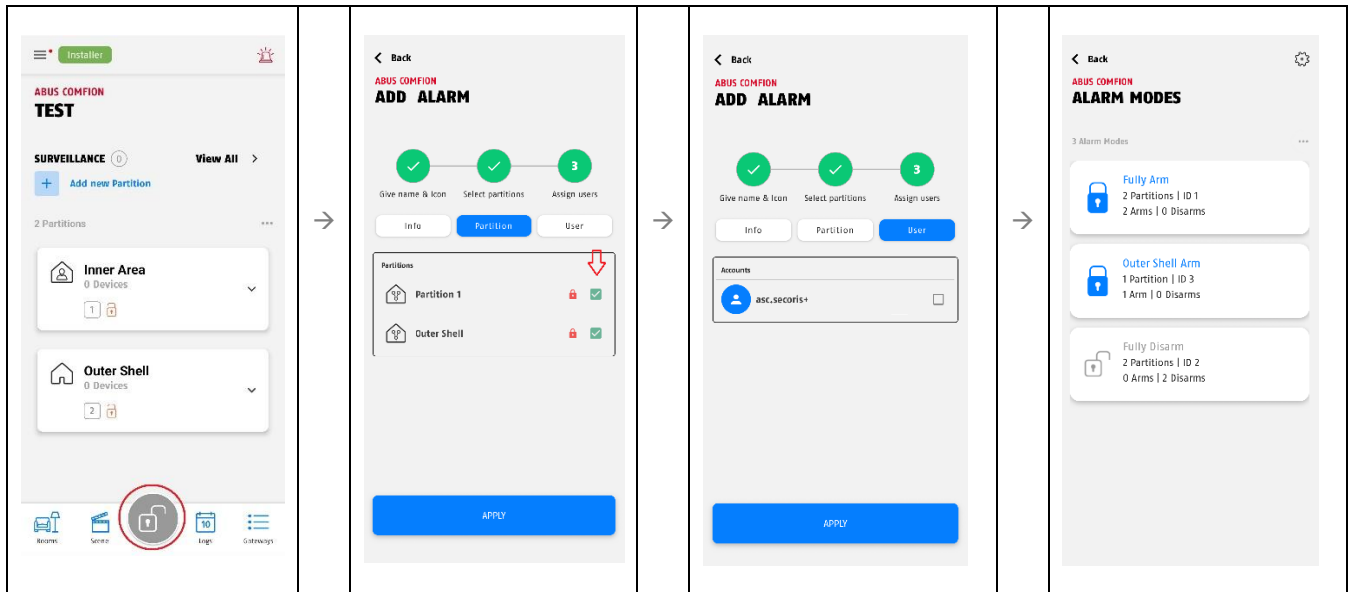
Executing an alarm mode

- The button at the bottom centre of the screen shows the system's current status (armed, disarmed, partially armed or maintenance mode)
- Pressing the button displays the available alarm modes and allows you to execute one of the switching commands shown there.



Creating or editing alarm modes

1. You can open the alarm mode management by clicking the status button on the dashboard and then clicking the settings icon (cogwheel) in the top right-hand corner of the screen.
2. Then click on 'Add alarm mode' or edit an existing alarm mode by long-pressing it.
3. Once you have named the alarm mode, select the zones AND the type of operation (Armed or Disarmed). To change the type of operation, click on the icon.
4. In the next step, select the users who should be authorised to activate this alarm mode.
5. Once completed, the alarm mode will appear in your overview and can be used.



4.3. WLX Pro Installation & Programming

Carry out the installation and wiring of the **Comfion Pro BUS-WLX** module as described in the product manual and in **section 3.2.7**.

 Note	To set up and configure the Comfion Pro BUS-WLX module and other WLX Pro access media, you will need the system card and reset card supplied. Keep these cards in a safe place!
---	--

- Program the Comfion Pro BUS-WLX module into the system as a "New Component". Proceed as described in **section 3.2.5** and follow the programming instructions.
- Then programme the WLX Pro locking cylinder or WLX Pro wall reader.
- During the programming process (Step 2), you will be prompted to assign the WLX Pro locking cylinder or WLX Pro wall reader to a Comfion Pro BUS-WLX module. Select the module that is closest to the cylinder/wall reader.

 Note	After programming the first lock cylinder or wall reader, you will be prompted to programme the enclosed reset card. The programmed reset card is permanently stored in the Comfion system as a fallback medium and is required to reset a cylinder. Further details can be found in section 6.1.8 WLX Information and in section 3.2.6 Component Settings
---	---

 Important	The following devices can currently be programmed into the Comfion Pro: - WLX Pro cylinder (Access/Intrusion) Type: LA-A, LA-I - WLX Pro wall reader (Access/Intrusion) Type: WR-A-S-0, WR-I-S-0 The WLX Pro repeater and other access media are not currently supported.
--	--

- You can programme RFID tags (NFC tags) in the user settings, or this can be done directly by the owner (administrator) upon handover. Further details can be found in **section 4.4.1 Access Rights**.

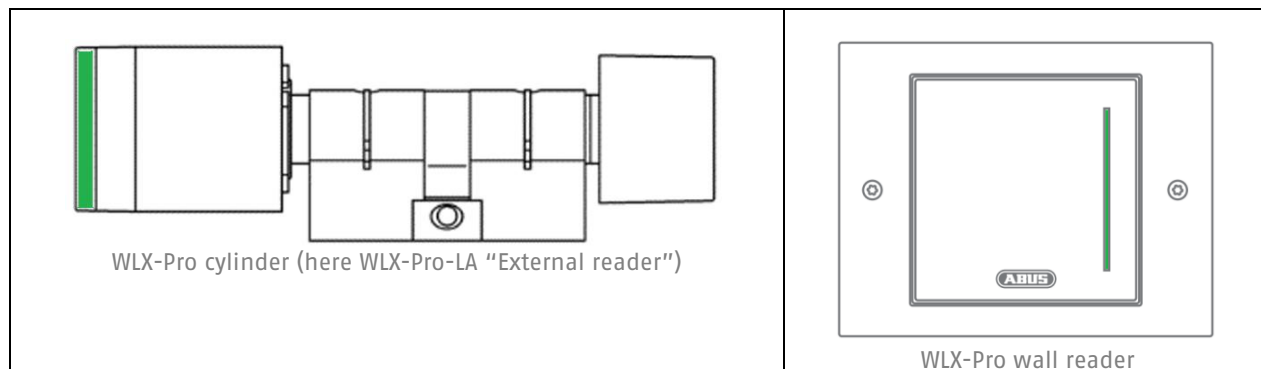
 Important	We recommend setting up at least one NFC tag as a fallback medium so that authorised persons can be granted access in an emergency (e.g. failure of the radio connection or prolonged power failure). Further details can be found in Chapter 4.4.1 Access Rights
--	---

4.3.1. Installation, configuration and use of WLX Pro cylinders and wall readers

Details on the installation of WLX Pro locking cylinders / WLX Pro wall readers can be found in the respective product installation guides. These are available online at abus.com in the download section of the product page:

- WLX-Pro locking cylinders: <https://abus.com/products/WLX-Pro-LA>
- WLX Pro wall-mounted readers: <https://www.abus.com/products/ACSE00026>

The WLX-Pro lock cylinder and the WLX-Pro wall reader indicate the following statuses via a sequence of LED flashes:



Signals	Description	
Commissioning & initialisation		
	1 x green, 1 x red, 1 x green, 1 x red	Initialisation after inserting the battery
	1 x green (long)	Cylinder is not programmed (& permanently paired)
	2 x red	Communication with external knob established
	2 x green	Communication with Comfion Pro BUS WLX module established.
Programming / Pairing / Reset (during the programming process (from FW 2.01), the cylinder flashes green cyclically)		
	2 x green	Programming successful
	3 x red	Unpairing successful
	1 x red	Programming failed
	10 x red	The system card was presented (programming/deprogramming mode); holding down the reset card whilst the lights are flashing resets the device.
In operation		
	1 x green	A short green flash indicates that the locking medium is being read and transmitted 1x green.
	1 x red	No radio connection to the Comfion Pro BUS-WLX module
	1 x red (long)	The Comfion Pro has been armed (acknowledgement)
	1 x green (long)	The Comfion Pro has been disarmed (acknowledgement)
	1 x red, 2 x green	Radio failure / authorised fallback (repeat process 3 times in total)
	2 x green	Access granted
	3 x red	Access denied, no authorised access
	3 x red, 2 x green	Battery warning (up to FW 2.07)

	5 x red, 2 x green	Battery warning (from FW 2.09) Cylinder engages with a delay of approx. one second
	1 x red, 2 x green	Battery warning level 2: no signal on the user transponder; fallback can still grant access 3 times→ Use fallback medium as for radio failure
	4 x red	Radio failure & unauthorised fallback transponder presented
	6 x red	- Arming not possible, or - Disarming not possible

4.3.2. WLX Pro functions – remote opening and office mode

Remote opening

Using remote unlocking (also known as remote release), the WLX Pro locking cylinder can be unlocked for a specified period (maximum 180 seconds). Configuration is carried out in the Comfion app (or web interface) as a scene or automation.

- The scene configuration adds a hotkey button to the Comfion app dashboard
- Further details on configuration can be found in **Chapter 6.4 Automations & Scenes**
- After remote opening has been executed, the external knob on the WLX-Pro lock cylinder must be turned to open the door.

 Note	Please note the following distinction: - The duration of the remote release is the period during which the cylinder can be engaged - After turning the external knob, the cylinder is paired in accordance with the defined opening time (6 or 12 seconds).
---	---

 Important	Remote opening is only possible when the Comfion Pro is disarmed.
--	---

Office mode (permanent access)

A cylinder with Office Mode enabled allows the door to be opened without an NFC tag by turning the cylinder knob. Configuration is carried out in the Comfion app (or web interface) as a scene or automation.

- The scene configuration adds a hotkey button to the Comfion app dashboard (you need two scenes to switch Office Mode on and off)
- The automation configuration allows you to switch Office Mode on or off, for example via a schedule: if time x→ then switch on ... if time Y→ then switch off
- Further details on the configuration can be found in **Chapter 6.4 Automations & Scenes**
- When Office Mode is active, the external knob on the WLX-Pro locking cylinder must be turned to open the door.

 Important	Opening via Office Mode is only possible when the Comfion Pro is disarmed. An activated Office Mode is interrupted for the duration of arming!
	Only programme this function if the operator is aware of the implications and has confirmed them in writing.

4.4. Cameras (NVR)

Using the ONVIF integration protocol, various cameras from the ABUS Professional Line can be integrated into the Comfion Pro wireless security system. Alternatively, integration via RTSP is possible. You can integrate up to 8 cameras into the Comfion Pro and have them record on event, when the system is armed, or continuously (24/7) (to a micro SD card or SSD).



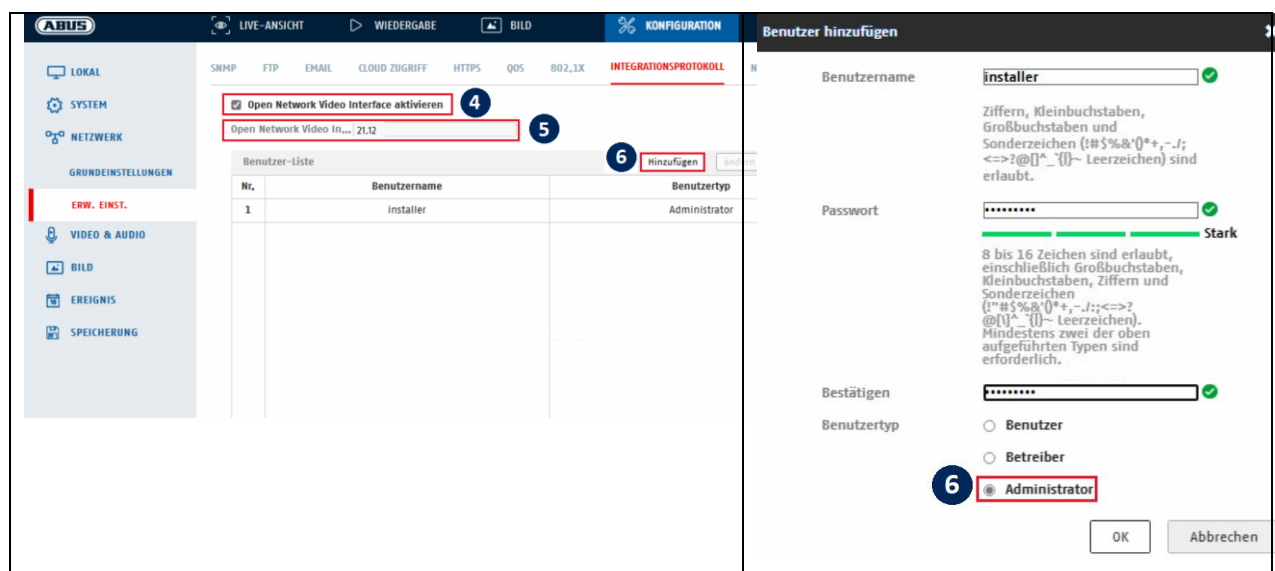
An SSD data storage device is required in the control panel for continuous recording (24/7).

4.4.1. Integrating cameras via ONVIF

In its factory settings, the Comfion Pro system automatically searches for ONVIF cameras on the network and adds them to the system. You can disable the automatic camera search in the camera settings under the camera overview.

Proceed as follows when integrating the cameras:

1. Connect the camera to the same network as the Comfion Pro.
2. Open the ABUS IP-Tool software and activate the camera.
3. Open the camera interface, log in as an installer and open the configuration.
4. Enable ONVIF in the camera's advanced network settings under the 'Integration Protocol' tab (Open Network Video Interface)
5. Here you can also see the camera's ONVIF version; Comfion Pro requires version 21.12 or higher.
(If necessary, please update the camera's firmware – this is available on abus.com in the download section of the product page)
6. In addition, a new ONVIF user must be added here. Please select the user type 'Administrator' here.
7. Configure the video settings in the camera as described in the note box below
8. Enter the ONVIF user details in Comfion Pro. (To connect to the camera in the Comfion Pro app and web interface, select the user created under (6).
9. Test the camera functions (live view, etc.)



The screenshot shows the ABUS configuration interface. On the left, a sidebar contains navigation options: LOKAL, SYSTEM, NETZWERK, GRUNDEINSTELLUNGEN, ERW. EINST., VIDEO & AUDIO, BILD, EREIGNIS, and SPEICHERUNG. The main area is titled 'KONFIGURATION' and has a sub-tab 'INTEGRATIONSPROTOKOLL'. Under this tab, there are two checkboxes: 'Open Network Video Interface aktivieren' (checked) and 'Open Network Video Interface In...', both with version '21.12'. A table below shows the 'Benutzer-Liste' (User List) with columns 'Nr.', 'Benutzername', and 'Benutzertyp'. It contains one entry: '1', 'installer', 'Administrator'. To the right, a dialog box 'Benutzer hinzufügen' (Add User) is open. It has fields for 'Benutzername' (filled with 'installer'), 'Passwort' (filled with '*****'), and 'Bestätigen' (filled with '*****'). Below these are radio buttons for 'Benutzer', 'Betreiber', and 'Administrator' (selected). The dialog also includes 'OK' and 'Abbrechen' buttons.

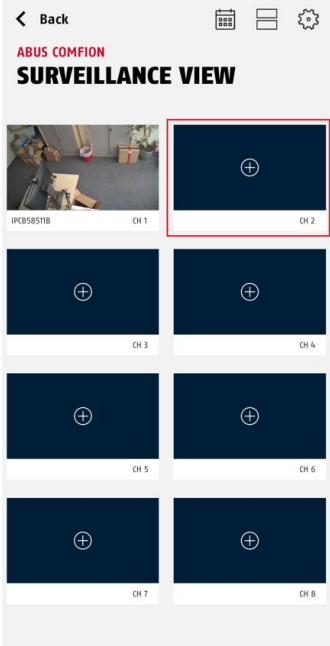
 Note	The following video stream settings are recommended depending on the number of connected cameras (channels) to ensure a smooth stream even when viewing and continuously recording 8 channels simultaneously. Primary stream: • 1 channel: Resolution 4K; Bitrate: 6Mbps • 8 channels: ➤ 4 x resolution: 4K (3840 x 2160); bitrate: 2048 kbps ➤ 4 x resolution: 1080p (1920 x 1080); bitrate: 2048 kbps Secondary stream: • 1–8 channels: Resolution: 360p; Bitrate: 512 kbps
 Note	• The maximum resolution of 4K (3840 x 2160) per channel must not be exceeded • The maximum bitrate must not exceed 8 x 2048 kbps

4.4.2. Integrating cameras via RTSP

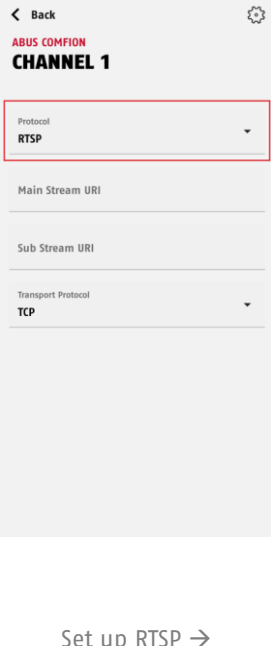
 Note	Integration via RTSP provides the camera's video and audio stream but does not allow for further configuration, PTZ control or motion detection.
---	---

To integrate cameras via RTSP stream, carry out the following steps:

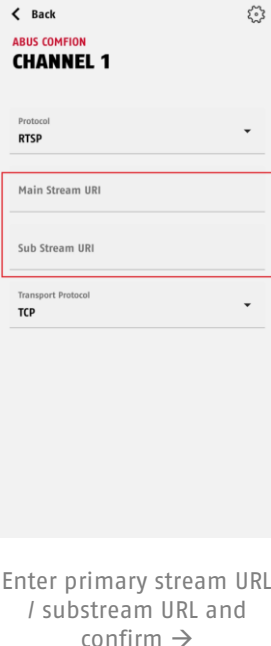
1. Connect the camera to the same network as the Comfion Pro.
2. Open the ABUS IP-Tool software and activate the camera. If necessary, create an installer account for the camera.
3. In the Comfion app, go to '→' > 'Camera overview' and select an (unused) camera channel (+)
4. In the configuration, select RTSP under "Network Protocol".
5. Enter the primary stream and sub-stream URLs. Compatible ABUS cameras use the following URLs:
 - **Note:** Replace "Username" and "Password" with the login details from step 2
 - Primary stream: rtsp://Benutzername:Passwort@192.168.0.27/ISAPI/Streaming/channels/101
 - Secondary stream: rtsp://Benutzername:Passwort@192.168.0.27/ISAPI/Streaming/channels/102



(+) Select channel →



Set up RTSP →



Enter primary stream URL / substream URL and confirm →

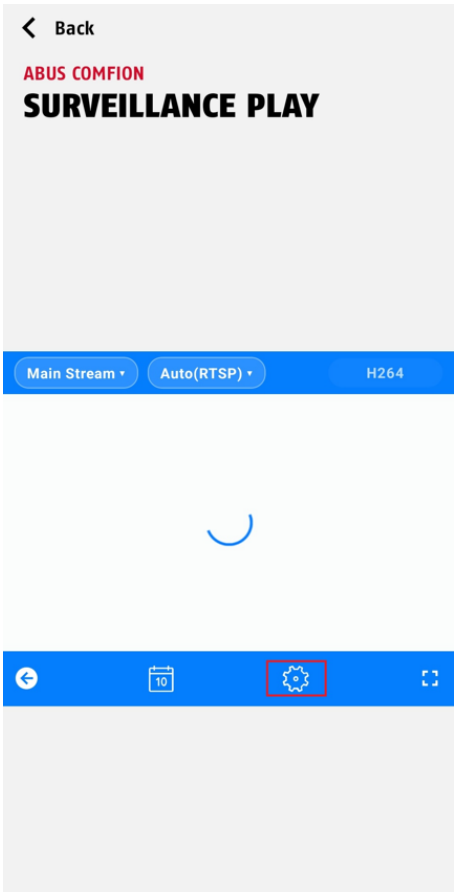
4.4.3. Camera settings (global)

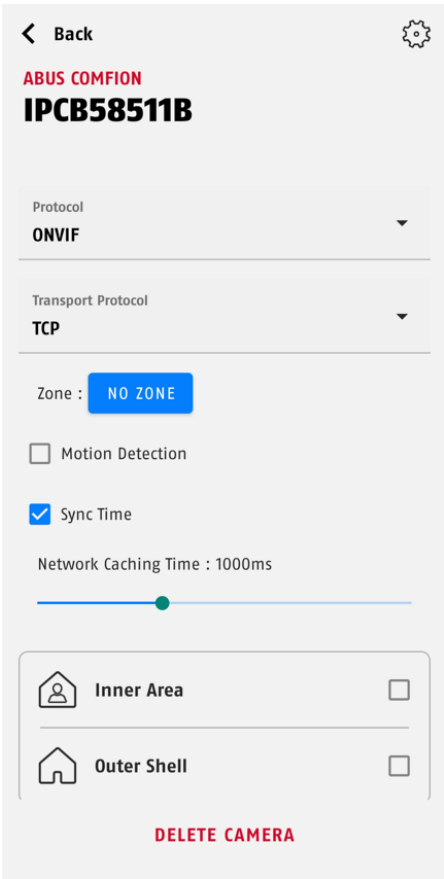
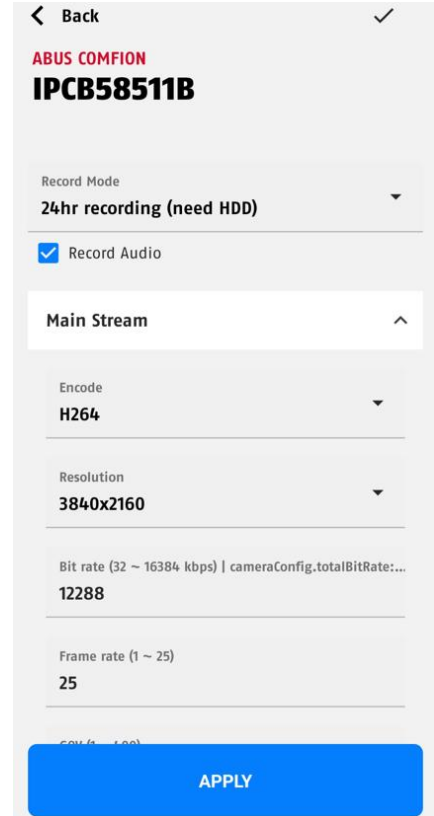
From the camera overview, click on the cog icon  to access the camera settings. These settings apply **equally** to **all connected cameras**.

Automatic camera search	OFF (default) / ON (none) Automatic search for ONVIF cameras on the same network
Data storage	OFF / ON & 1 – 365 days Recordings are deleted from the storage medium after the specified time has elapsed, provided that "ON" has been selected.
Recording stream type	Primary stream (default) / Secondary stream The stream type used for recording.

In the camera details view (live video stream), you will find another gear icon  for further configurations **of this camera**. Further details can be found in **Chapter 3.4.4**.

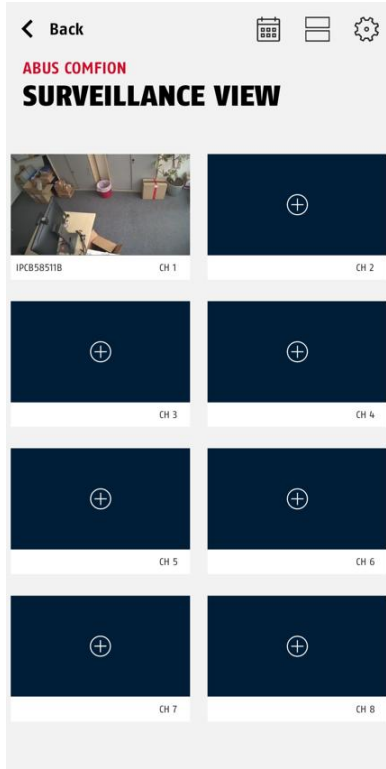
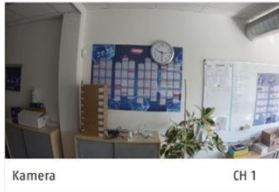
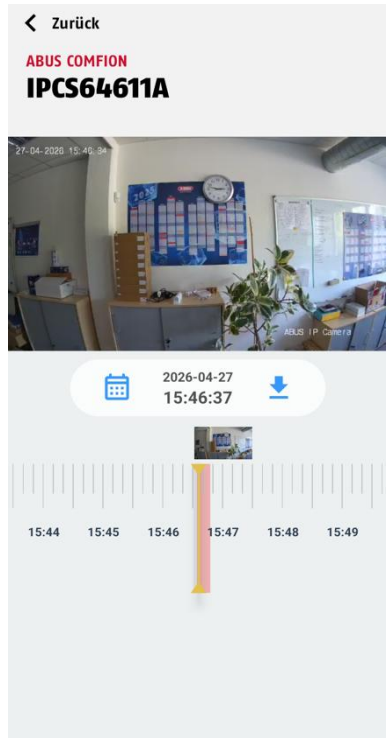
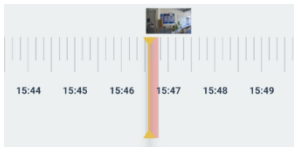
4.4.4. Camera settings (individual)

	From the camera overview, you can access the live video stream by clicking on the camera tile  Back to the camera overview Pan/Tilt, Speaker, Microphone (if supported by camera)  For further control functions and details, please refer to the Comfion Pro User Manual.  Camera events – for further details, see Chapter 3.4.5 NVR Operation  Settings for this camera  Switches the viewing angle between Portrait and Landscape mode
---	---

	Camera name, IP address, port, username, password, network protocol, transmission protocol • See 3.4.1 and 3.4.2 Integrating cameras Zone • If the camera has been added to a sub-area (here: indoor area), the zone number is displayed here. Motion detection • If enabled, the camera's motion detection is evaluated by Comfion Pro and can be programmed as a trigger event in automations.  Wichtig To activate this function, you must enable it in the camera's direct configuration (web interface or ABUS IP Tool).  Note Sync.Time • If enabled, the camera adopts the time setting from the Comfion Pro control panel Network caching time • Buffer time of the Comfion Pro NVR for temporarily storing incoming video data before display. Delete Camera Removes the camera from the channel slot and from the components list.
	Click the cog icon in the camera settings (individual) to set the recording mode: Record mode • Continuous recording ◦ 24/7 Recording ◦ Requires a hard drive (e.g. SSD storage) • Recording only when the system is armed ◦ Recording when the system is armed (or a sub-area) ◦ Requires a hard drive (e.g. SSD storage) • Recording only upon event ◦ Depends on the camera's set zone type, e.g. intrusion or perimeter ◦ Requires a micro SD card or hard drive • No recording Record Audio • Recording including audio stream (if supported by the camera) Main Stream • Settings like Encode, Resolution... for Main-Stream Sub Stream • Settings like Encode, Resolution... for Sub-Stream

4.4.5. NVR operation

The camera overview takes you to the parallel view of all channels. Here you can view the live feed from all connected cameras. Using the calendar function, you can view the recordings stored in the system, sorted by date.

	 Camera events per camera channel (Continuous recording and/or events)   View of camera channels in grid or row format.  Camera settings (global) see 3.4.3  Kamera CH 1  CH 3
	First select the camera channel to access this view.  Searching for camera recordings in the calendar (days with events are marked with a dot) 10 11 12 12  Downloading camera events - Start time is set in the timeline - Recording duration adjustable from 10 sec. to 30 min  15:44 15:45 15:46 15:47 15:48 15:49 Selecting camera events on the timeline Event recording → Red Continuous recording (grey)

5. Users and permission groups

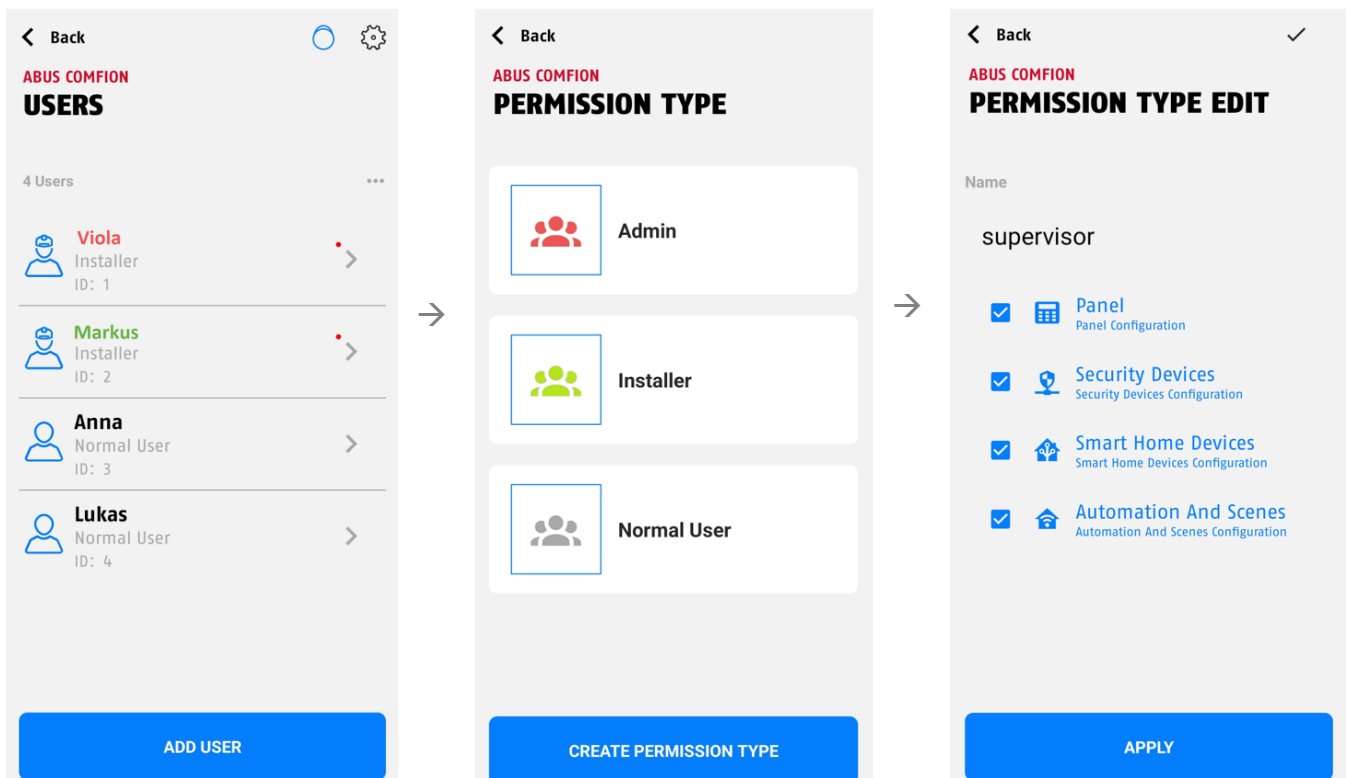
5.1. Explanation of the different roles

Installer	The installer has all user rights during initial commissioning. After handover of the system, the installer retains all configuration rights. The system owner can revoke the installer's rights to view the live camera feed and completely block their access to the system.
Admin	The system admin has full user rights for the system. Provided the installer grants the admin configuration rights, the admin can assume the rights of an installer and thus, for example, create and edit automations and scenes.
Custom Role (User-defined)	You can create your own non-admin user groups and set their permissions (see below)
Owner (Additional role)	The Owner role is automatically assigned to the first admin on the system. The Owner role cannot be assigned manually. In addition to admin rights, the system owner has the rights to add, invite and delete users. The system owner is marked in red in the user list.

The following settings are available under the Installer user:

- Grant access: Blocks/allows access to the system and push notifications
- Main installer: Specifies which installer account the system is connected to for remote maintenance (specialist installer portal)

Creating user groups:



5.2. Commissioning

In the control unit's factory settings, the authorisation groups "Installer" and "Admin" are currently available. When the system is commissioned by an installer, they are initially authorised to access all functions in the control unit.

5.2.1. Handover to the owner

Once you, as the installer, have completed the setup of the control panel, the system must be handed over to the end user. The first admin invited becomes **the owner** of the system. You can recognise this by the fact that this user is highlighted in red.

Once the owner has been invited, the installer loses the rights to edit and add users. Further users must be added by **the owner**.

5.3. Inviting/adding users

Once the system has been handed over, new users can only be invited by the owner. When adding a new user, the following options are available:

- Invite a new user
 - Invite a user using their email address.
- Select from my members
 - Invite a member. Members can be added to your personal member list in the Central Overview. (See **6.3.2 Members**)
- Create local user
 - Create a local user without an Abus Cloud account and without app usage. A remote control, a code for the control panel, and an NFC tag/card can be assigned to the local user. Additionally, a phone number and email address can be stored for notifications.

Furthermore, the permissions for the user to be added can be selected. Here, you can choose between Installer, Admin and user groups you have created yourself.

5.4. Editing users

User data is divided into 3 sections: access rights, notifications and permitted alarm modes during operation

5.4.1. Access rights

Permissions:

The permission group (Installer, Admin, Standard User) can be set for each user here

PIN code:

Enter the 4-digit PIN code for identification on the Comfion wireless control panel

 Note	Each 4-digit code can only be assigned once. If the same code is assigned to a second user, an error message will appear.
---	---

Allow access

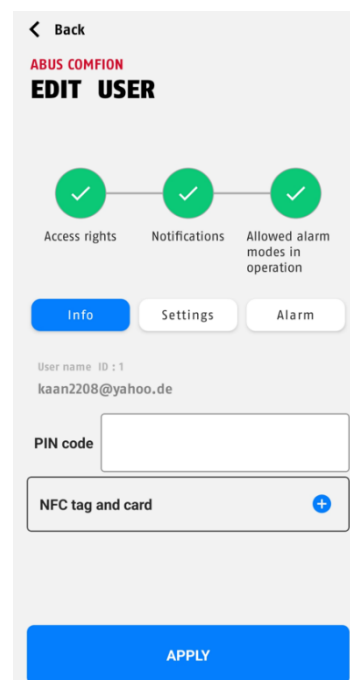
In conjunction with entering the email address and telephone number. Enables access for this user

Email & Phone (Local users only)

Entering the email address and telephone number to receive notifications via email, SMS

NFC tag and card

Up to 2 NFC tags/cards can be programmed and assigned per user. Pressing "+" starts the pairing process



Tapping on media that has already been programmed opens the settings with further configuration options:

- Off - (deactivates the tag if switched on)
- Forced arming - (Enables arming in the event of faults)
- Fallback medium - (if enabled, access is verified locally at the cylinder/wall reader in the event of disrupted radio communication between the cylinder/wall reader and the BUS-WLX module)
- Name - (Tag designation - the name also appears in the logbook for access events)
- User - (Assignment to a user set up in the Comfion Pro system)

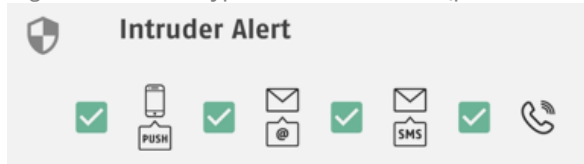
Changes must be confirmed by clicking "Save" or "Confirm"

5.4.2. Notifications

The Comfion Pro security system offers the following communication channels: Email, push notifications, SMS, phone calls & connection to a control centre

Under the menu item "Users  Edit User  Notifications", you can select individually for each user which notifications should be sent for each event.

e.g. for the event type "Intruder alarm" (push notification/email/SMS/phone call)

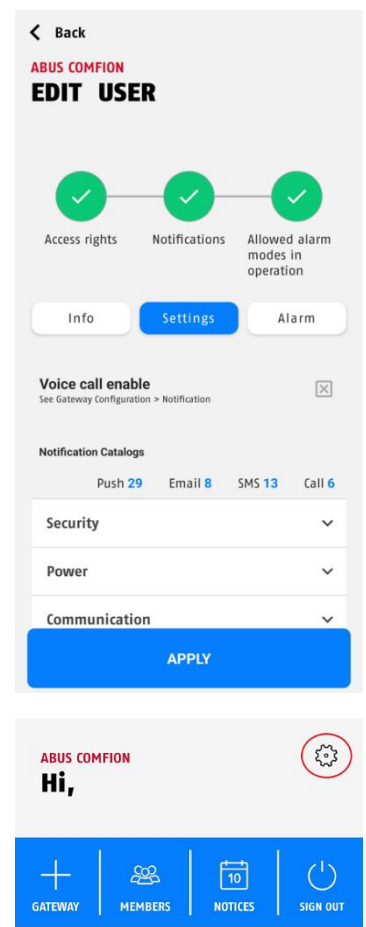


 Note	Some events are restricted to specific communication methods. For example, a phone call is not possible for some events. Push notifications are only available to Comfion App users, i.e. they cannot be used for local users.
---	---

The phone number for text messages and phone calls, as well as the email address for notifications, are stored in your user account. You can change these at any time. To do so, go to your main dashboard and click on the cog icon in the top-right corner. You can then enter your notification phone number and notification email address.

For local users, the email address and phone number are entered in the user settings (access rights).

 Note	Please always enter the telephone number with the country code, e.g. +49.....
---	--

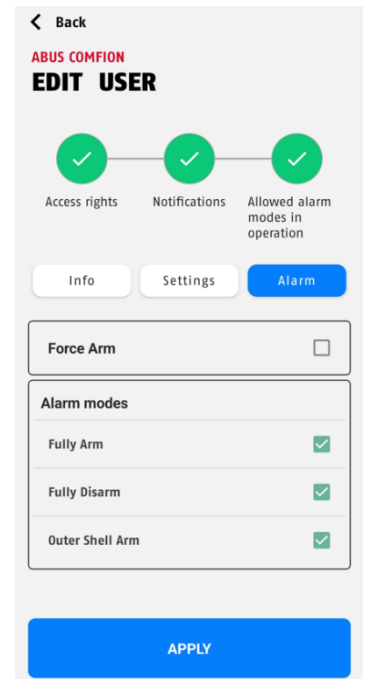


5.4.3. Permitted alarm modes in operation

Here you specify whether the user is permitted to force the system to arm (in this case, arming takes place even if a zone is open/triggered and without the bypass procedure); further details can be found in **section: 6.7.3**

You can also define the authorisation for arming and disarming each sub-area here. The user must have at least one authorisation.

All changes are applied by pressing "Confirm".



5.5. Deleting users

There are two ways to remove users from the control panel:

6. The system owner (user marked in red) can remove any other user from the system by clicking on them and then on the "Delete user" button.
7. Any user can delete themselves from the system by long-pressing the relevant control panel in the control panel overview and then confirming the deletion prompt.

 Note	The system owner can only remove themselves from the system using the second method (deleting the control centre from the control centre overview). Once the owner has been removed, the role reverts to the installer. The installer can designate a new admin as the new owner by inviting them.
---	---

6. Communication

6.1. Modem (Mobile module)

The Comfion Pro security system features an integrated mobile communication module (2G/3G/4G). This allows you to send text messages and make calls in the event of an alarm. It also provides a redundant channel for all system communication. This means that if your internet connection fails, all communication with the cloud – including remote access and push notifications – will be handled via the mobile module.

 Note	Set your SIM card to PIN-free before inserting it into the mobile module. You can usually disable the PIN in the settings of any mobile phone.
---	---

 Note	Do not use SIM cards from abroad for continuous use in the Comfion Pro.
---	--

A SIM card is required to operate the mobile network mode. You are free to choose your own SIM card (ABUS recommendation: Telekom, Vodafone, o2) and it must support the features you wish to use on the control panel. If you wish to use all functions, you will need a SIM card with SMS, a voice tariff and data allowance.

 Note	ABUS advises against using pay-as-you-go cards in the Comfion Pro security system due to concerns regarding reliability. Furthermore, the use of multi-SIMs is not advisable, as this can lead to connection problems.
 Note	Depending on the intended use, the SIM card should have the following features: • "SMS over IMS" – SMS transmission via the 4G network • "Voice over LTE" – call function via the 4G network

RSRP value (dbm)	Meaning	 Hinweis
< -80	Very good	RSRP is the strength of the useful signal (LTE reference signal) received by the device from the mobile phone mast. The installation location can affect signal strength, e.g. the distance from the mobile phone mast or attenuation caused by building structures. If in doubt, we recommend using an external antenna.
-80 to -90	Good	
-91 to -100	Average	
-101 to -110	Poor	
> -111	Very poor	

No further settings need to be made in the mobile communication module itself for sending SMS messages or making calls. If you wish to use the redundancy of the network services, it is necessary to enter the APN data for the SIM card being used. You will find the menu item under "Control Centre Configuration" → cogwheel → "Modem".

If no SIM card is inserted in the Comfion Pro, please deselect the "Activate" box. In this case, the SIM card will not be checked and no error message will be displayed.

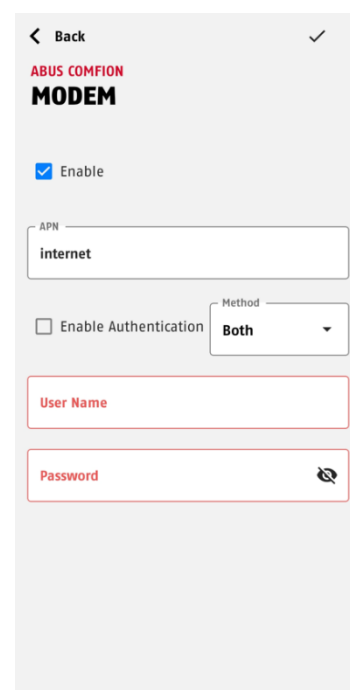
The APN details for your mobile network provider are included with your SIM card. Alternatively, you can look them up online. The details are not specific to the SIM card, but are the same for every provider. If a username and password are specified in the APN details, tick the "Authentication" box.

Example: Telekom:

- APN: internet.telekom
- Username: t-mobile
- Password: tm

Example: Vodafone

- APN: web.vodafone.de
- No username
- No password



6.2. Email

Email sending in Comfion Pro works without configuration and is carried out via the cloud.

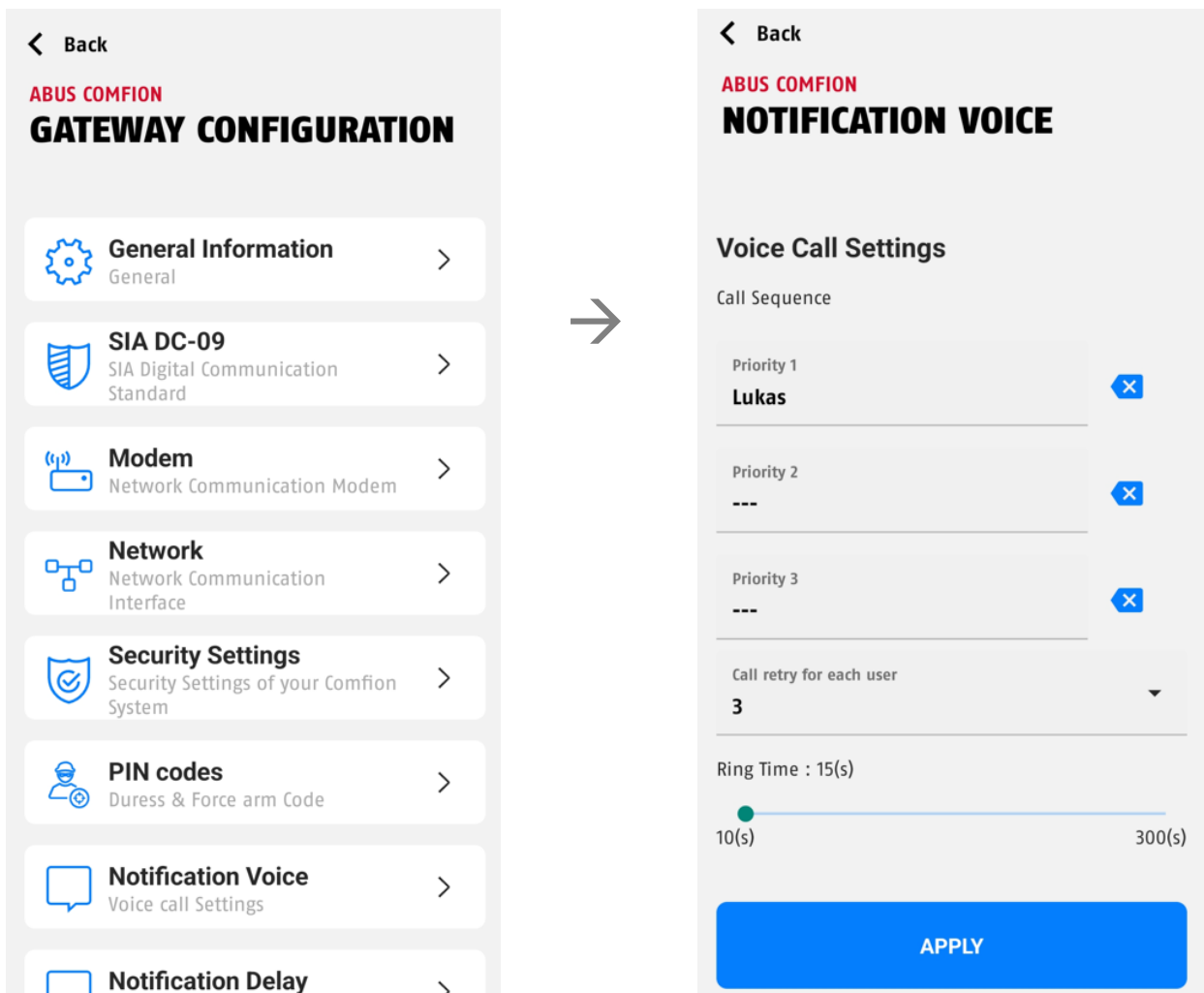
If the email address to be notified is different from your account email, you can set up a notification address in your account (see **4.4.2 Notifications**). If you do not set up a notification email, emails will be sent to your account address.

6.3. Telephone call

The Comfion Pro security system can call you in the event of an alarm. The system does not have a voice dialler, which means that no voice message is played during this call. The call serves solely to alert the user and is intended to inform the recipient of an alarm. The nature of the alarm can be determined from the push notification sent simultaneously.

A SIM card with call functionality must be inserted for the call function to work. Further information on the mobile communication module can be found in **section 5.1 Mobile Communication Module**.

- To receive calls, the recipient's telephone number must be stored in the user account (see **5. Communication**).
- Furthermore, you must set the call sequence under "Control Panel Configuration" → "Notification Voice". A maximum of 3 users can be called in succession.



Note

The number of call retries per user is set to 3 by default. This means that each caller is given three attempts. The call cannot be confirmed.

6.4. SMS

The Comfion Pro system can send SMS messages based on the event list (see **5. Communication**). Furthermore, you can use automations to have SMS messages with freely definable text sent to you for any events.

To enable SMS sending, simply insert a SIM card into the module and ensure the notification phone number is stored in the account (see **5. Communication**).

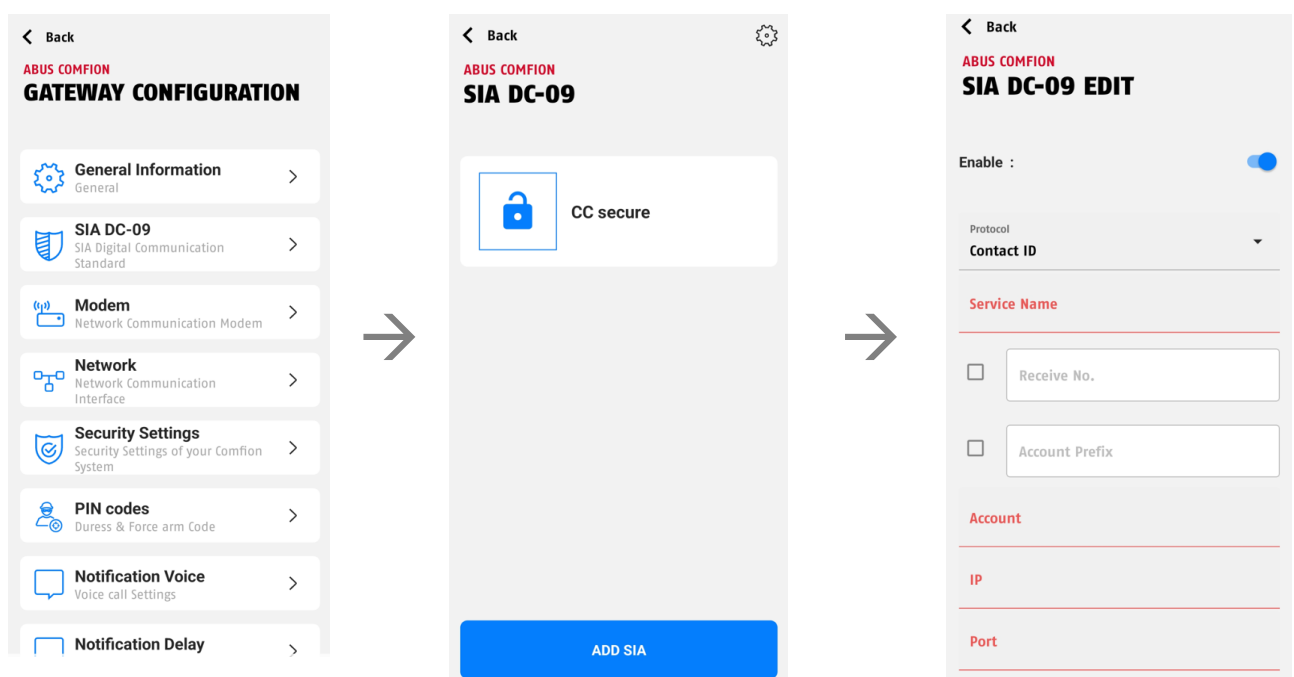
6.5. SIA DC-09 (Control Centre Connection)

The Comfion Pro wireless security system features a digital control centre dialler capable of sending the Contact-ID protocol via the SIA DC-09 standard. You can configure multiple connections simultaneously and thus communicate with different security services.

Enter the details provided by your service provider into the relevant fields. The two greyed-out fields, 'Recipient' and 'Customer ID Prefix', are not usually required and only need to be activated if explicitly requested by your service provider.

In the "Static Test Message" field, you can choose between the following options:

- **DC-09 Line Monitoring** -> Supervision integrated into the control centre log (must be supported by the control centre)
- **CID test message 602** -> Transmission of Contact ID code 602 at the set interval
 - **Note:** The set interval determines the time elapsed since the last event was sent to the control centre. If an event is transmitted to the control centre in the meantime, the interval restarts.



You can access the Advanced Settings via the cog icon in the top right-hand corner of the screen. Here you can enable the static test message and set the interval

 Note	A list of Contact-ID codes can be found in the appendix (Chapter 11.1)
---	--

7. General, Maintenance and Notes

7.1. Control panel configuration

Under the menu item 'Control Panel Configuration', you will find all the important information about your control panel and can also make important system settings

Once you have selected the Control Panel Configuration menu item, you will see the following information:

- Control panel name → (input field)
- Icon → (Can be replaced with your own photo)
- Network → (Display of network connection type)
- Mobile network status → (Drop-down)
 - Module type → (installed mobile chip)
 - SIM card → (indicates whether inserted)
 - IMEI → (unique 15-digit serial number of the mobile module)
 - Phone call → (Indicates whether possible with SIM inserted)
 - LTE connection → (Connection status indicator)
 - Signal strength (dBm) → (RSRP measured in dBm; for recommended signal strength, see **section 5.1**)
- Power supply → (Power supply or battery indicator)
- Firmware → (Click to display the version and release notes)
- Radio module → (Display of the radio module's firmware)
- Item number

Confirm

- Confirms the changes in this menu.
- The changes are then also updated in the ABUS Cloud.
-

Delete control panel

- Removes the control panel from the app and from the ABUS Cloud account!

You can open further settings menus via the cog icon in the top right-hand corner.

The settings for SIA DC-09, telephone calls and the mobile module can be found under 5. Communication.

7.1.1. General information

Under the heading "Storage", you will see information about the storage medium inserted (hard drive and/or SD card).

Under the heading "Date and Time", the time zone used and the NTP server are displayed.

You can restart the control panel using the "Restart" button.

7.1.2. Network

In this menu, you can view and, if necessary, adjust the network settings.

You have three options to choose from:

DHCP (default): The Dynamic Host Configuration Protocol is a client/server protocol through which the Comfion Pro automatically obtains its IP address and other relevant information from the router.

PPPoE: Point-to-Point Protocol over Ethernet is a network protocol that provides a direct connection within the internal network. This requires authentication via username and password.

Static: If you select "static", the Comfion Pro's network settings are assigned manually. Please discuss this with the network operator and do not assign an IP address from the DHCP pool.

 Note	Incorrect IP settings will prevent your system from connecting to the network, making it inaccessible to the app. In this case, press the "Network Reset" button (No. 14) on the back of the unit for 6 seconds and then release it. The control unit will then restart and reset its network settings to the default DHCP settings.
---	---

7.1.3. Security settings

Maintenance mode	On/Off (Default OFF)	Maintenance mode is used for system installation and maintenance. While maintenance mode is active, the system cannot trigger any alarms.
Zone lock	3x–20x (default 5x)	If a zone is triggered more often than the set number, that zone will not trigger again until the alarms have been cleared from the alarm history
Max. Keypad Repetition	3x–20x (default 5x)	Specifies after how many incorrect PIN entries the keypad will be locked
Control panel timeout	5–180 sec (default 30 sec)	Time setting for how long the control panel remains locked after X incorrect entries
Entry delay	5–45 sec (default 10 sec)	When the system is armed, the entry delay is displayed on the wireless control panel.
Exit delay	5–45 sec (default setting 30 sec)	Delay time displayed on the keypad before the control panel switches to the armed state.
Transmission delay	5–180 sec (Default: 60 seconds)	If this property is enabled in the zone, the transmission of a trigger is delayed by the set time.
Power failure delay	0–30 min (Default setting 0 min)	Adjustable delay for reporting a loss of power (12V DC)
Activate intrusion siren	On/Off (default ON)	Siren control in the event of a burglar alarm
Burglar alarm siren duration	5–180 sec (default setting 60 sec)	Duration of the audible signal from sirens integrated into the system
Activate tamper siren	On/Off (default ON)	Siren control in the event of a tamper alarm
Sabotage alarm siren duration	5–180 sec (default setting 60 sec)	Duration of the audible signal from sirens integrated into the system
Logo LED display: Tamper	On/Off (default ON)	Visually indicates the 'Tamper' alarm type via the illuminated ABUS logo. (Flashing red)
Activate panic siren	On/Off (Default setting: OFF)	Siren control in the event of a panic alarm
Panic alarm siren duration	5–180 sec (default setting 60 sec)	Duration of the audible signal from sirens integrated into the system
Logo LED display: Hold-up	On/Off (default ON)	Visually indicates the "Robbery" alarm type via the illuminated ABUS logo. (Flashing red)
Activate water siren	On/Off (Default setting: ON)	Siren activation in the event of a water alarm
Water alarm siren duration	5–180 sec (default setting 60 sec)	Duration of the audible signal via sirens integrated into the system
Logo LED display: Flood	On/Off (default ON)	Visually indicates the 'Flood' alarm type via the illuminated ABUS logo. (Flashing red)
Activate fire siren	On/Off (Default setting: ON)	Siren control in the event of a fire alarm
Fire alarm siren duration	5–180 sec (default setting 60 sec)	Duration of the audible signal from sirens integrated into the system
Logo LED display: Fire alarm	On/Off (default ON)	Visually indicates the 'Fire' alarm type via the illuminated ABUS logo. (Flashing red)
Activate panic APP siren	On/Off (Default setting: OFF)	Siren control in the event of a panic alarm triggered via the app
Assault APP Siren duration	5–180 sec (default 60 sec)	Duration of the audible signal from sirens integrated into the system
Display logo LED: Panic App	On/Off (default ON)	Visually indicates the "Overfall App" alarm type via the illuminated ABUS logo. (Flashing red)
Activate siren masking	On/Off (Default setting: ON)	Siren control when a detector is masked (cover monitoring)
Siren duration during masking	5–180 sec (default setting 30 sec)	Duration of the audible signal via sirens integrated into the system
Display logo LED: Muting	On/Off (default ON)	Visually indicates the "cover monitoring" alarm type via the illuminated ABUS logo. (Flashing red)
Hide Network error	On/Off (Default setting: OFF)	Deactivate arming prevention due to a network error

Hide battery error	On/Off (Default OFF)	Deactivate arming prevention for a battery fault
Hide power loss	On/Off (Default OFF)	Deactivate arming prevention for power loss (12V DC)
Enable automatic reset	ON/OFF (Default ON)	ON: The reset is performed when the system is disarmed. As soon as all triggered detectors are back to normal, the warning overview disappears from the dashboard when the system is disarmed. OFF: Alarms and errors must always be reset manually.
NFC open mode	ON/OFF (default OFF)	OFF: Only ABUS Mifare DESFire transponders can be used, as these are checked against the Comfion application for security reasons. Third-party transponders and Mifare Classic transponders cannot be used. ON: All Mifare Classic & Mifare DESFire transponders can be used (see the note box below for restrictions).
Allow factory reset	ON/OFF (Default setting: ON)	OFF: The control panel cannot be reset using the reset button ON: The control panel can be reset using the reset button.
Disable tamper detection	ON/OFF (Default OFF)	ON: Tamper detection for all programmed devices is disabled.
Input sequence in the same area	ON/OFF (default OFF)	OFF: Subsequent zones react to the input delay regardless of the area ON: Zones following the input only react to the input delay triggered in the same zone.



Note

Mifare DESFire transponders from third-party manufacturers only work if they have a fixed UID. No random ID mechanism must be activated on the transponders.

7.1.4. PIN codes

In this menu, you can change the panic code and forced arming code. These codes apply to all users of the system and are 3 digits long

The codes can only be used in conjunction with a Comfion wireless control panel



Note

The duress code and forced arming code are entered together with the user code, i.e.: User code (4 digits) → duress/forced arming code (3 digits), e.g. 1357999

Threat code

- Entering this code on the Comfion wireless keypad enables forced disarming
- The Comfion Pro is disarmed, but a signal is sent to the configured receivers.

Forced arming code

- See **Section 6.7.3**
- Enables the arming of one (or more sub-areas) with open zones, without a bypass procedure.

7.1.5. Notification delays

In this menu, you can set the delays for **network failure notifications**.

Server notification delay:

Delay time in the event of a cloud connection failure. Defines the delay, e.g. in the event of cloud issues, before a notification is sent. (Default = 10 sec.); (Adjustable from 10–600 sec.)

Client notification delay:

Delay time in the event of a loss of internet connection at the Comfion Pro control panel. This can occur, for example, due to a DSL failure, a missing LAN cable or a power failure at the router. (Default setting = 0 sec); (Adjustable from 0–600 sec.)

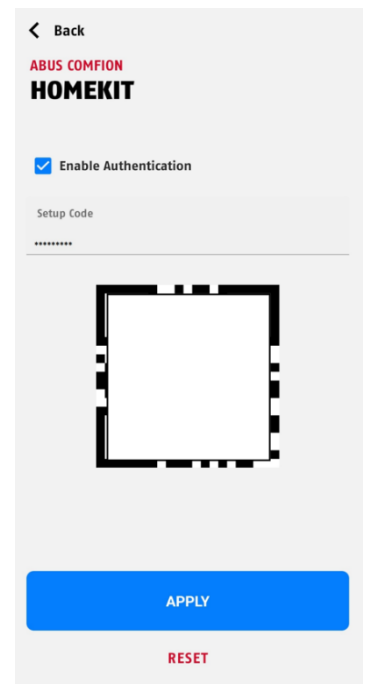
 Note	Depending on the network infrastructure, it may be advisable to increase the delay time slightly, particularly if the router manages a large number of IP clients.
---	--

Click 'Confirm' to apply the changes.

7.1.6. HomeKit

Add a new device in the Apple HomeKit interface

- During the process, you will be prompted to scan the QR code shown here and/or enter the 8-digit pairing code.



7.1.7. Backup

 Note	For security reasons, your control panel's backup file is stored in the Abus Cloud with full encryption.
---	--

Create a backup

In the Backup menu of the control panel configuration, you can create a backup manually and enable automatic backups. Automatic backups are performed weekly.

Restore backup

 Note	Please ensure that the new control panel has been updated to the latest firmware version before importing the backup.
---	---

To import the backup into a new control unit, please proceed as follows:

1. If you haven't already done so, disconnect the control unit from which the backup originates from the network and switch it off.
2. In the control panel overview in the app, tap the + icon to add a new control panel

3. Select "Backup Import"
4. Scan the QR code on the back of your new control centre
5. Select the control panel from which you wish to load the backup
Note: Once imported, the backup will be deleted from the cloud and the components will no longer work with the old hub.
6. Enter the desired name for your new control centre
7. Once confirmed, a verification code will be sent to the system owner's email address. Enter this code in the app and click on "Start Import"
8. The import will now be carried out. You can now close your app and wait until you receive the push notification that the control centre is online and the power supply is available.

To restore a configuration to the same hardware (control unit), please proceed as follows:

1. Reset the relevant control unit to factory settings (press the reset button for 10 seconds -> see 6.5.1)
2. In the hub overview in the app, tap the + icon to add a new hub
3. Select "Restore"
4. Scan the QR code on the back of your control panel
5. Enter the desired name for your control centre
6. The import will now take place. You can now close your app and wait until you receive the push notification that the control unit is online and powered up.

7.1.8. WLX Information

Here you will find a list of fallback permissions, including the reset card

Fallback authorisation:

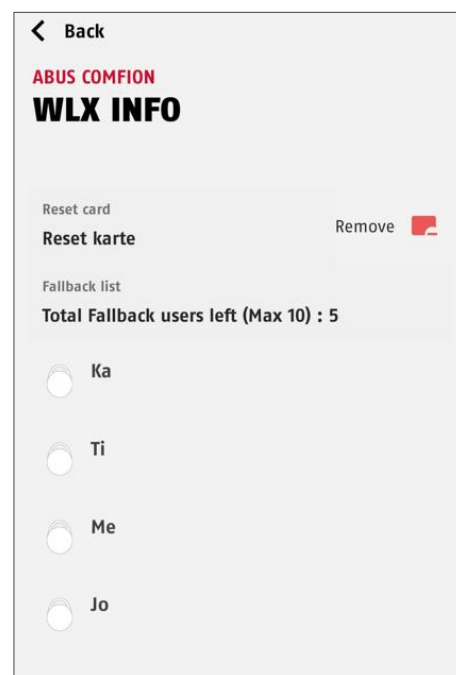
- The fallback authorisation is stored directly in the cylinder and allows access if there is no wireless connection to the Comfion Pro control panel & BUS-WLX module. Up to 10 fallback authorisations can be assigned in the Comfion Pro system (the reset card is always a fallback medium).
- In the event of an interrupted wireless connection, the authorised medium must be presented three times at the wAppLoxx cylinder (waiting for the signal each time)
- The fallback authorisation is stored directly in the user's NFC tag settings; see **Section 4.4** Editing Users

Reset card

- The reset card is included with the Comfion Pro BUS-WLX module.
- Once the first wAppLoxx component (cylinder or wall reader) has been programmed, the process for programming the reset card starts automatically.
- The reset card is required to reset a cylinder (in addition to the system card)
- If the reset card is lost, it can be deleted here by selecting 'Remove', after which a new reset card can be programmed. The programming process starts immediately after removal!

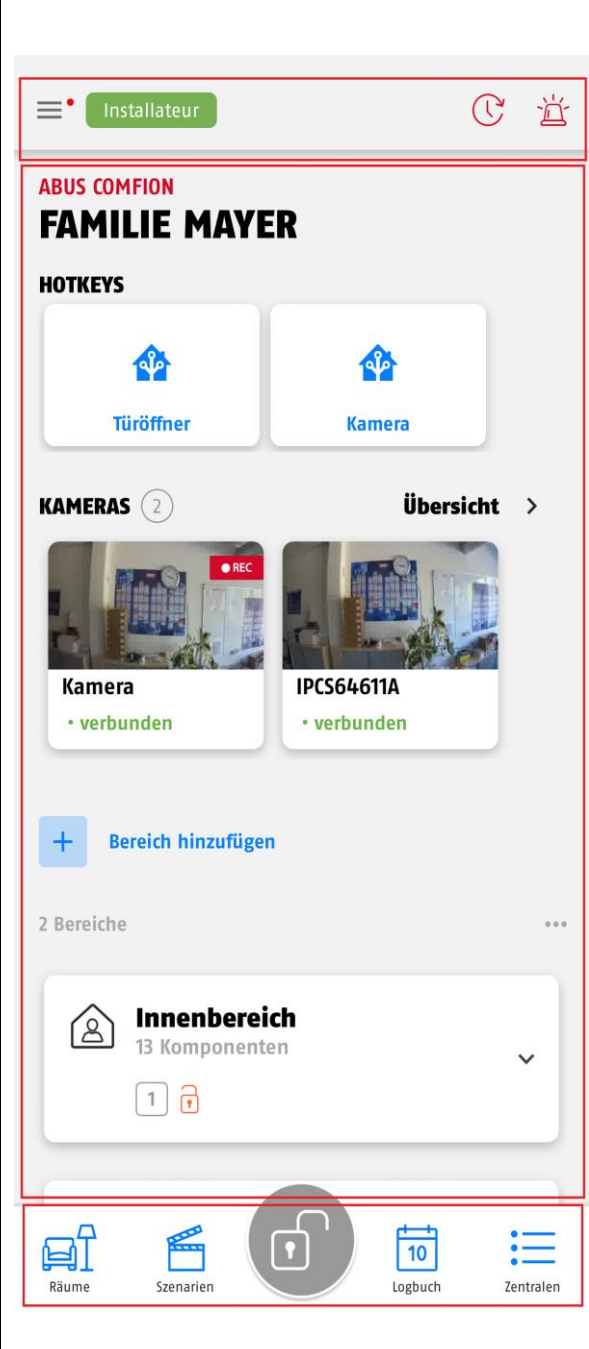
Fallback list

- In addition to the reset card, up to 9 further tags with fallback authorisation appear here.



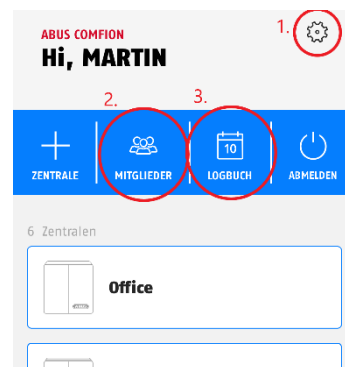
7.2. Dashboard (System set up)

You can control the system via the dashboard and, as an installer, carry out the majority of your work here.

	Header bar: •  Configuration & User Settings •  User role (installers only) •  Firmware update (if available) •  Trigger panic alarm Dashboard / Function Area • Hotkey buttons ◦ A short press starts the scene & execution is briefly confirmed by pressing and holding  ◦ Hold down to configure the scene • Camera preview images ◦ Clicking on a preview image switches to the live stream ◦ Clicking on "Overview" takes you to the camera details page & further configuration • Overview of sub-areas ◦ Clicking on '  ' displays assigned components and their status (if configured) ◦ Click on '  ' to customise the sorting of the sections. Navigation bar • Rooms (& component list) see 3.2.4 and 3.2.5 • Scenarios (scenes and automations) – see 6.4 • Alarm modes (lock icon) – see 3.2.8 • Logbook (event list & filter function) • Control centres (overview) – see 6.3
--	---

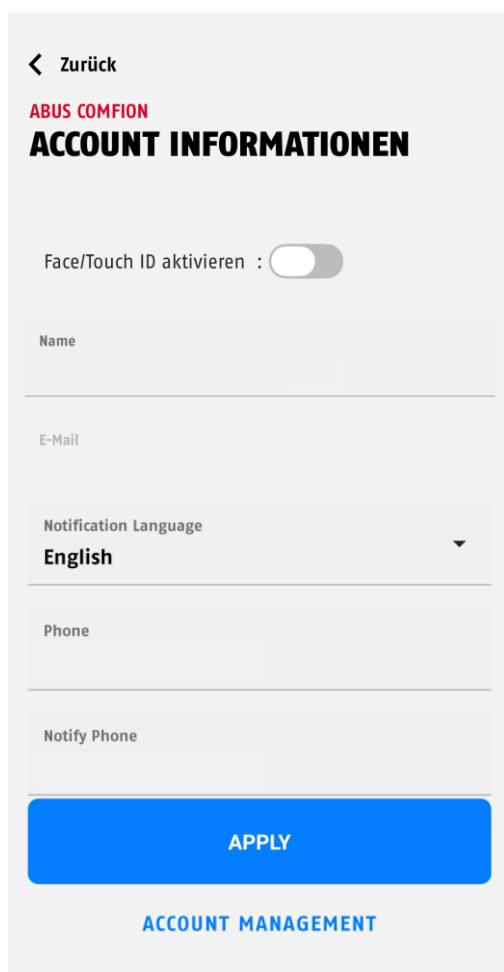
7.3. Control Centre overview

In the system's control panel overview, you can view and access existing control panels, add new ones, edit your account details (1), manage your members (2) and view the account log (3).



7.3.1. Account information

Access via the cog icon in the control centre overview.



- Enable Face/Touch ID
 - Secures the app using Face ID or Touch ID
- Account Name (displayed in Control Centre & Logbook)
- Account email
- Notification language
 - Defines the language for push, email and SMS notifications, the logbook, zones and rooms
- Phone number
- Notification phone number for SMS & calls
- Notification email address for emails sent by the control centre
- Date the account was created
- Confirmation button to save the entries
- In-app delete function for the ABUS account

7.3.2. Members

The Comfion app allows you to maintain a list of members. This is entirely optional and is not required for the operation of Comfion Pro systems. The member list makes it very easy to select new users from your existing members when adding or inviting them to a control centre.

7.3.3. Account Log

The account logbook lists all messages from systems with access authorisation. If access to a system is blocked, log entries from that control centre are not saved in the account log.

7.4. Automations & Scenes

The Comfion Pro system allows you to configure up to 100 scenarios. These scenes or automations can be set up entirely as you wish, offering you maximum flexibility.

Under the 'Scenarios' tab, you can add both scenes and automations.

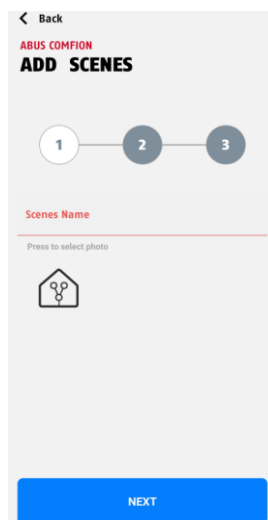
 Warning	Automations that contradict each other or trigger each other in a circular manner must not be created. This can lead to serious functional problems with the control panel.
---	--

 Note	Ensure that you leave a gap of at least 5 seconds between two switching commands for the same device to ensure smooth operation.
--	---

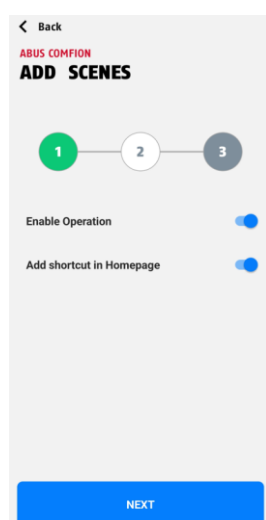
Scene = an action triggered by a user via the app (hotkey). Can be displayed in the dashboard. Example: Switching a socket ON/OFF via the app

Example configuration of a scene:

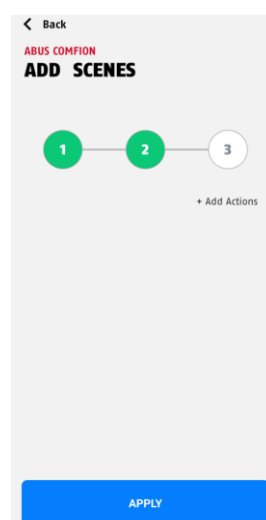
Assigning names / symbols



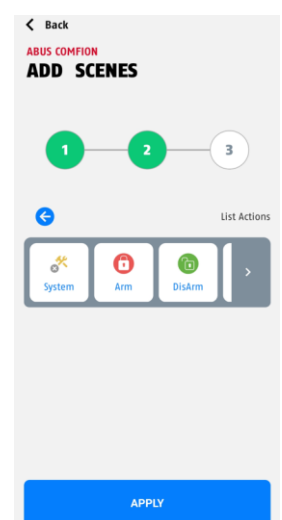
Scene settings



Add action



Select action



Step 1:

- The scene name is a required field
- Change the symbol by clicking on the icon

Step 2:

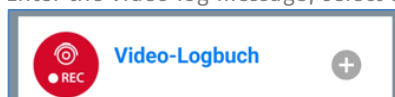
- Specify whether the scene should be active or inactive (inactive = scene name is greyed out)
- 'Show on Dashboard' displays the scene in the 'Hotkeys' section of the dashboard

Step 3 (Add action):

- Select the action from the list by clicking on it, enter any additional data if necessary, and finally add it by clicking on the '+' icon.

Example: Video Log:

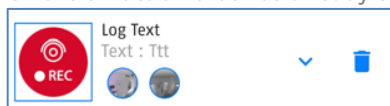
- Enter the video log message, select the cameras, and then press the '+' icon



- You can add some actions directly by clicking the "+" icon and then add further settings by clicking the 

icon.

- You can remove an action that has already been added by clicking on the bin icon



- You can configure multiple actions, which will then be executed one after the other. You can change the order in which they are executed by clicking on the '↕' icon. You can then reorder the actions using drag and drop. Clicking '↕' again saves the changes.
- Complete the scene configuration by clicking "Confirm" at the end.

The following actions can be added:

System	Video Log	Create a log entry with a log message and a clip from the camera recording (15 sec.) or the PIR-Cam image
	System restart	Restarts the Comfion Pro control panel.
	Push Event Video	Creates a push notification with message text and camera images, and sends it to the selected recipients
	Push Event Text	Creates a push notification with message text and sends it to the selected recipients
	Delay	Executes the scene with a delay of the specified time (seconds) or delays successive actions.
Arm		Arms a sub-area of the system Note: After adding this action, the sub-area must be specified by tapping the icon: 
Disarm		Disarms a sub-area of the system Note: After adding this action, the sub-area must be defined by clicking on the icon: 
Scene		Executes a pre-configured scene. Note: Select this function to execute multiple scenes simultaneously (or with a time delay).
Comfion socket	Switch on	Switches the socket on
	Switch off	Switches the socket off
	Toggle	Toggles the socket (on  off, off  on)
Comfion relay module	Switch on	Switches the relay module on
	Switch off	Switches the relay module off
	Toggle	Toggles the relay module (on  off, off  on)
Comfion blind module	Open	Moves the blind slats to the open & raised end position
	Close	Moves the blind slats to the closed end position & down
	Stop	Stops the Open or Close command
	100% up (50% / 1/3 / 25%)	Moves the blind slats up by the specified value
	100% close (50% / 1/3 / 25%)	Lowens the blind slats by the specified amount
	Open slats 100% (50% / 1/3 / 25%)	Opens the blind slats by the specified amount
	Close slats 100% (50% / 1/3 / 25%)	Closes the blind slats by the specified amount
	Manual control	Individual adjustment of the blind slats. Tap the icon:  to adjust the tilt angle (5 levels) and height (10 levels).
Comfion Pro control centre	Output On	Switches the Comfion Pro control unit's relay output on
	Output Off	Switches the relay output of the Comfion Pro control unit off
	Output Toggle	Switches the relay output of the Comfion Pro control panel.
Comfion indoor siren	Fire	Plays the voice announcement "Fire alarm"
	Alarm	Turns on the siren sound (set the duration at  ; max. 180 s)
	Stop	Turns the siren sound off
	Beep (signal tone)	Switches on the confirmation tone (set the number of repetitions (max. 30) and the piezo interval (max. 30 s) under '  '
	Failed	Enables the failure tone (under '  ' , set the number of repetitions (max. 30) and the piezo interval (max. 30 s)

	Doorbell	Enables the doorbell tone (under '  , set the number of repetitions (max. 30) and the buzzer interval (max. 30 s)
	Panic	Plays the voice announcement "Hijacking alarm"
	Water alarm	Plays the voice announcement
Comfion outdoor siren	Alarm	Switches on the siren sound (set duration under '  ' to max. 180 s)
	Stop	Turns off the siren sound
	Beep (signal tone)	Switches on the confirmation tone (set the number of repetitions (max. 30) and the piezo interval (max. 30 s) under ' )
	Gong	Enables the chime sound (set the number of repetitions (max. 30) and the piezo interval (max. 30 s) under ' )
Comfion smoke detector	Alarm Stop	Switches off the Comfion smoke detector alarm sound. (The detector will trigger again upon detection)
WLX-out (Comfion Hybrid Module)	Output 1, 2, 3 on	Switches output 1, 2 or 3 of the Comfion hybrid module on
	Output 1, 2, 3, off	Switches output 1, 2 or 3 of the Comfion hybrid module off
	Switch output 1, 2, 3	Switches output 1, 2 or 3 of the Comfion hybrid module
Comfion PIR Cam / Outdoor PIR Cam	Snapshot	Takes a manual snapshot
WLX Pro Cylinder (Access/Intrusion)	Office mode (permanent access)	Complements Office Mode (allows access without an NRC tag) By clicking on the icon:  , you can select whether Office Mode should be 'enabled' or 'disabled'.
	Remote release (Remote opening)	Pairs the lock cylinder via the app, thereby granting access. By clicking on the icon:  , you can set the pairing time (max. 180 sec.)
WLX Pro Wall reader (Access/Intrusion)	Remote release (Remote opening)	Controls the door opener (output to bridge box) via the app, thereby granting access. Click on the icon:  to set the pulse duration (6 or 12 s)
IP camera (IPxxxxxxx)	Go to Preset	Aligns the PTZ camera to a predefined position. By clicking on the icon:  Select position 1, 2, 3 or 4.

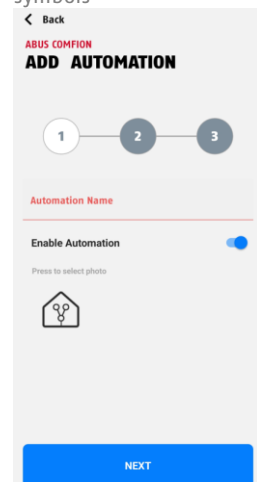
- Click on existing scenes to edit or delete them.

Automation = always consists of an 'if' and 'then' part. Freely configurable.

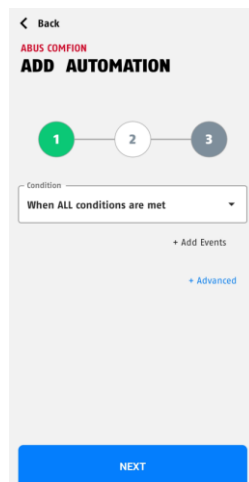
Example: If system is armed, then lights off

Example configuration of an automation:

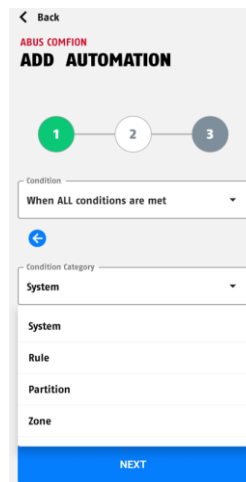
Assigning names / symbols



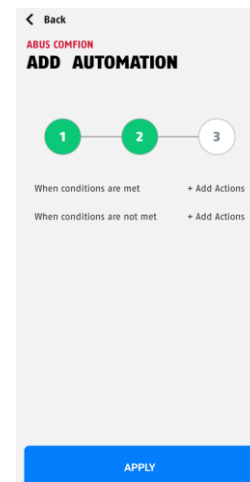
'If' part



Category selection



Then clause



Step 1:

- Enter the automation name (required field)
- Specify whether the automation is enabled or disabled
- Change the symbol by clicking on the icon

Step 2: (If defining an event)

- Choose between an 'And' link or an 'Or' link.
 - With the 'And' link, ALL conditions must be met for the action to be executed. With the 'Or' link, at least ONE condition must be met for the action to be executed.
- Select the "If" event.
 - You can set up multiple events, which must either ALL be met (AND condition) or at least ONE must be met (OR condition).
- The following "If" events can be selected:
 - System -> Here you will find system events such as a power cut, as well as the schedule
 - Rule  Existing automations can be integrated into an automation ...
 - Area -> Here you will find area events such as Armed/Disarmed, Intrusion, Ready to Arm and much more
 - Zone -> Here you will find all zone-related events (e.g. zone intrusion)
 - Room -> Here you will find all components and the associated events (e.g. opening detector contact open or wall switch button pressed)
- Additionally, under "Advanced", select ...
 - ... how long the set conditions must apply before the action is executed. The action will only be executed if the conditions apply for the set duration and do not change.
 - Example: If door is open for 30 seconds, then... send a push notification.

Step 3: (Then define event)

- The "If, then" -> action is executed if the conditions specified in the "If" section are met
 - The actions configurable here correspond to those in the Scene Configurator (Step 3)
- "If over, then" -> Action is executed if the conditions specified in the "If" section NO LONGER apply

Editing a scene/automation

To edit, press and hold the scene/automation icon for about 2 seconds, then release it

Deleting a scene/automation

You can delete a scene/automation by entering edit mode (see "Editing a scene/automation") and then clicking the "Delete scene/automation" button at the bottom of the screen.

7.5. Resets



7.5.1. Factory reset

To reset the control unit to factory settings, press and hold the reset button (button 12, see *2.3 Device description*) for >10 seconds and then release it. The control unit's LEDs will switch off after a few seconds and the control unit will restart. After restarting, the control unit will be set to factory settings and can be reconfigured.

7.5.2. Reboot

Press and hold the reboot button (button 13) for 2 seconds. The control unit's LEDs will switch off briefly. The control unit will restart.

 Note	The power supply is not interrupted during the restart described here. If, for example, the control unit is manually disconnected from the power supply during a restart, the control unit will carry out a check of all connected devices once the restart is complete – and this check results in numerous log entries.
---	---

7.5.3. User reset

To reset the system's users or delete all users from the system, press the network reset button (No. 14) five times within five seconds. After a few seconds, the Internet LED will briefly turn red. You should receive a push notification on the connected devices stating that the control unit in question has been removed.

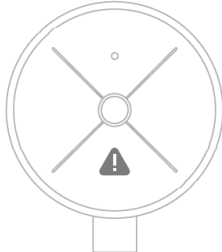
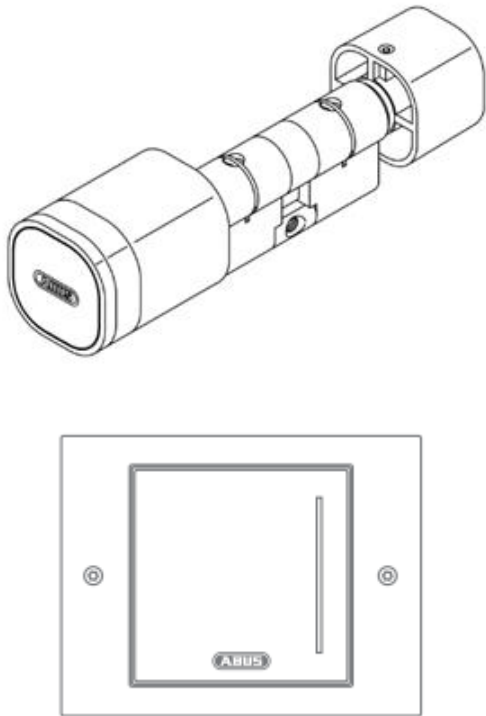
Once all the LEDs are green again (the Internet LED may be flashing green), you can add the device again via the + icon in your app.

7.5.4. Network reset

If you can no longer access your system on the network due to incorrect IP settings, you can reset the control panel to DHCP. To do this, press and hold the network reset button on the back of the control panel (No. 14) for 6 seconds. The system should be accessible again after a few minutes.

7.6. Operation

7.6.1. Arming / Disarming

APP: The system can be armed or disarmed in the app by selecting the alarm modes. To do this, click on the central button at the bottom of the screen in the dashboard (lock icon) and then select the action (e.g. Arm all).	
CONTROL PANEL: You can arm and disarm the system via a wireless control panel. To do this, enter your user code or hold the NFC tag in front of the control panel and then click on the action button (lock buttons). You can find more detailed information in the user guide or in the control panel manual	
REMOTE CONTROL: You can assign the alarm modes to the buttons on your wireless remote control and use them to perform the respective action at the touch of a button. You will find the settings under the remote control.	
WLX-Pro Cylinder / WLX Pro Wall Reader: carried out directly on the reader Arming: • Present the RFID tag to the reader • If necessary, lock the door within the opening time and present the RFID tag again • Arming successful: Red LED flashes once • Unsuccessful: Red LED flashes 6 times Disarming: • Present the RFID tag to the reader • After successfully disarming, the cylinder engages and the green LED flashes once • Failure: Red LED flashes 6 times  Note If the radio connection is interrupted, the fallback function is executed after the third unsuccessful read operation. For further details, see Section 6.1.8	

AUTOMATION: You can use an automation to link the arming or disarming of the system to specific conditions. This allows switching, for example, according to a schedule or when a wire input is triggered.

Important

According to EN 50131, disarming may only be carried out by authorised persons. A time-controlled arming operation may only take place in compliance with the principle of necessity (e.g. the user must leave the building and lock the door before arming can take place) and whilst the system is in a fault-free state. In this case, the arming process should be indicated by an audible and/or visual signal.

7.6.2.Resetting alarms

Depending on the settings, the Comfion Pro system can be reset in the following ways:

- If the 'Enable automatic reset' option is activated (under Control Panel Config. – Security Settings), the control panel automatically resets the alarm upon disarming, provided the relevant detectors are closed.
- If the "Enable automatic reset" option is deactivated (under Control Panel Config. – Security Settings), a message is displayed at the top of the app screen after an alarm and must be reset manually by the user.

Security settings	Dashboard	Reset alarm

7.6.3. Forced arming

The "Forced arming" function allows the control panel to be armed despite a triggered/open zone. The affected zone is bypassed automatically. No further manual bypassing of the detector is required.

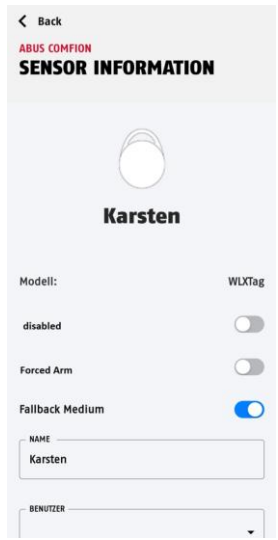
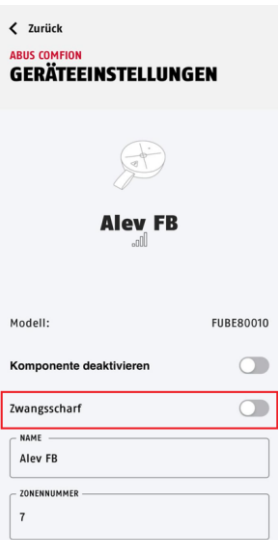
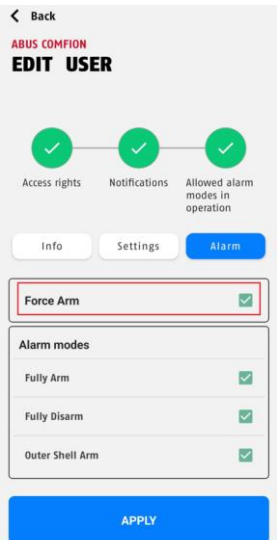
 Note	Please note that the forced arming function can only be executed if the triggered/open zone has the zone behaviour "Can be bypassed".
---	---

enable forced arming **via the keypad**, the forced arming code can be set under 'PIN codes' in the control panel configuration (see **Section 6.1.4**). This 3-digit code is entered after the 4-digit user code to perform forced arming via the keypad.

In addition, the "Forced arming" property can be assigned to a **transponder** to enable arming with it.

To enable forced arming **via the wireless remote control**, tick the "Forced arming" box in the remote control settings.

To enable forced arming **via the app**, tick the 'Forced arming' box under each user in the 'Alarm' tab.

			
Control panel & forced arming code	Transponder settings	Remote control	User settings Alarm

7.7. Key to symbols

Power supply	
	Battery charge level 100% / 75% / 50% / 25% / Battery empty
	Left: external power supply (DC or AC) connected Right: Emergency power supply (rechargeable battery) on standby
Radio signal	
	4 bars = Excellent 3 bars = Very good 2 bars = Moderate 1 bar = poor
	Radio connection interrupted. Occurs following failure of the supervision signal for the respective component, i.e. after > 1 hour (may vary for individual components)
Device behaviour	
	Component triggered (e.g. door contact open, vibration detector triggered, smoke detector triggered, water detector triggered)
	Movement detected (PIR motion detector / microwave motion detector)
	Device triggered (e.g. siren activated, button pressed)
	Zone closed (e.g. contact closed)
	Zone open (e.g. contact open) → Appears in addition to the 'Component triggered' symbol

Faults	
	Tampering detected (e.g. housing opened or device removed from mounting surface) Alternative symbol: 
	Cable break detected (e.g. 3-in-1 detector)
Action icons (pressing the icon triggers the described action)	
	Device status OFF (e.g. wireless socket switched off) → Pressing the icon switches the device ON
	Device status ON (e.g. wireless socket switched on) → Pressing the icon switches the device OFF
	PIR camera 1. Create recording (pressing the icon triggers manual recording) 2. Recording is being created 3. Recording is transferred to the central storage.
WLX icons (access control)	
	Access granted Display is active for the duration that the cylinder is engaged (6/12 sec)
	Permanent access is activated (office mode switched on)  Hinweis Permanent access is a configuration in the control panel. To activate it, the cylinder must first be 'woken up' (i.e. turned) and establish a wireless connection to the control panel. Access is then granted.
	Sub-area armed The sub-areas to which the cylinder / wall reader is assigned are armed

7.8. ABUS Cloud

The Comfion Pro wireless security system connects to the ABUS Cloud during initial commissioning. The system is also stored in the installer's ABUS Cloud specialist installer account. If this is not desired, the tick next to 'Main installer' can be removed for the relevant user in the system, or set for a different installer.

7.9. Notes on the hard drive / SSD data storage

- The screws used to secure the hard drive must only be tightened by hand
- The control panel's battery life is affected by the built-in hard drive and its power consumption, as well as the number of connected BUS devices.
 - The emergency power duration required by EN 50131 for Grade 2 burglar alarm control panels is ensured by the use of an SSD data storage device and the connection of up to 2 BUM080000 WLX Pro modules to the Comfion Pro BUS!
- The hard drive installed in the Comfion Pro must be formatted in exFAT or NTFS
- Only replace the hard drive/SSD data storage device when the control panel is powered off

7.10. maintenance and servicing by the installer

During routine maintenance, check that the system is functioning correctly:

- Check the Comfion Pro for obvious signs of damage to the housing, wall bracket or front cover.
- Check the operation of the tamper switch
- Check the condition of the emergency power batteries
- Clean the housing
 - To clean, please wipe the surface with a dry, soft cloth.
 - Do not use water, solvents or cleaning agents.
- Check the signal strength and the battery/rechargeable battery status of all components
- Replace the batteries as recommended in the manufacturer's instructions
- Test each component.
- Carefully clean the lenses of all PIR detectors and cameras with a clean, dry, soft cloth.
 - Do not use water, solvents or cleaning agents.
- Carry out a walk-through test of all detectors.
- Test all signal transmitters
- Test the communication.



Note

ABUS recommends replacing the control panel battery after a maximum of 3 years. If used for longer, a sudden drop in performance cannot be ruled out.

To replace the control unit's battery:

- Set the control unit to maintenance mode (security settings)
- Remove the control unit from the wall bracket
- Set the battery switch to "OFF"
- Open the front cover by loosening the screws at the back and prying the cover open (for further details, see **section 3.1** Wall mounting of the control unit)
- Disconnect the power supply and the old battery from the control unit
- Wait 30 seconds
- Reconnect the new battery and the power supply
- Close the system cover and then exit maintenance mode

7.11. Table of wireless signal strengths

The following table describes the meaning of the signal values displayed in dBm for Comfion wireless components.

RSSI value (dBm)	Meaning	Display on component
≤ -100	Poor	0 bars
≤ -96	OK	1 bar
≤ -91	Good	2 bars
≤ -86	Very good	3 bars
> -86	Excellent	4 bars

8. Warranty

- ABUS products are designed, manufactured and tested with the utmost care in accordance with applicable regulations.
- The warranty covers only defects attributable to material or manufacturing faults at the time of sale. If a material or manufacturing fault is proven to exist, the module will be repaired or replaced at the discretion of the warranty provider.
- In such cases, the warranty expires at the end of the original warranty period of 2 years. Any further claims are expressly excluded.
- ABUS shall not be liable for defects and damage caused by external influences (e.g. transport, force, incorrect operation), improper use, normal wear and tear, or failure to observe these instructions and the care instructions.
- When making a warranty claim, the product in question must be accompanied by the original proof of purchase showing the date of purchase and a brief written description of the fault.
- If you discover a defect in the product that was already present at the time of sale, please contact your retailer directly within the first two years.

9. Disposal instructions



Dispose of the device in accordance with the EU Directive 2012/19/EU on waste electrical and electronic equipment (WEEE). If you have any queries, please contact the local authority responsible for waste disposal. Information on collection points for your old appliances can be obtained, for example, from your local council or town hall, local waste disposal companies or your retailer.

10. Conformity

10.1. EU Declaration of Conformity

ABUS Security Center GmbH & Co. KG hereby declares that the radio equipment type FUAA85000 complies with Directive 2014/53/EU and 2011/65/EU. The full text of the EU Declaration of Conformity is available at the following web address: abus.com > Product search > FUAA85000 > Downloads

10.2. Conformity to EN 50131

The FUAA85000 security system is certified to Security Level 2 and, when properly installed, complies with EN 50131-1+A3:2020, EN 50131-3:2009, EN 50131-10:2014, EN 50136-1+A1:2018, EN 50136-2:2013 and EN 50131-5-3:2017.

11. Appendix

11.1. Contact-ID Code Table

Code	Code class	Additional data	Type	Description
111	Fire alarm	Zone	Smoke	A smoke detector has triggered a 24-hour fire alarm
120	Panic alarm	Zone	Panic	A panic alarm was triggered at the control panel
121	Panic Alarm	User	Threat	A user has entered the threat code
130	Burglary Alarm	Zone	Intrusion	An intrusion zone has been triggered whilst the system is armed
131	Burglary Alarm	Zone	Perimeter	A perimeter zone triggers a pre-alarm
133	Intruder Alarm	Zone	24-hour zone	A 24-hour intrusion alarm zone has been triggered
134	Burglar Alarm	Zone	Entry/Exit	An entry/exit zone has been triggered whilst the system is armed
135	Intruder Alarm	Zone	Immediate Monitored Zone	An immediate (monitored) zone was triggered whilst the system was armed
137	Intruder Alarm	Zone	Tamper	Control panel tamper alarm was triggered
139	Intruder alarm	Zone	Glass break	Burglary confirmed by a zone
154	24 hours Technical alarm	Zone	Water alarm	Water detector reports fault
301	System fault	Zone	AC mains power failure	Loss of mains voltage to the control panel or expansion module whilst the system is disarmed
302	System fault	Zone	Battery fault	Control panel buffer battery empty whilst system is disarmed
305	System fault	Zone	Reset	The system has been reset and restarted
306	System fault	Zone	Restart	The system has restarted
308	System fault	Zone	Shutdown	The system has been shut down and has ceased operation
311	System fault	Zone	Battery missing / out of service	The control panel's backup battery is missing or completely discharged
338	Peripheral fault	Zone	Control panel locked	The control panel is locked due to repeated incorrect code entries
344	Peripheral fault	Zone	Jamming detection	The wireless receiver has detected a jamming signal.
350	Communication fault	Zone	Comm. error	The system has detected a communication error.
381	Detector fault	Zone	Supervision	The specified zone has not reported during the supervision interval.
383	Detector fault	Zone	Tamper	A tamper alarm has been triggered in the relevant zone
384	Detector fault	Zone	Low battery	A low battery alarm has been triggered in the relevant zone
393	Detector fault	Zone	Fault – Maintenance	The relevant zone has reported a fault
400	Arming/Disarming/ Remote access	User	Armed/ Disarmed	The user in question has armed or disarmed the system via remote control
401	Arm/Disarm/ Remote access	User	Arm/Disarm via user	The relevant user has armed or disarmed the system via the smartphone app
406	Arming/Disarming/ Remote access	User	Reset	The user in question has reset the previously triggered alarm

407	Arming/Disarming/ Remote access	User	Arm/Disarm via control panel	The user in question has armed or disarmed the system using a wireless control panel
443	Arming/Disarming/ Remote access	User	Arming with fault suppression	The user in question has armed the system by bypassing faults
454	Arming/Disarming/ Remote access	User	Arming failed	The system could not be armed after the exit delay
461	Arming/Disarming/ Remote access	Zone	Incorrect code entered	An incorrect code has been entered on the control panel.
570	Hide	Zone	Hide zone	The relevant zone has been hidden
572	Hide	Zone	Hide 24-hour zone	The relevant 24-hour zone has been hidden
602	Test	-	Periodic test message	A periodic test message has been transmitted to the control centre.

ABUS | Security Center GmbH & Co. KG
abus.com

Linker Kreuthweg 5
86444 Affing
Germany

Tel: +49 82 07 959 90-0



Security Tech Germany

FUAA85000

INSTRUCTION D'INSTALLATION

Système de sécurité sans fil Comfion Pro



1.	Mises à jour	5
1.1.	Instructions	5
1.2.	Comfion Pro Firmware & Release notes	5
2.	Généralités	6
2.1.	Introduction	6
2.2.	Utilisation conforme / Informations juridiques	6
2.3.	Service à la clientèle / Customer Support	6
2.4.	Mentions légales	6
2.5.	Signification des symboles	7
3.	Principe de fonctionnement et caractéristiques	7
3.1.	Caractéristiques du produit	7
3.2.	Contenu de la livraison	8
3.3.	Description de l'appareil	9
3.4.	Données techniques	11
4.	Montage et mise en service	12
4.1.	Montage mural de la centrale	12
4.2.	Mise en service du système	15
4.2.1.	Installation via l'application & fin des préparatifs matériels	15
4.2.2.	Tableau de bord (après la première connexion)	18
4.2.3.	Partitions	18
4.2.4.	Pièces	19
4.2.5.	Composants	20
4.2.6.	Paramètres des composants	22
4.2.7.	Remarques sur le câblage (entrées/sorties/BUS)	23
4.2.8.	Modes d'alarme	24
4.3.	Installation et programmation de WLX Pro	25
4.3.1.	Installation, configuration et utilisation des cylindres et lecteurs muraux WLX Pro	26
4.3.2.	Fonctions WLX Pro - Ouverture à distance et mode bureau	27
4.4.	Caméras (NVR)	28
4.4.1.	Intégration de caméras par ONVIF	28
4.4.2.	Intégration de caméras par RTSP	29
4.4.3.	Paramètres de la caméra (global)	30
4.4.4.	Paramètres de la caméra (un par un)	30
4.4.5.	Fonctionnement du NVR	32

5. Utilisateurs et groupes d'autorisation	33
5.1. Explication des différents rôles	33
5.2. Mise en service	34
5.2.1. Remise au propriétaire	34
5.3. Inviter/ajouter des utilisateurs	34
5.4. Modifier les utilisateurs	34
5.4.1. Droits d'accès	34
5.4.2. Notifications	35
5.4.3. Modes d'alarme autorisés en fonctionnement	36
5.5. Suppression d'utilisateurs	36
6. Communication	36
6.1. Module GSM	36
6.2. Courrier électronique	37
6.3. Appel téléphonique	38
6.4. SMS	38
6.5. SIA CC-09 (connexion à la station de contrôle)	39
7. Généralités, entretien et remarques	40
7.1. Configuration de la centrale	40
7.1.1. Informations générales	40
7.1.2. Réseau	40
7.1.3. Paramètres de sécurité	41
7.1.4. Codes PIN	43
7.1.5. Retards de notification	43
7.1.6. HomeKit	44
7.1.7. Backup	44
7.1.8. Informations sur WLX	45
7.2. Tableau de bord (système configuré)	46
7.3. Aperçu des centrales	47
7.3.1. Informations sur le compte	47
7.3.2. Membres	48
7.3.3. Journal de bord du compte	48
7.4. Automations & scènes	48
7.5. Réinitialisations	52
7.5.1. Réinitialisation d'usine	52
7.5.2. Redémarrage (reboot)	52

7.5.3.	Réinitialisation de l'utilisateur	52
7.5.4.	Réinitialisation du réseau	52
7.6.	Utilisation	53
7.6.1.	Armement / désarmement	53
7.6.2.	Réinitialisation des alarmes	54
7.6.3.	Armement forcé	55
7.7.	Signification des symboles	56
7.8.	ABUS-Cloud	57
7.9.	Remarques sur le disque dur / le stockage de données SSD	58
7.10.	Maintenance et entretien par l'installateur	58
7.11.	Tableau des forces du signal radio	58
8.	Garantie	59
9.	Élimination	59
10.	Conformité	59
10.1.	Déclaration de conformité UE	59
10.2.	Conformité à la norme EN 50131	59
11.	Annexe	59
11.1.	Contact ID Tableau de codes	59

1. Mises à jour

1.1. Instructions

Version	Date Publication	Modifications
1.0	12.05.2026	Version initiale
1.1	13.05.2026	Compléments : - Nouveau : Chapitre 1 Mises à jour (précédemment chapitre 7) - Chapitre 3.2.6 : Complément des caméras IP & MotionAlarm - Nouveau : Chapitre 3.3 Installation et programmation de WLX Pro - Nouveau : Chapitre 3.4.3 Paramètres de la caméra (global) - Nouveau : Chapitre 3.4.4 Paramètres de la caméra (individuellement) - Nouveau : Chapitre 3.3.2 Intégrer des caméras par RTSP - Nouveau : Chapitre 10.1 Tableau des codes Contact ID - Chapitre 6.6.1 : Cylindre WLX Pro armé/désarmé & Wallreader complétés
1.2	30.06.2026	Compléments : - Nouveau : Ajout des versions en anglais, français et néerlandais. - Ajout des notes de mise à jour pour le micrologiciel 1.0.2945 de Comfion Pro

1.2. Comfion Pro Firmware & Release notes

Version firmware	APP-Version	Date Publication	Modifications
1.0.2864	2.1.96	12.05.2026	Version initiale
1.0.2945	2.1.134	30.06.2026	Modifications : - Ajustement des valeurs par défaut du FUBE80100 afin d'augmenter l'autonomie de la batterie - Ajustement du délai de réveil du FUBE80100 afin d'augmenter l'autonomie de la batterie - Ajustement de diverses entrées du journal (ajout d'utilisateur, de zone, etc.) - Ajustement de la préconfiguration du module hybride lorsqu'il est utilisé avec wApploxx - Améliorations apportées au flux vidéo H.265 - Ajustements de sécurité - Ajustements des chaînes de caractères et de la conception Corrections: - Problème d'inévitabilité des composants WLX Access - Message d'autorisation « Accès à la galerie » au lancement de l'application - Correction des paramètres de sécurité – sabotage du panneau d'alarme

Vous trouverez les notes de mise à jour de la dernière mise à jour du firmware dans votre application Comfion ou en cliquant sur le lien suivant : <https://l.ead.me/bgiCEA>

2. Généralités

2.1. Introduction

Nous vous remercions d'avoir choisi le **système de sécurité sans fil Comfion Pro**, un produit ABUS Security-Center (également appelé « ABUS » dans sa forme abrégée).

Le présent manuel contient des descriptions essentielles, des données techniques, des aperçus et des informations complémentaires sur la configuration, la mise en service et l'utilisation du **système de sécurité sans fil Comfion Pro**.

Les produits/systèmes décrits ici ne doivent être installés et entretenus que par des personnes qualifiées pour la tâche en question. Le personnel qualifié pour l'installation et la maintenance du système est en général un partenaire spécialisé ABUS formé.

2.2. Utilisation conforme / Informations juridiques

La responsabilité d'une utilisation du produit conforme à la législation incombe à l'acheteur ou au client et à l'utilisateur final. Conformément à la responsabilité civile du fabricant pour ses produits, définie dans la loi sur la responsabilité du fait des produits, les informations ci-dessus doivent être respectées et transmises aux exploitants et aux utilisateurs. Le non-respect de cette consigne libère ABUS Security Center de sa responsabilité légale.

Une utilisation non conforme ou inhabituelle, des travaux de réparation ou des modifications non expressément autorisés par ABUS ainsi qu'un service non conforme peuvent entraîner des dysfonctionnements et doivent être évités. Toute modification non expressément autorisée par ABUS entraîne la perte des droits de responsabilité, de garantie et des droits de garantie convenus séparément.

Les architectes, les planificateurs techniques de bâtiments (TGA) et autres institutions de conseil sont tenus de se procurer toutes les informations nécessaires sur les produits auprès d'ABUS afin de satisfaire aux obligations d'information et d'instruction conformément à la loi sur la responsabilité du fait des produits. Les commerçants spécialisés et les transformateurs sont tenus de respecter les consignes de la documentation ABUS et, le cas échéant, de la transmettre à leurs clients.

Vous trouverez de plus amples informations sur www.abus.com à la page générale ou, pour les revendeurs et les installateurs, sur le portail des partenaires à l'adresse <https://partner-asc.abus.com/>

2.3. Service à la clientèle / Customer Support

Pour toute aide supplémentaire, notre équipe d'assistance est à votre disposition : support@abus-sc.com

Vous trouverez des informations générales sur le **système de sécurité sans fil Comfion Pro** sur notre site Internet sous : <https://www.abus.com/de/Privat/Alarmsysteme/Comfion-Funk-System>

2.4. Mentions légales

La parution d'un guide d'installation plus récent rend cette édition caduque.

Tous droits réservés. Sans l'accord écrit de l'éditeur, il est interdit de reproduire ces instructions d'installation, même partiellement, sous quelque forme que ce soit ou de les copier ou de les traiter en utilisant des procédés électroniques, mécaniques ou chimiques.

ABUS Security Center décline toute responsabilité pour les erreurs de nature technique ou d'impression et leurs conséquences. Les informations contenues dans ce guide d'installation ont été rédigées en toute bonne foi et en tenant compte de l'état actuel de la technique. Elles sont régulièrement contrôlées et, si nécessaire, mises à jour ou corrigées.

Toutes les marques et tous les droits de propriété intellectuelle sont reconnus, des modifications peuvent être apportées sans préavis dans le sens du progrès technique.

2.5. Signification des symboles

Les symboles suivants sont utilisés dans ce guide d'installation :

Symbole	Mot-signal	Signification
	Attention	Indique un risque de blessure ou de danger pour la santé dû à la tension électrique
	Important	Indique un risque d'endommagement de l'appareil/accessoire ou un risque de blessure ou pour la santé
	Remarque	Signale des informations importantes

3. Principe de fonctionnement et caractéristiques

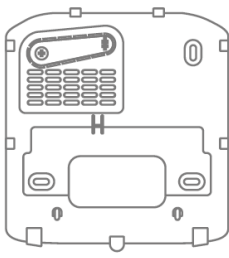
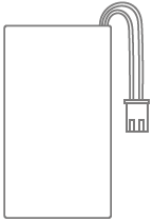
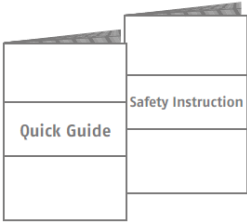
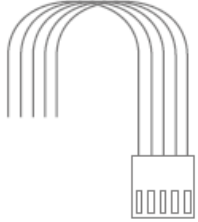
3.1. Caractéristiques du produit

Le système de sécurité sans fil FUAA85000 Comfion Pro est un système de détection d'intrusion certifié EN-niveau-2 avec des fonctions Smart Home. Le système peut être configuré et utilisé via l'application intuitive ou le portail ABUS Cloud.

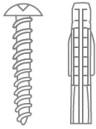
Principales caractéristiques :

- Système de sécurité tout-en-un : Système d'alarme, NVR vidéo (jusqu'à 8 caméras) et contrôle d'accès en un seul système - réduit la diversité des appareils et les frais d'installation.
- Intégration native de wAppLoxx Pro : Armement/désarmement direct au niveau de la porte - moins de fausses alarmes, meilleure acceptation de l'utilisation par le client final.
- Alarme périmétrique avec composants extérieurs : Détection précoce des intrus - augmentation du temps d'intervention et réduction du risque d'intrusion.
- Enregistreur vidéo en réseau intégré : Enregistrement et gestion centralisés pour jusqu'à 8 caméras - images vidéo directement visibles dans l'application en cas d'alarme et réalisables sans enregistreur NVR supplémentaire.
- Commande par application & scénarios Smart-Home : Commande centralisée de tous les composants, scénarios configurables de manière flexible - solution idéale pour les exigences individuelles des clients.
- Évolutif et capable de gérer des projets : Jusqu'à 160 composants radio et 40 partitions - avec une grande portée radio jusqu'à 2600 m en champ libre pour une planification efficace des petits objets jusqu'aux grands projets.
- Radio 868 sécurisée avec cryptage AES128 bits : Cela garantit une grande sécurité de transmission, la radio bidirectionnelle assure que le signal radio est bien arrivé
- EN 50131 niveau 2 : Convient aux exigences de sécurité liées à l'assurance et aux projets professionnels.
- Sauvegarde de la téléphonie mobile 4G : Transfert d'alarme sécurisé même en cas de panne de réseau - disponibilité accrue du système.
- Anti-sabotage : Contact d'arrachement & surveillance système - fonctionnement fiable au quotidien.
- Surveillance du brouillage : Si un brouilleur est détecté, Comfion Pro émet une alarme.
- Engager un service de sécurité : Protocole de la station de contrôle intégré (SIA CC-09)
- Toujours toutes les informations à portée de main : Notifications au choix par SMS, e-mail ou message push

3.2. Contenu de la livraison

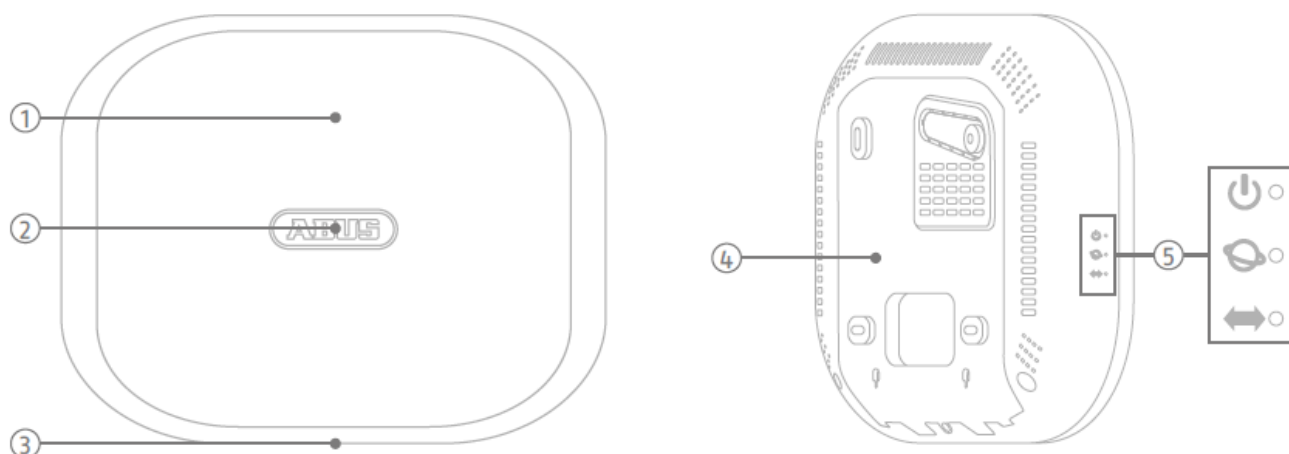
		
1 x centrale	1 x support mural	1 x batterie
		
Guide de démarrage rapide & consignes de sécurité	2 x câble détecteur filaire	4 x vis pour disque dur
		
1 x outil d'ouverture		

Nécessaire :


4 x vis / cheville Ø 7,0 mm

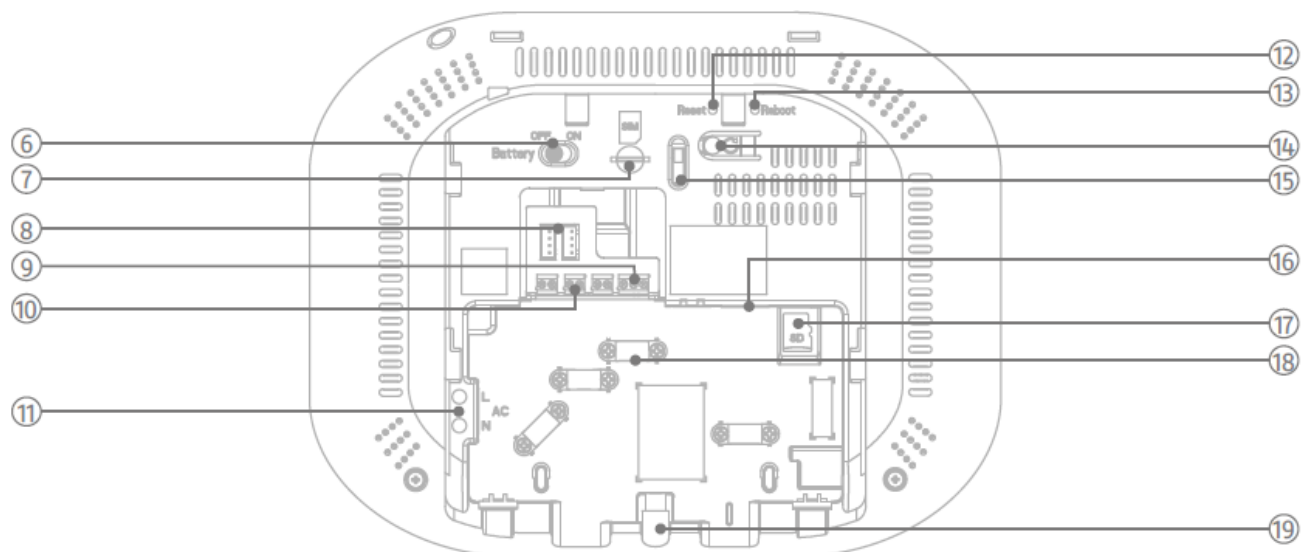
3.3. Description de l'appareil

Structure du produit (recto/verso)



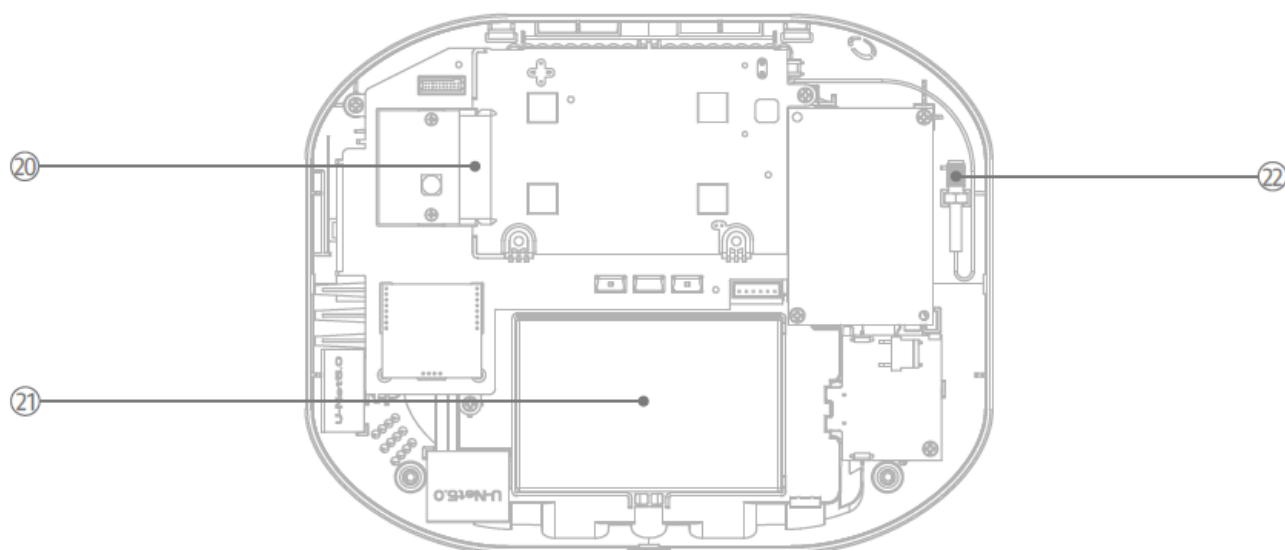
1	Couvercle	2	Logo (état de l'alarme)	3	Mécanisme d'ouverture
4	Plaque arrière	5	LED d'état Alimentation, Internet, réseau		

Dos (ouvert)



6	Interrupteur de pile	7	Emplacement pour carte SIM (nano-SIM)	8	Entrées de détecteurs filaires
9	Sortie relais	10	Bornes BUS	11	Bornes de raccordement AC (L/N)
12	Touche Reset	13	Bouton de redémarrage	14	Réinitialisation du réseau
15	Interrupteur anti-sabotage	16	Prise RJ45	17	Emplacement MicroSD
18	Décharge de traction	19	Vis de fixation		

Face avant (ouverte)



20 Connexion SATA pour disque dur SSD	21 Batterie de secours	22 Connexion Antenne externe de téléphonie mobile (SMA)
---------------------------------------	------------------------	---

LED d'état

			
Logo (état de l'alarme)		LED d'état	
Désarmé	Blanc	LED d'alimentation (en haut)	
Armé	Bleu	Tension du réseau	Vert
Partiellement armé	Bleu	Fonctionnement sur piles	Rouge
Alarme	Rouge (clignoter)	M-à-j firmware	Jaune (clignoter)
Centrale de sabotage	Rouge (clignoter)	LED Internet (au centre)	
Procédure d'apprentissage	Vert (clignoter)	Enregistré en ligne & Admin	Vert
Mode mainten.	Violet	En ligne & Admin non enregistré	Vert (clignoter)
Défaut	Orange (clignoter)	Hors ligne	Rouge
		LED réseau (en bas)	
		LAN	Vert
		Téléphonie mobile 3G/4G	Rouge

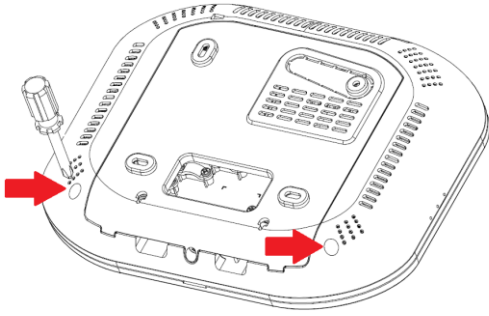
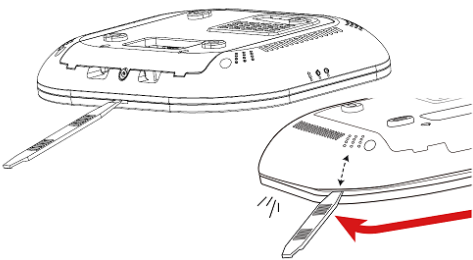
3.4. Données techniques

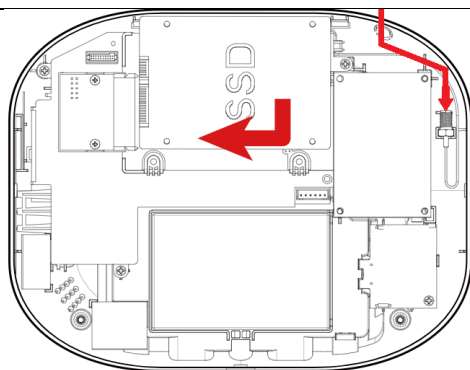
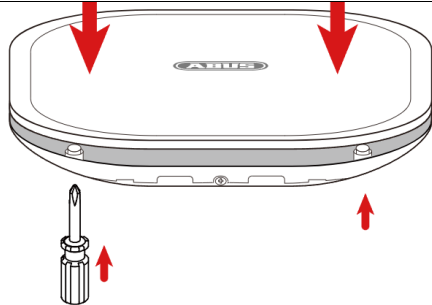
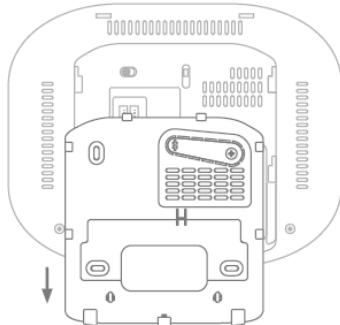
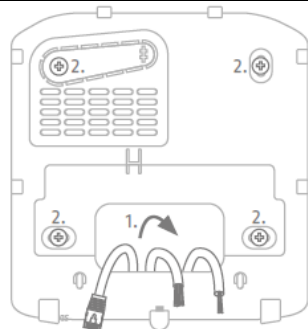
Dimensions (LxHxP)	242 x 190 x 45 mm
Poids	950 g (avec batterie de secours)
Température de fonctionnement	-10 °C à +40 °C
Classe d'environnement	II (EN 50131-1 + A3:2020)
Protection contre les effets sur l'environnement	IP40 / IK06
Humidité de l'air	max. 85 % HR (humidité relative de l'air)
Raccordements	Prise L/N (230 volts), RJ45 (LAN), prise SATA 3.0 (pour SSD 2.5"), emplacement pour carte SIM (nano sim), emplacement pour carte Micro-SD
Entrées/sorties	4 entrées de groupe de détecteurs (NC/NO) sans potentiel (type de câblage 2 fils CC, EOL, DEOL) 1 sortie relais (NC/COM/NO) max. 30 V CC / 1,6 A
Interface BUS	(GND / +V / B / A) 13,0 V Longueur de câble max. 200 m
Affichages	LED d'état (alimentation, Internet, communication) Logo ABUS (état du système)
Touches	Bouton de redémarrage, bouton de réinitialisation, réinitialisation du réseau, interrupteur de batterie
Fréquence radio / modulation	868,0 - 868,6 MHz / GFSK
Puissance, radio / portée	max. 25 mW (14 dBm) / 1000 m, champ libre
Nombre de composants radio	160
Nombre de partitions	40
Nombre d'utilisateurs	51
Nombre d'événements	> 10 000
Enregistreur réseau	Max. 8 canaux @ 2048 kbps, En utilisation 4 canaux @ 4096 kbps Exemple : 4 canaux a 4K (3840 x 2160) + 4 canaux a 1080p (1920 x 1080)
Communication	Ethernet 1 GbE LAN SSL/TLS Réseau mobile (sauvegarde) : 3G UMTS / 4G LTE SMS & voix : 2G GSM / 4G LTE
Catégorie AÛA	SP5 (LAN) SP2 (GSM) DP3 (LAN + GSM)
Alimentation électrique	Primaire : AC 230 V / 50 Hz Secondaire : Accu LiPo 7,4 V / 6000 mAh
Type d'alimentation électrique	Type A, alimentation électrique conforme aux normes EN50131-1+A3:2020 et EN50131-6+A1:2021
Temps de tampon - Fonctionnement sur batterie	> 12 heures selon EN50131-1+A3:2020 niveau 2
Sécurité anti-sabotage (détection/protection)	oui (1x contact d'arrachement mural)
Temps de supervision	900 - 3 600 s (préréglage : 3 600 s)
Degré de sécurité	Niveau 2 (EN 50131-1 + A3:2020)
Conformité	Degré de sécurité 2 en cas d'installation correcte conforme aux normes EN 50131-1+A3:2020, EN 50131-3:2009 et EN 50131-5-3:2017
Directives européennes	RED : 2014/53/UE, RoHS : 2011/65/UE + 2015/863 Sécurité générale : 2001/95/CE

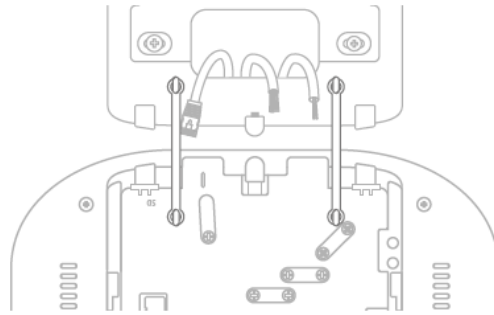
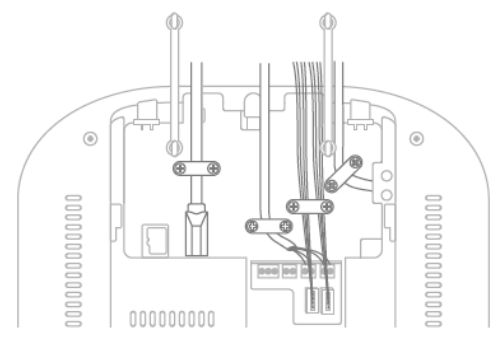
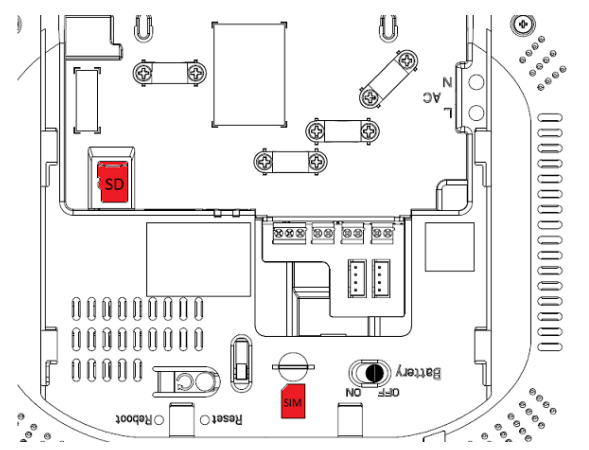
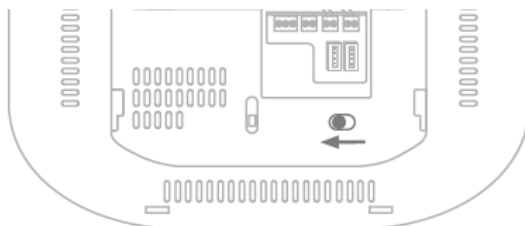
4. Montage et mise en service

4.1. Montage mural de la centrale

 Attention	ATTENTION : AVANT D'INSTALLER CE SYSTÈME, VOUS DEVEZ VOUS ASSURER QUE L'ALIMENTATION SECTEUR DE LA CENTRALE D'ALARME EST COUPÉE ET INTERROMPUE. (Veillez également à ce que l'interrupteur de la pile soit sur « Off »). Tous les raccordements électriques doivent être effectués par un électricien qualifié et être conformes aux réglementations locales en vigueur.
 Attention	ATTENTION : Si l'appareil est raccordé au réseau électrique alors qu'il est sous tension, la tension du réseau est également présente sur les têtes enrobées des bornes à vis du raccordement au réseau. ATTENTION : Le câble d'alimentation de la centrale d'alarme doit être équipé d'un dispositif de séparation bipolaire conforme à la norme EN 62368-1. Attention : Lorsque vous manipulez le circuit imprimé dans la centrale d'alarme, vous devez prendre les précautions d'usage pour éviter tout dommage dû à l'électricité statique.
 Remarque	- Montez la centrale au mur à une hauteur d'environ 1,5 m. - Maintenez une distance d'au moins 1,5 m de tous les côtés par rapport aux appareils suivants : les appareils électriques, les objets métalliques ou les appareils émettant des ondes radio (par exemple les routeurs, les micro-ondes) - car ils peuvent affecter les performances radio du système.

Fixation du disque dur / de la mémoire de données SSD et de l'antenne externe de téléphonie mobile (non fournie)	
Ouvrez le couvercle de la centrale. Pour ce faire, desserrez les 2 vis à l'arrière.	
Soulevez le couvercle à l'aide de l'outil fourni.	
Disque dur / stockage de données SSD : (non fourni)	

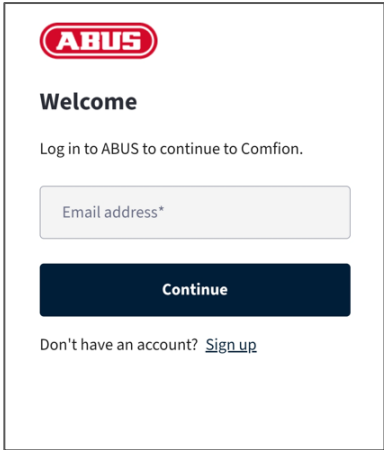
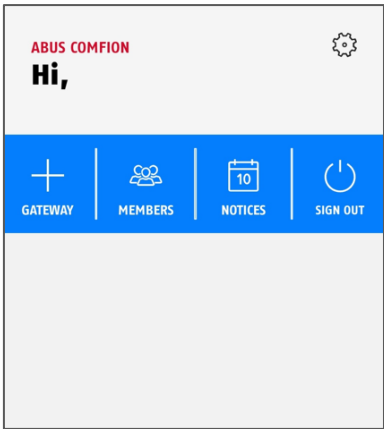
Connectez le disque dur SSD 2,5" à l'emplacement prévu. (SATA 3.0) et fixer le support de données avec les vis fournies. Antenne externe de téléphonie mobile : (non fournie) Passez le câble de raccordement par l'ouverture préparée et vissez-le sur la prise SMA. Accessoires recommandés chez ABUS : TVAC41210 - 1 To de stockage de données SSD 2,5" SATA WD Red TVAC41220 - 2 To de stockage de données SSD 2,5" SATA WD Red FUZU85000 - Antenne externe de téléphonie mobile pour Comfion Pro  Remarque Formatez le disque dur au format exFAT ou NTFS avant de l'insérer.  Remarque L'emplacement pour disque dur de 2,5" permet d'utiliser des disques durs HDD et des dispositifs de stockage de données SSD. Les exigences de la norme EN 50131 (durée de l'alimentation de secours) sont remplies en cas d'utilisation d'une mémoire de données SSD.	
Fixez le couvercle jusqu'à ce qu'il s'enclenche de manière audible et fixez les vis à l'arrière.	
Montage mural & câblage	
Desserrez la vis de fixation (en bas au milieu) et retirez la plaque arrière du boîtier de la centrale.	
 Attention : Veillez à ce que l'alimentation électrique (câble d'alimentation) soit coupée et isolée ! 1. Faites passer tous les câbles de raccordement nécessaires par le passe-câbles de la plaque de montage de la centrale. 2. Fixez ensuite la plaque de montage au mur.	

Accrochez les fusibles de maintien de la centrale (2 câbles de maintien) dans les dispositifs de la plaque arrière.							
Introduisez les câbles de raccordement dans la centrale • Raccordez le câble d'alimentation à la borne L/N. • Connectez le câble Ethernet à la prise RJ45 • Le cas échéant, connectez le câble de bus ainsi que les détecteurs câblés, etc. aux bornes correspondantes. • Vous trouverez de plus amples détails sur le raccordement des détecteurs câblés et des appareils de bus aux chapitres 3.2.5 et 3.2.6. Fixez tous les câbles de raccordement avec les serre-câbles.							
Le cas échéant, insérez une carte micro-SD (capacité max. 512 Go) et/ou une carte SIM (nano-SIM) dans les emplacements prévus à cet effet jusqu'à ce qu'elles s'enclenchent de manière audible. (Cartes non fournies)  Remarque Formatez votre carte SD au format exFAT ou NTFS avant de l'insérer.							
Activez maintenant l'alimentation électrique. La centrale exécute maintenant le processus de démarrage.							
Mettez l'interrupteur de batterie sur « ON ». Une fois le processus de démarrage terminé, les LED d'état s'allument comme suit : <table border="0"> <tr> <td></td> <td>LED d'alimentation : Vert (tension du réseau)</td> </tr> <tr> <td></td> <td>LED Internet : Vert (clignoter) (En ligne & Admin non enregistré)</td> </tr> <tr> <td></td> <td>LED de réseau : Vert (LAN)</td> </tr> </table>		LED d'alimentation : Vert (tension du réseau)		LED Internet : Vert (clignoter) (En ligne & Admin non enregistré)		LED de réseau : Vert (LAN)	
	LED d'alimentation : Vert (tension du réseau)						
	LED Internet : Vert (clignoter) (En ligne & Admin non enregistré)						
	LED de réseau : Vert (LAN)						

4.2. Mise en service du système

4.2.1. Installation via l'application & fin des préparatifs matériels

 Remarque	La première mise en service de la centrale Comfion Pro et donc le lien avec le portail du partenaire spécialisé et l'installateur correspondant doit se faire via l'application.
---	--

Téléchargez l'application Comfion sur votre smartphone ou tablette (IOS ou Android) à partir de votre App-Store Suivez les instructions dans l'application jusqu'à ce que vous arriviez à la page de connexion	
Connectez-vous avec vos données ABUS Single Sign-On (accès partenaire) Si vous n'avez pas d'accès, créez un compte gratuit sous « S'inscrire ».	
Après vous être connecté, vous verrez l'aperçu des centrales. Ajoutez une nouvelle centrale en cliquant sur le bouton « plus ».	

Sélectionnez, si vous mettez l'installation en service pour un client, « **Je suis un installateur** ». Votre utilisateur sera ainsi créé dans le rôle d'installateur.

Si vous installez l'installation pour vous-même, sélectionnez « **Je suis un utilisateur** ». Vous êtes ainsi créé en tant que rôle Admin avec des droits d'installateur & d'administrateur.

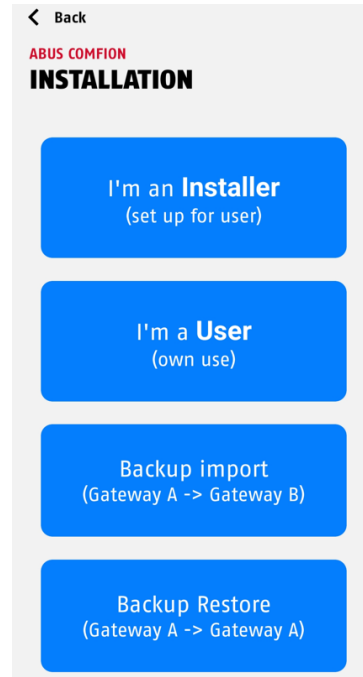


Remarque

En tant qu'installateur, vous pouvez créer des utilisateurs, mais vous perdez cette autorisation en invitant un utilisateur admin (propriétaire).

Vous trouverez plus de détails au **chapitre 4.1.** (rôles des utilisateurs) et **chapitre 4.2** (Mise en service)

Vous trouverez plus de détails sur l'« importation de sauvegarde » et la « restauration » dans le **chapitre 6.1.7** (Sauvegarde)



Remarque

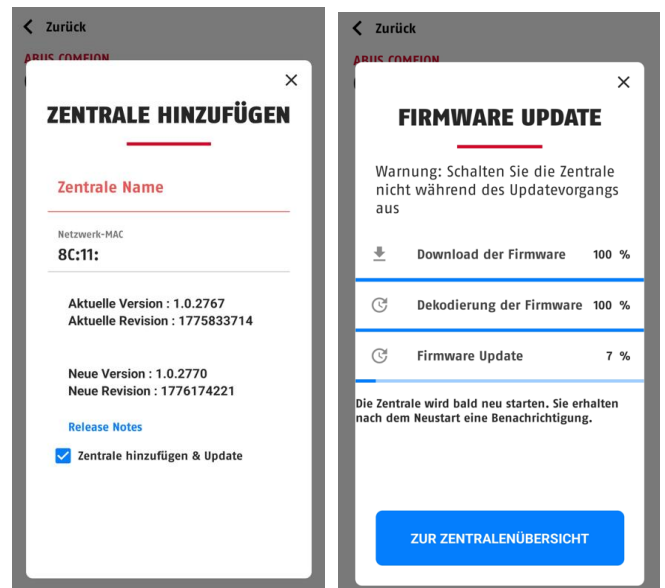
Veillez à ce que la centrale soit connectée à Internet.

Dès que la LED d'état « Internet » clignote en vert, vous pouvez lancer le processus d'appairage dans l'application.

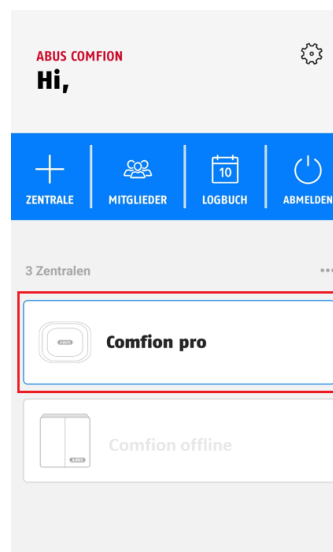
Pour ce faire, scannez le code QR portant l'inscription « Pairing-Code ».



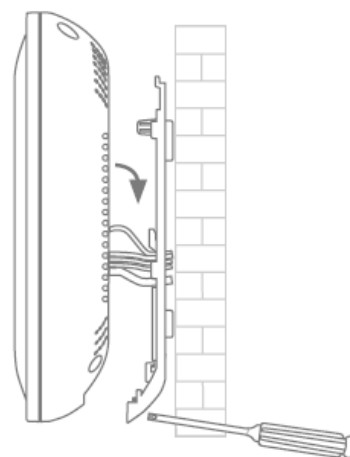
Attribuez un nom de centrale et confirmez-le. L'installation va alors lancer une mise à jour du firmware avant que vous ne puissiez y accéder. La mise à jour du firmware peut prendre quelques minutes et implique un redémarrage de la centrale. Pendant la mise à jour, la LED d'alimentation clignote en jaune.



Après le redémarrage de la centrale, celle-ci n'est plus grisée dans l'aperçu des centrales et peut être appelée en cliquant dessus.



Détachez la sécurité de maintien de la plaque arrière et placez les câbles de maintien à l'intérieur. Insérez la centrale dans la plaque arrière, faites-la glisser vers le bas et vissez la centrale sur la plaque arrière.



Remarque

Après l'installation et la mise en service, le retrait de la centrale de son support mural, ainsi que l'ouverture du couvercle du boîtier, déclenchent une alarme anti-sabotage. N'effectuez les travaux nécessaires sur le matériel que si le mode de maintenance est activé (*Configuration de la centrale -> Paramètres de sécurité*)

4.2.2. Tableau de bord (après la première connexion)

Barre de tête :

- Configuration & paramètres utilisateur
- Installateur** Rôle de l'utilisateur (installateur uniquement)
- Mise à jour du firmware (si disponible)
- Déclencher l'alarme de panique

Tableau de bord / Domaine fonctionnel

- Touches de raccourci clavier (si configurées)
- Aperçus de la caméra (si configurés)
- Aperçu des partitions (l'intérieur, l'extérieur est pré-réglé & peut être étendu à d'autres partitions, voir : 3.2.3 Partitions)
 - Un clic sur permet d'afficher les composants attribués et leur statut (si configuré)

Barre de navigation

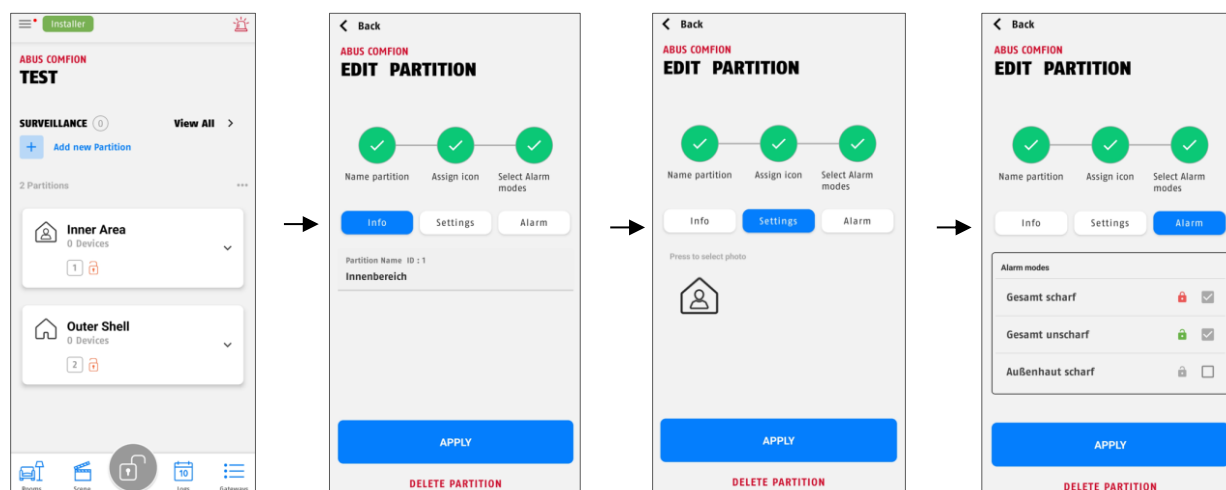
- Pièces (& liste des composants) voir 3.2.4 et 3.2.5
- Scénarios (scènes et automatisations) voir 6.4
- Modes d'alarme (symbole du cadenas) - voir 3.2.8
- Journal de bord (liste d'événements & fonction de filtrage)
- Centrales (aperçu) - voir 6.3

Vous trouverez une vue du tableau de bord déjà configurée au chapitre 6.2 Tableau de bord

4.2.3. Partitions

Les partitions vous donnent la possibilité de diviser l'objet à surveiller et donc de l'armer ou de le désarmer de manière différenciée. En interaction avec les modes d'alarme, vous pouvez commuter des partitions ensemble ou séparément.

A l'état d'usine, l'installation dispose de deux partitions - l'enveloppe extérieure et l'intérieur. Vous pouvez modifier ces partitions en appuyant longuement dessus.

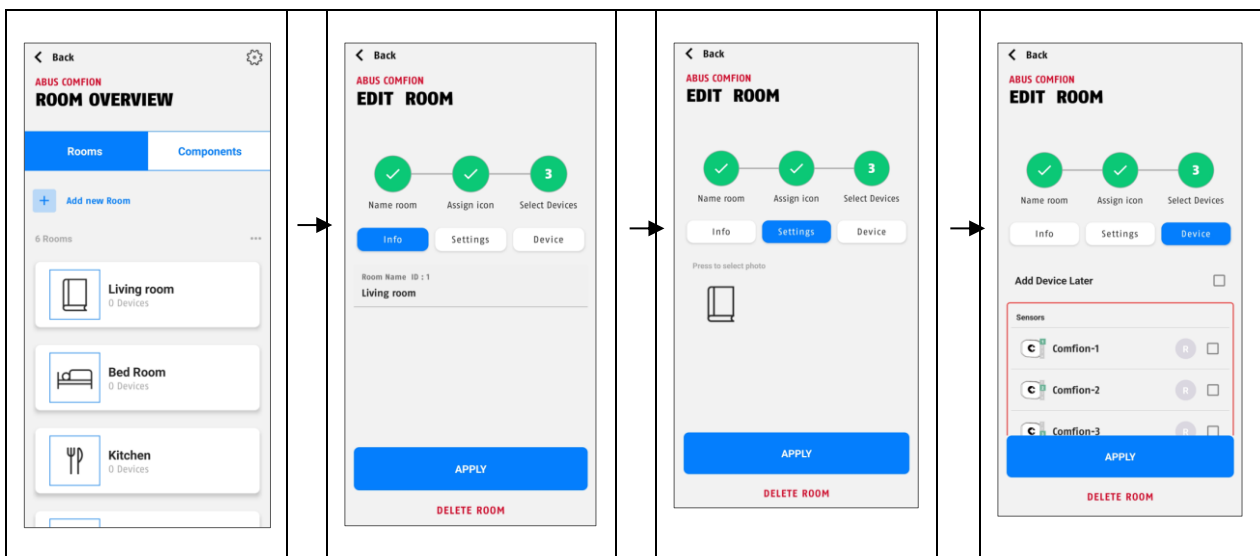


En cliquant sur le bouton « Ajouter une partition », vous pouvez créer d'autres partitions.

4.2.4. Pièces

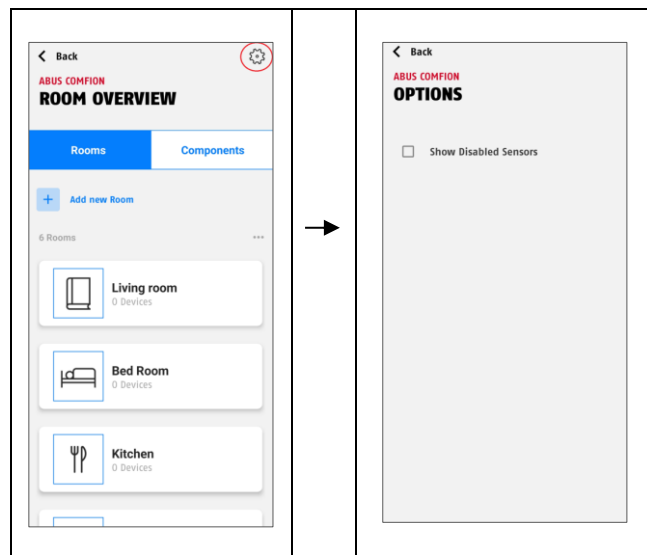
Depuis le tableau de bord, la barre de navigation vous permet d'accéder à la partition « Pièces » pour la configuration des pièces et des composants. Le système de sécurité sans fil Comfion Pro vous permet d'attribuer vos composants à des pièces. Cela sert à faciliter l'identification des composants et n'a pas de propriétés fonctionnelles. Les pièces ne sont pas affectées à des partitions, ce qui signifie que vous pouvez avoir des composants de différentes partitions dans une pièce.

A l'état d'usine, l'installation dispose de quelques pièces prédéfinies. Vous pouvez modifier librement ces espaces ou les supprimer complètement. Vous pouvez modifier cette partition en appuyant longuement dessus.



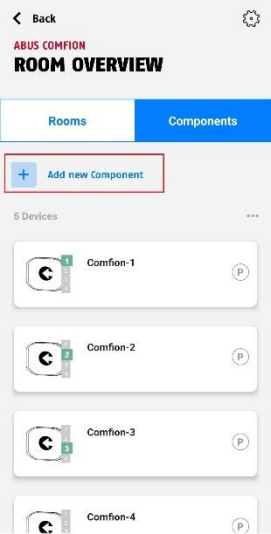
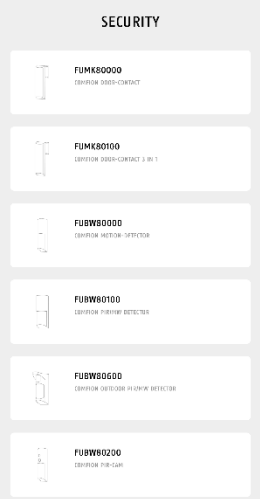
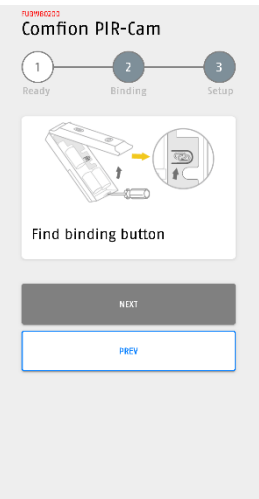
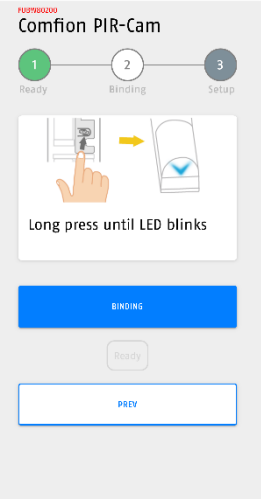
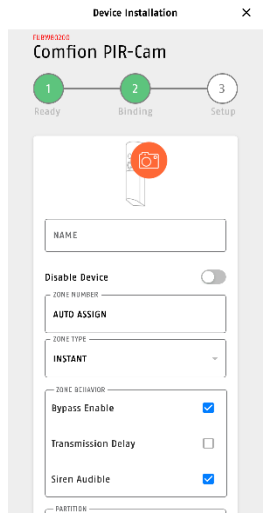
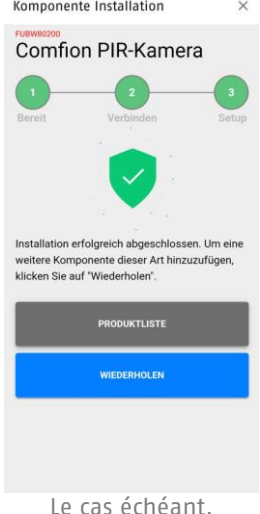
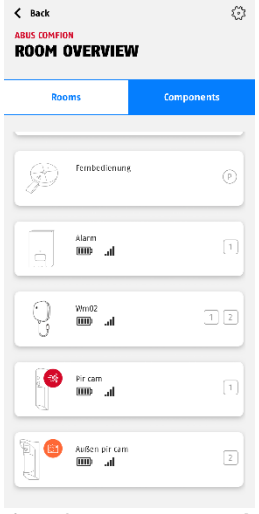
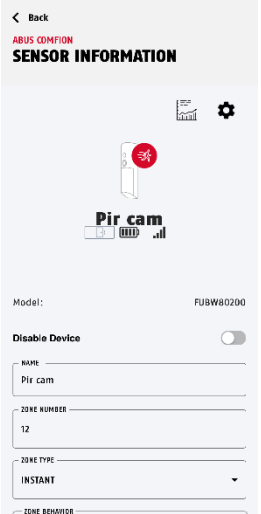
Dans l'aperçu de la pièce, le symbole de la roue dentée en haut à droite de l'écran permet d'activer ou de désactiver le paramètre « Afficher les composants désactivés ». (désactivé est pré-réglé)

Lorsque cette option est activée, les composants désactivés sont affichés dans le tableau de bord sous les pièces et dans la liste des composants.



4.2.5. Composants

De la vue d'ensemble de la pièce, vous accédez à la vue des composants. En cliquant sur « Nouveau composant », vous pouvez ajouter vos composants Comfion au système.

 Sélectionner « Nouveau composant » →	 Sélectionner un appareil dans la liste →	 Suivre le dialogue Cliquez sur « Suivant » →	 Appuyer sur la touche d'apprentissage & « Connecter » →
 Réglages de l'appareil + « Enregistrer » →	 Le cas échéant, programmer d'autres appareils →	 Liste des composants →	 Vue détaillée & paramètres.

En cliquant sur un composant déjà appris, vous pouvez l'éditer et adapter les paramètres suivants de l'appareil :

Désactiver le composant	OFF : (réglage par défaut) : Appareil en fonctionnement normal ON : L'appareil est désactivé (pas de fonction)
Nom	Attribution d'un nom au composant
Numéro de zone	Attribution d'un numéro de zone (effectuée automatiquement par le système)
Type de zone	- Entrée -> déclenche une temporisation d'entrée, une alarme d'intrusion est déclenchée une fois la temporisation écoulée - Sortie -> peut être ouverte pendant la temporisation de sortie, fonctionne comme une zone immédiate après armement - Entrée/Sortie -> utilise une temporisation de sortie & d'entrée - Entrée suivante -> le détecteur réagit comme une zone immédiate, sauf si une temporisation d'entrée a été déclenchée avant. Cela peut être limité à la même partition dans les paramètres de sécurité.

	• Immédiat (intrusion) -> <i>déclenche une alarme d'intrusion en cas d'installation armée</i> • Alerte périmétrique -> <i>type de zone pour détecteur extérieur. Déclenche l'événement, y compris l'inscription au journal et la notification. Pas d'alarme sonore.</i> • Immédiat (Surveillé) -> <i>fonctionne comme la zone immédiate en cas d'installation armée ; en cas d'installation désarmée, une notification est envoyée en cas de déclenchement</i> • Alarme d'intrusion 24 heures sur 24 -> <i>alarme d'intrusion indépendante de l'état de l'installation</i> • Alarme dégâts des eaux 24h/24 -> <i>alarme dégâts des eaux indépendante de l'état de l'installation</i> • Feu 24h/24 -> <i>alarme incendie indépendante de l'état de l'installation</i> • 24 heures de sabotage -> <i>alarme de sabotage indépendante de l'état de l'installation</i> • Surveillance de fermeture -> <i>la zone ouverte empêche l'armement, mais ne déclenche pas d'alarme</i>
Heure d'entrée/heure de sortie	• Pour le type de zone entrée, sortie et entrée/sortie, il est possible de régler un délai en secondes (de 5 à 180 secondes) • Préréglage 10 s (temporisation d'entrée) / 30 s (temporisation de sortie)
Comportement de la zone	• Peut être masqué : <i>Si la zone est déclenchée lors de l'armement, vous avez la possibilité de la masquer</i> • Délai de transmission : <i>Si ce point est activé, la notification des alarmes de zone est retardée de la durée programmée.</i> • Déclenchement de la sirène : <i>Ce détecteur commande les sirènes intégrées à la partition</i>
Partition	• L'appareil peut être attribué à une ou plusieurs partitions. -> Cette affectation, associée au type de zone, provoque le déclenchement d'une alarme.
Pièce	• L'appareil peut être attribué à une pièce. • « Attribuer plus tard » signifie que l'appareil n'a pas été attribué à une pièce.
Démarrer le test de détection (détecteur de mouvement)	• Cliquer sur « Démarrer le test de détection » démarre une fenêtre de temps de 1:00 minute dans laquelle l'appareil doit être déclenché. • Le test de détection peut être interrompu en cliquant sur « Stop ». • En cas de déclenchement, la fenêtre de temps (temps de silence du détecteur) redémarre. • Dans le cas de capteurs multiples (par ex. PIR + micro-ondes), les capteurs peuvent être testés séparément ou ensemble.
Démarrer le test de la force du signal (Composants radio)	 Testez la force du signal avant de monter le composant et utilisez un répéteur en cas de doute. Vous trouverez un aperçu de l'évaluation de la force du signal au chapitre 6.11 Remarque • Cliquez sur « Démarrer le test de la force du signal » et déclenchez l'appareil. • En cas de capteurs multiples (par ex. PIR + micro-ondes), chaque capteur peut être testé séparément.
Fonctions de la caméra (caméras uniquement)	• MotionAlarm Désactivé/Activé (réglage par défaut Désactivé), « Activé » déclenche une alarme si la caméra a été affectée à une partition.
Enregistrer	• En cliquant sur « Enregistrer », vous acceptez les modifications apportées aux paramètres.

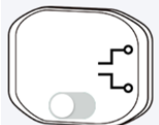
 Remarque	Si un détecteur est programmé sur le type de zone sortie ou entrée/sortie, l'installation ne vérifie l'état du détecteur lors de l'armement qu'après l'expiration du délai de temporisation. - Si le détecteur n'est pas prêt à la fin du délai et que « Masquable » est activé, le détecteur est automatiquement masqué après le délai et le système est armé. - Si le détecteur n'est pas prêt à la fin du délai et si « Masquable » est désactivé, le système ne s'arme pas.
---	---

 Remarque	Vous trouverez un aperçu détaillé des symboles de la liste des composants au chapitre 6.7 (explication des symboles)
---	--

4.2.6. Paramètres des composants

Dans les réglages des composants à droite au-dessus de l'icône de l'appareil, il est possible d'effectuer des réglages détaillés sur le composant en cliquant sur la roue dentée . Pour plus de détails, consultez le guide d'installation du composant concerné. Vous trouverez ci-dessous les réglages pour la centrale Comfion Pro FUAA85000, le module Comfion Pro BUS-WLX BUM080000 et les caméras IP

Centrale Comfion Pro FUAA85000

Symbole	Désignation	Possibilité de réglage	Explication
 (par entrée, c.-à-d. 1, 2, 3, 4)	Mode filaire	2 fils CC / EOL / DEOL (réglage par défaut CC)	Type de câblage des entrées de groupes de détecteurs
	NC ou NO	Normalement ouvert / Normalement fermé (Par défaut : NO)	État de repos du relais, c'est-à-dire ouvert ou fermé
	Présentation du logo	Toujours éteint / toujours allumé / s'allumer (Par défaut : On)	Allume, éteint l'éclairage du logo de manière permanente, ou en cas de changement d'état, allumé pendant 10 secondes (s'allume)
	Couleur Armé Couleur Désarmé Couleur Partiellement armé	Matrice couleur	Adaptation de la couleur d'éclairage en cliquant sur le symbole de couleur

Module Comfion Pro WLX Pro BUM080000 et moyens de fermeture WLX Pro

Symbole	Désignation	Possibilité de réglage	Explication
 (module BUS-WLX)	Rétablir les paramètres d'usine	Exécuter	Réinitialisation du module radio WLX-Pro. Remarque : tous les cylindres de serrure et lecteurs muraux doivent ensuite être reprogrammés ! (le module BUS-WLX reste programmé !)
 Cylindre de fermeture (Accès / Intrusion)	Temps de supervision	4 - 720 min (Par défaut : 720)	Vérification régulière de la communication radio selon l'intervalle défini.
	Caractère obligatoire (accès uniquement)	Arrêt / Marche (Par défaut : On)	Lorsqu'il est réglé sur « On », aucun accès n'est autorisé lorsque le Comfion Pro est armé.
	Heure d'ouverture	6 sec / 12 sec (Par défaut : 6 sec)	Définit la période couplée du cylindre pour l'ouverture du ferme-porte
 Lecteur mural (Accès / Intrusion)	Temps de supervision	4 - 720 min (Par défaut : 720)	Vérification régulière de la communication radio selon l'intervalle défini.
	Caractère obligatoire (accès uniquement)	Arrêt / Marche (Par défaut : On)	Lorsqu'il est réglé sur « On », aucun accès n'est autorisé lorsque le Comfion Pro est armé.
	Heure d'ouverture	6 sec / 12 sec (Par défaut : 6 sec)	Définit la période couplée du cylindre pour l'ouverture du ferme-porte

Caméras IP

Symbole	Désignation	Possibilité de réglage	Explication
 (caméra IP)	Fonction de la caméra « Alarme de mouvement »	Arrêt/marche (Par défaut : Arrêt)	Utiliser la détection de mouvement pour déclencher l'alarme. Remarque : D'autres réglages sont nécessaires, entre autres dans la configuration de la caméra. Voir chapitre 3.4.4

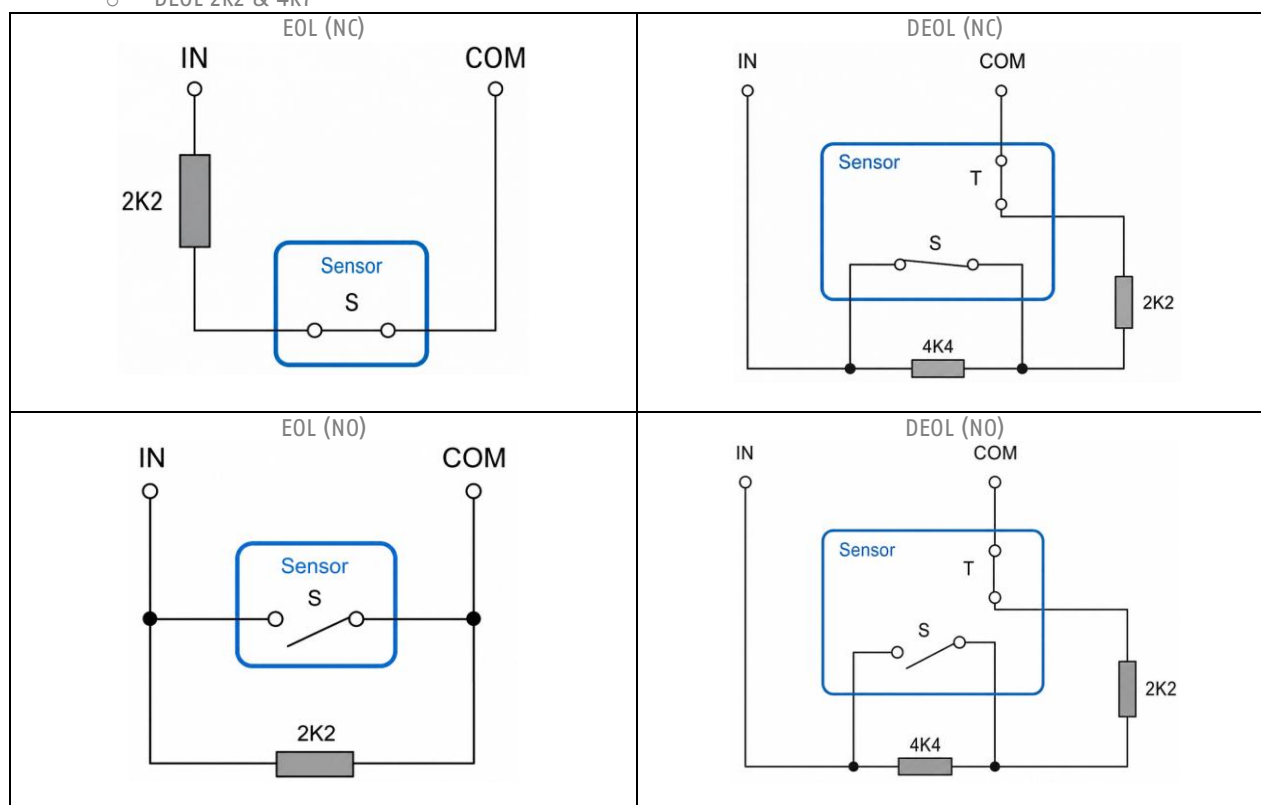
4.2.7. Remarques sur le câblage (entrées/sorties/BUS)



La centrale Comfion Pro dispose de plusieurs possibilités de raccordement pour jusqu'à 4 détecteurs câblés (8), une sortie relais (9) et une interface RS485 BUS (10).

Entrées de détecteurs filaires

- Utilisez les câbles adaptateurs de 30 cm fournis avec des extrémités de câble ouvertes. Les paires de câbles sont marquées en couleur pour chaque entrée.
- Dans les réglages de l'appareil de l'appli Comfion, vous réglez pour chaque entrée le mode filaire (2 fils CC, EOL ou DEOL) ainsi que la position de repos NO ou NC.
- Les valeurs de résistance suivantes sont prédéfinies pour le câblage de résistance surveillé :
 - EOL : 2k2
 - DEOL 2k2 & 4k7



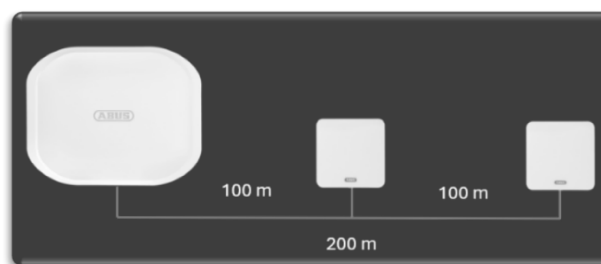
Sortie relais

- La sortie relais est hors tension. Raccordez la sortie à la masse et, selon les besoins, à la borne NC (contact à ouverture) ou NO (contact à fermeture). max. 30 V CC & max. 1,6 A

Interface BUS RS485

- Le Comfion Pro possède une interface de BUS RS485 à 4 fils (GND / +V / B / A), 13,0 V pour connecter jusqu'à 2 participants au BUS (**module Comfion Pro BUS-WLX BUM080000**)
- Vous pouvez connecter des appareils en série ou en parallèle au port de la centrale Comfion Pro.
- La longueur maximale de câble est de 200 m et peut être divisée de manière flexible en cas d'utilisation de deux appareils :

- Exemple :



- Recommandation de câble : Câble à paire torsadée (blindé et torsadé), par ex : Câble RS485/DMX ou câble CAT5e ou CAT6.

 Important	Lors de l'installation de la centrale Comfion Pro et du module BUS-WLX ainsi que d'autres appareils électriques, antennes et métaux, respectez une distance minimale de 1,5 mètre afin d'éviter tout défaut dans la communication radio (par ex. retards ou perte de signal) !
---	---

4.2.8. Modes d'alarme

Le système de sécurité sans fil Comfion Pro fonctionne avec ce que l'on appelle des « modes d'alarme », qui constituent le cœur du système. Il s'agit de liens entre partitions et utilisateurs pouvant être armés ou désarmés.

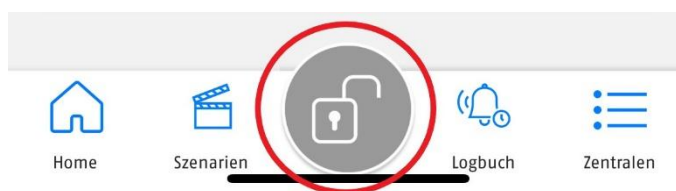
Dans un mode d'alarme, vous définissez quel utilisateur armera ou désarmera quelle partition avec celui-ci. Cela permet de reproduire tous les scénarios possibles d'armement et de désarmement.

Dans la pratique, lorsqu'un utilisateur arme ou désarme un système, il exécute en réalité un mode d'alarme.

 Remarque	Le système de sécurité sans fil Comfion Pro possède trois modes d'alarme préconfigurés en usine : « Entièrement armé », « Enveloppe extérieure armée » et « Entièrement désarmé ».
--	---

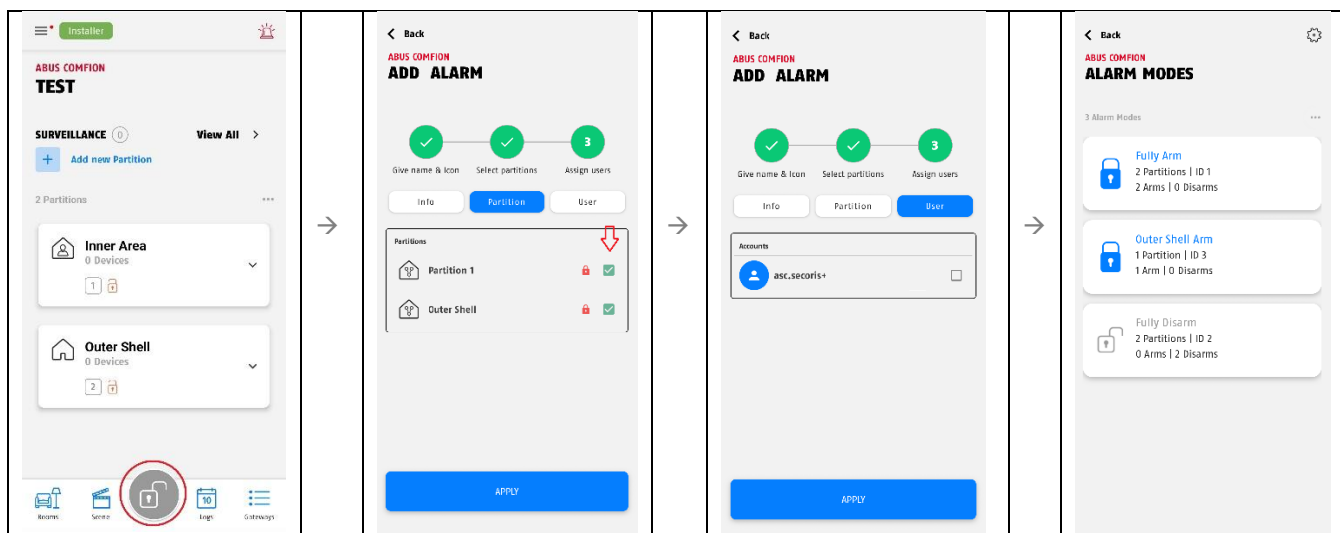
Exécution d'un mode d'alarme

- Le bouton central en bas de l'écran indique l'état actuel de l'installation (armé, désarmé, partiellement armé ou mode de maintenance)
- En appuyant sur le bouton, les modes d'alarme existants s'affichent et vous pouvez exécuter l'un des ordres de commutation qui y sont indiqués.



Créer ou modifier des modes d'alarme

1. Vous ouvrez la gestion des modes d'alarme en cliquant sur le bouton Statut dans le tableau de bord, puis sur l'icône de réglage (roue dentée) dans le coin supérieur droit de l'écran.
2. Cliquez ensuite sur « Ajouter un mode d'alarme » ou modifiez un mode d'alarme existant en appuyant longuement dessus.
3. Après avoir attribué un nom au mode d'alarme, sélectionnez les partitions ET le type d'armement/désarmement. Pour changer le type de circuit, cliquer sur le symbole.
4. Dans l'étape suivante, sélectionnez les utilisateurs qui doivent avoir l'autorisation d'activer ce mode d'alarme.
5. Une fois terminé, le mode d'alarme apparaît dans votre aperçu et peut être utilisé.



4.3. Installation et programmation de WLX Pro

Effectuer le montage et le câblage du **module Comfion Pro BUS-WLX** comme décrit dans le manuel du produit et au **chapitre 3.2.7**.

 Remarque	Pour l'installation et la configuration du module Comfion Pro BUS-WLX et d'autres moyens de fermeture WLX Pro, vous avez besoin de la carte système et de la carte de réinitialisation fournies. Conservez ces cartes avec soin !
---	--

- Programmez le module Comfion Pro BUS-WLX comme « nouveau composant » dans le système. Procédez comme décrit au **chapitre 3.2.5** et suivez les instructions de programmation.
- Programmez ensuite le cylindre de serrure WLX Pro ou le lecteur mural WLX Pro.
- Lors de la procédure d'apprentissage (étape 2), vous êtes invité à attribuer le cylindre de serrure WLX Pro ou le lecteur mural WLX Pro à un module Comfion Pro BUS-WLX. Sélectionnez le module qui est placé le plus près du cylindre/lecteur mural.

 Remarque	Après la programmation du premier cylindre de serrure ou lecteur mural, vous serez invité à programmer la carte de réinitialisation jointe. La carte de réinitialisation apprise est enregistrée de manière fixe dans le système Comfion comme support Fallback et est nécessaire pour réinitialiser un cylindre. Vous trouverez plus de détails dans le chapitre 6.1.8 Informations WLX et dans le chapitre 3.2.6 Paramètres des composants
---	---

 Important	Les appareils suivants peuvent actuellement être programmés dans le Comfion Pro : - Cylindre WLX Pro (accès/intrusion) Type : LA-A, LA-I - Lecteur mural WLX Pro (accès/intrusion) Type : WR-A-S-O, WR-I-S-O Le répéteur WLX Pro et d'autres moyens de fermeture ne sont actuellement pas pris en charge.
--	--

- Les tags RFID (tags NFC) se programment dans les réglages de l'utilisateur ou peuvent être directement effectués par le propriétaire (administrateur) après la remise. Vous trouverez plus de détails dans le **chapitre 4.4.1 Droits d'accès**.

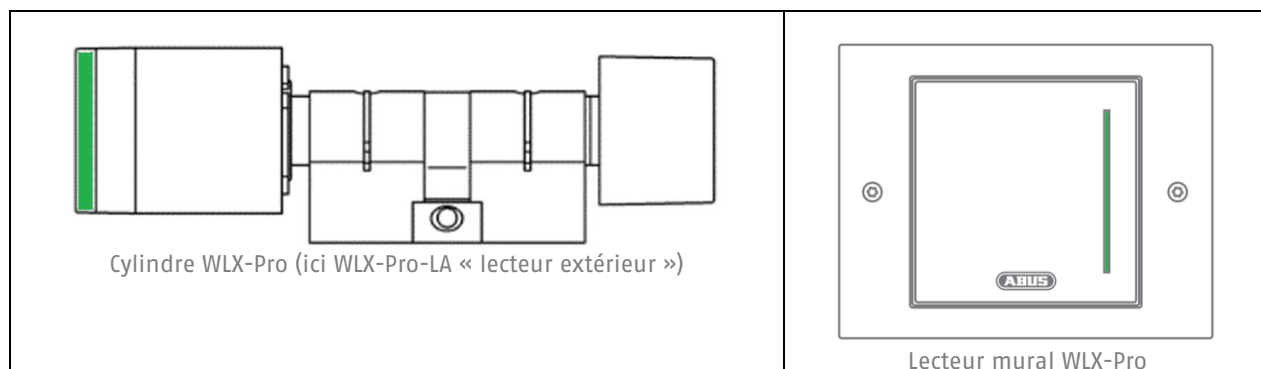
 Important	Nous recommandons d'installer au moins un tag NFC comme support Fallback afin d'autoriser l'accès aux personnes autorisées en cas d'urgence (p. ex. défaillance de la liaison radio ou panne prolongée de l'alimentation électrique). Vous trouverez plus de détails dans le chapitre 4.4.1 Droits d'accès
--	--

4.3.1. Installation, configuration et utilisation des cylindres et lecteurs muraux WLX Pro

Vous trouverez des détails sur l'installation des cylindres de serrure WLX-Pro / des lecteurs muraux WLX-Pro dans les instructions d'installation respectives des produits. Elles sont disponibles en ligne sur abus.com dans la zone de téléchargement de la page du produit :

- Cylindre de serrure WLX-Pro : <https://abus.com/products/WLX-Pro-LA>
- Lecteur mural WLX-Pro : <https://www.abus.com/products/ACSE00026>

Le cylindre de serrure WLX-Pro ainsi que le lecteur mural WLX-Pro signalent les états suivants par une séquence de clignotements de LED :



Signaux	Description
Mise en service & initialisation	
	1 x vert, 1 x rouge, 1 x vert, 1 x rouge
	1 x vert (long)
	2 x rouge
	2 x vert
Programmation/déprogrammer/réinitialiser (pendant le processus d'apprentissage (à partir de FW 2.01), le cylindre clignote cycliquement en vert)	
	2 x vert
	3 x rouge
	1 x rouge
	10 x rouge
Lors du fonctionnement	
	1 x vert
	1 x rouge
	1 x rouge (long)
	1 x vert (long)
	1 x rouge, 2x vert
	2 x vert
	3 x rouge

	3 x rouge, 2 x vert	Avertissement pile faible (jusqu'à FW 2.07)
	5 x rouge, 2 x vert	Avertissement pile faible (à partir de FW 2.09) Le cylindre se couple avec un retard d'environ une seconde
	1 x rouge, 2 x vert	Avertissement pile faible niveau 2 : pas de signalisation sur le transpondeur de personnes, le fallback peut encore autoriser l'accès 3x → Utiliser le support fallback comme en cas de panne de radio
	4 x rouge	Panne radio & transpondeur Fallback non autorisé a été présenté
	6 x rouge	- Pas d'armement possible ou - Pas de désarmement possible

4.3.2. Fonctions WLX Pro - Ouverture à distance et mode bureau

Ouverture à distance

L'ouverture à distance (également appelée libération à distance) permet de coupler le cylindre de serrure WLX-Pro pour une durée déterminée (180 secondes maximum). La configuration s'effectue dans l'application Comfion (ou interface Web) en tant que scène ou automation.

- La configuration des scènes complète une touche de raccourci clavier dans le tableau de bord de l'application Comfion
- Vous trouverez plus de détails sur la configuration au **chapitre 6.4 Automations & scènes**
- Après avoir effectué l'ouverture à distance, le bouton extérieur du cylindre de serrure WLX-Pro doit être tourné pour effectuer une ouverture.

 Remarque	Veuillez faire la différence : - La durée de la libération à distance est la période pendant laquelle le cylindre peut être couplé - Après avoir tourné le bouton extérieur, le cylindre est couplé selon la durée d'ouverture définie (6 ou 12 secondes).
---	--

 Important	L'ouverture à distance n'est possible que lorsque le Comfion Pro est désarmé.
--	---

Mode bureau (accès permanent)

Un cylindre dont le mode bureau est activé permet d'ouvrir la porte sans tag NFC en tournant le bouton du cylindre. La configuration s'effectue dans l'application Comfion (ou interface Web) en tant que scène ou automation.

- La configuration des scènes complète une touche de raccourci clavier dans le tableau de bord de l'application Comfion (vous avez besoin de 2 scènes pour activer et désactiver le mode bureau)
- La configuration de l'automation permet d'activer/désactiver le mode bureau par exemple par le biais d'un calendrier : si l'heure x → alors activer ... si l'heure Y → alors désactiver
- Vous trouverez plus de détails sur la configuration au **chapitre 6.4 Automations & scènes**
- Lorsque le mode bureau est activé, le bouton extérieur du cylindre de serrure WLX-Pro doit être tourné pour effectuer une ouverture.

 Important	L'ouverture par le mode bureau n'est possible que lorsque le Comfion Pro est désarmé. Un mode bureau activé est interrompu pendant la durée de l'armement ! Ne programmez cette fonction que si l'exploitant en connaît les conséquences et les a confirmées par écrit.
--	--

4.4. Caméras (NVR)

Grâce au protocole d'intégration ONVIF, diverses caméras de la gamme ABUS Professional Line peuvent être intégrées au système de sécurité sans fil Comfion Pro. L'intégration par RTSP est également possible. Il est possible d'intégrer jusqu'à 8 caméras dans Comfion Pro et de les faire enregistrer (sur carte micro-SD ou SSD) lors d'un événement, lorsque le système est armé ou en permanence (24h/24 et 7j/7).



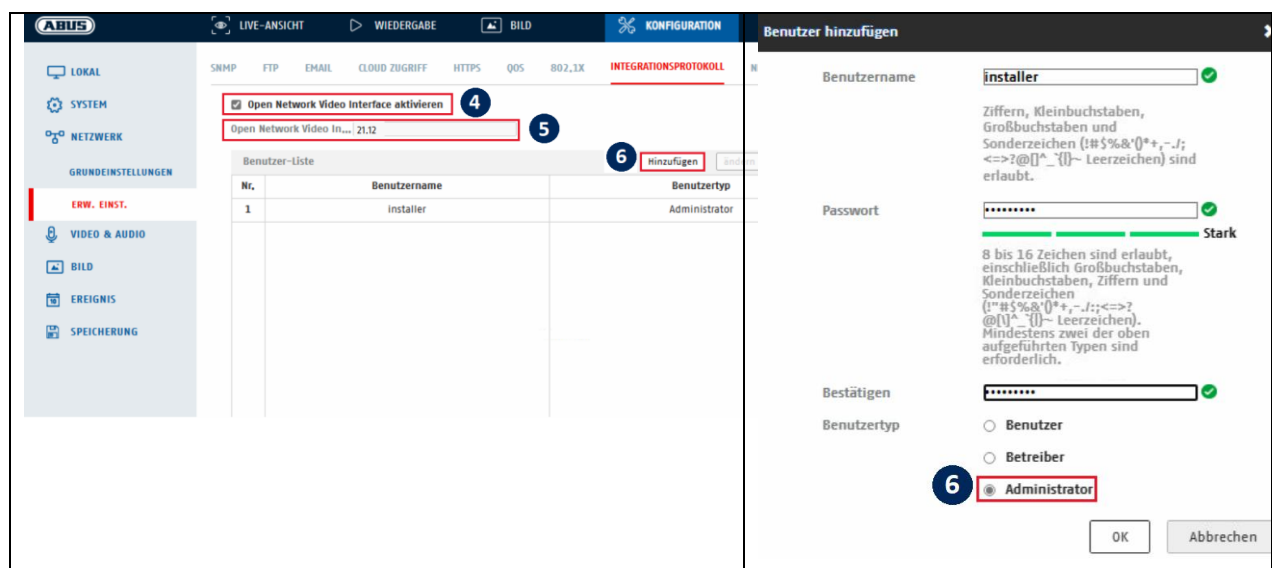
Pour l'enregistrement en continu (24h/24 et 7j/7), une mémoire de données SSD est nécessaire dans la centrale.

4.4.1. Intégration de caméras par ONVIF

Par défaut, le système Comfion Pro recherche lui-même les caméras ONVIF sur le réseau et les ajoute au système. Vous pouvez désactiver la recherche automatique de la caméra sous l'aperçu de la caméra dans les paramètres de la caméra.

Procédez comme suit pour intégrer les caméras :

1. Connectez la caméra au même réseau que le Comfion Pro.
2. Ouvrez le logiciel ABUS IP-Tool et activez la caméra.
3. Ouvrez l'interface de la caméra, connectez-vous en tant qu'installateur et ouvrez la configuration.
4. Activez ONVIF dans les paramètres réseau avancés de la caméra, sous l'onglet « Protocole d'intégration » (Open Network Video Interface)
5. Ici, vous pouvez également voir la version ONVIF de la caméra & pour Comfion Pro, 21.12 ou plus est nécessaire. (En cas de besoin, veuillez actualiser le firmware de la caméra - celui-ci est disponible sur abus.com dans la zone de téléchargement de l'article)
6. En outre, un nouvel utilisateur ONVIF doit être ajouté ici. Veuillez sélectionner ici le type d'utilisateur « Administrateur ».
7. Effectuez les réglages vidéo décrits dans le champ de remarques ci-dessous dans la caméra
8. Enregistrez les données d'utilisateur ONVIF dans le Comfion Pro. (Pour la connexion à la caméra dans l'application Comfion Pro & interface Web, sélectionnez l'utilisateur créé sous (6.).
9. Testez les fonctions de la caméra (image en direct, etc.)



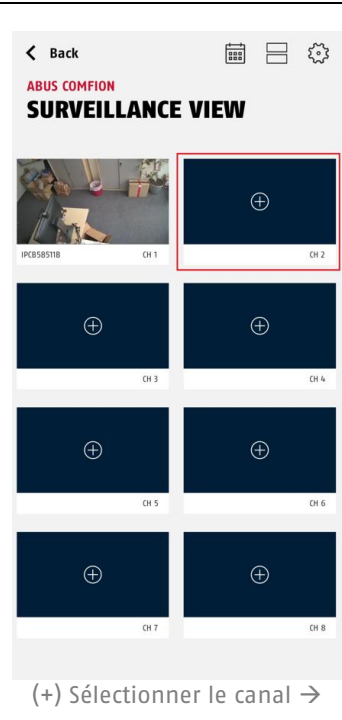
 Remarque	Les réglages de flux vidéo suivants sont recommandés en fonction du nombre de caméras connectées (canaux), afin de pouvoir garantir un flux sans perturbation même en cas d'appel et d'enregistrement en continu simultanés de 8 canaux. Flux primaire : • 1 canal : Résolution 4K ; débit binaire : 6 Mbps • 8 canaux : ➢ 4 x résolution : 4K (3840 x 2160) ; débit binaire : 2048 kbps ➢ 4 x résolution : 1080 p (1920 x 1080) ; débit binaire : 2048 kbps Flux secondaire : • 1 à 8 canaux : Résolution : 360 p ; débit binaire 512 kbps
 Remarque	• La résolution maximale de 4K (3840 x 2160) par canal ne doit pas être dépassée • Le débit binaire maximal ne doit pas dépasser 8 x 2048 kbps

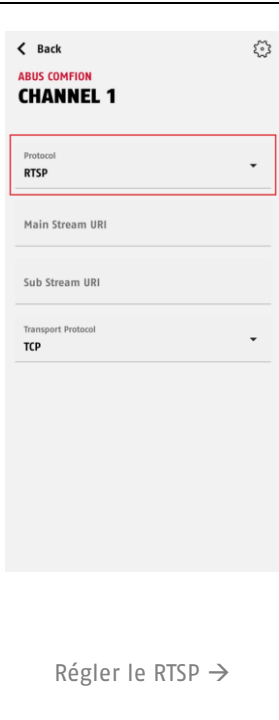
4.4.2. Intégration de caméras par RTSP

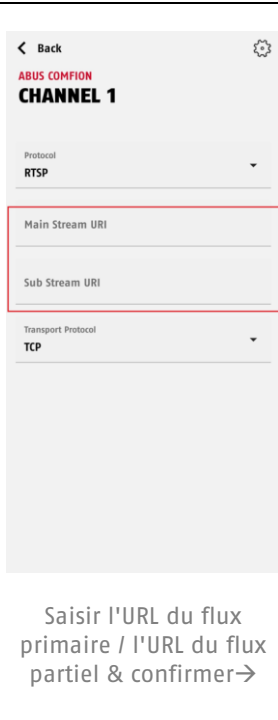
 Remarque	L'intégration via RTSP fournit le flux vidéo et audio de la caméra, mais ne permet pas de configuration plus poussée ni de commande PTZ ni de détection de mouvement.
---	--

Pour intégrer des caméras via le flux RTSP, procédez comme suit :

1. Connectez la caméra au même réseau que le Comfion Pro.
2. Ouvrez le logiciel ABUS IP-Tool et activez la caméra. Le cas échéant, créez un compte d'installateur pour la caméra.
3. Dans l'application Comfion → Aperçu des caméras, sélectionnez un canal de caméra (encore libre) (+)
4. Dans la configuration, sélectionnez RTSP sous « Protocole réseau ».
5. Insérez le flux primaire et l'URL du flux partiel. Les caméras ABUS compatibles utilisent les URL suivantes :
 - **Remarque :** Remplacez le « nom d'utilisateur » et le « mot de passe » par les données d'accès de l'étape 2
 - Flux primaire : `rtsp://nom d'utilisateur:mot de passe@192.168.0.27/ISAPI/Streaming/channels/101`
 - Flux secondaire : `rtsp://nom d'utilisateur:mot de passe@192.168.0.27/ISAPI/Streaming/channels/102`







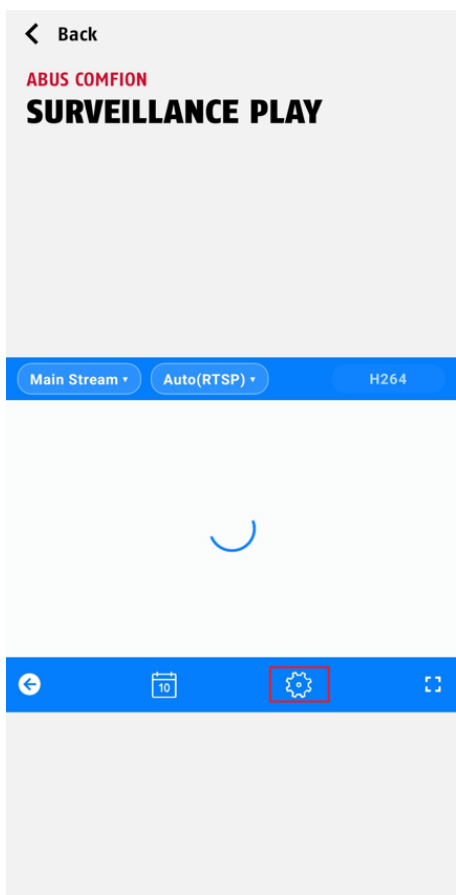
4.4.3. Paramètres de la caméra (global)

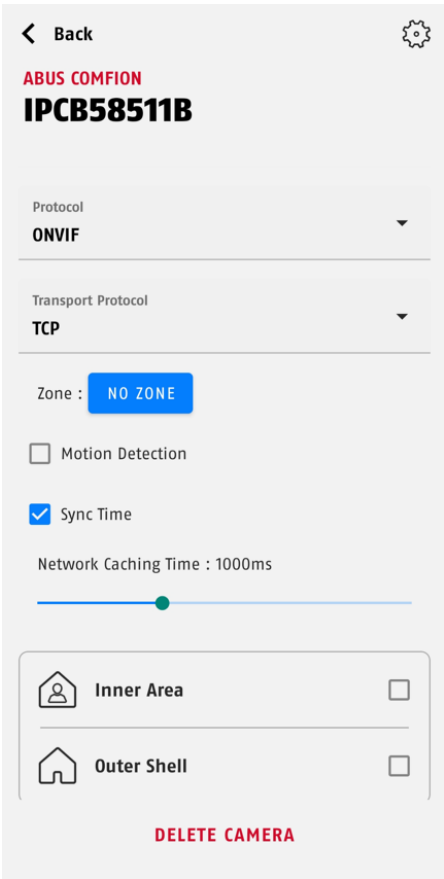
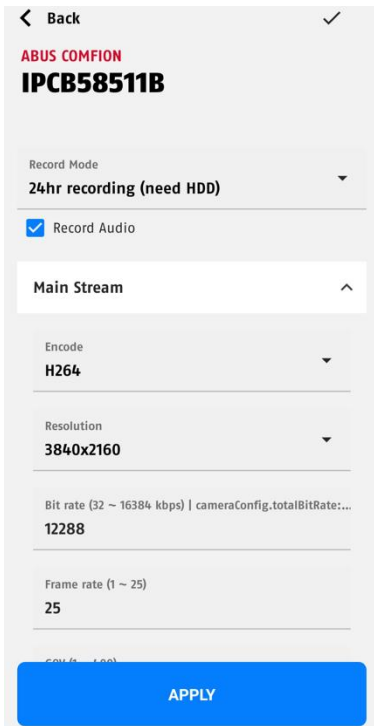
Via l'aperçu de la caméra, vous accédez aux paramètres de la caméra en cliquant sur le symbole de la roue dentée . Ils s'appliquent **de la même manière à toutes les caméras connectées**.

Recherche automatique de caméras	OFF (par défaut) / ON (aucune) Recherche automatique de caméras ONVIF sur le même réseau
Sauvegarde des données	OFF / ON & 1 - 365 jours Les enregistrements sont supprimés du support de données après l'écoulement du temps indiqué, si « ON » a été activé.
Type de flux d'enregistrement	Flux primaire (par défaut) / flux secondaire Type de flux utilisé pour l'enregistrement.

Dans l'affichage détaillé de la caméra (flux vidéo en direct), vous trouverez un autre symbole en forme de roue dentée  pour d'autres configurations **de cette caméra**. Vous trouverez plus de détails au **chapitre 3.4.4**.

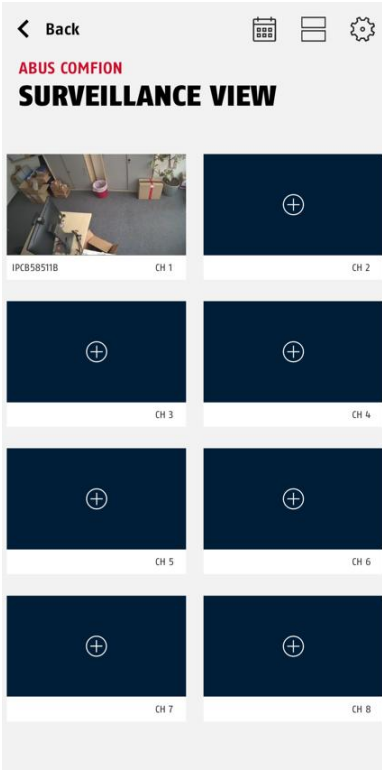
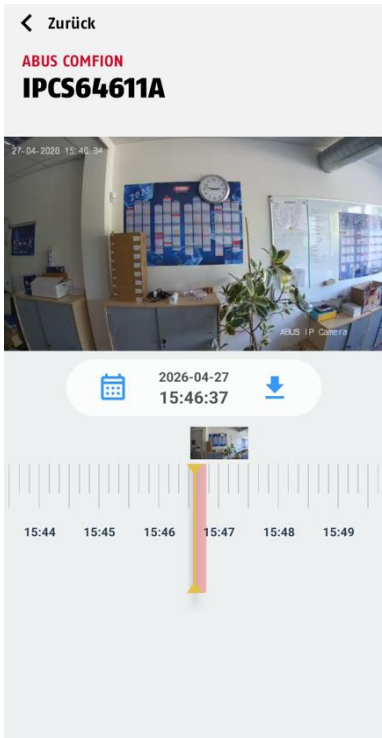
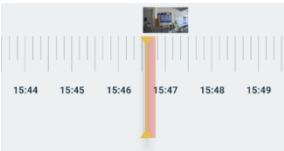
4.4.4. Paramètres de la caméra (un par un)

	Depuis l'aperçu des caméras, vous accédez au flux vidéo en direct en cliquant sur le carreau de la caméra  retour à l'aperçu des caméras Panoramique/inclinaison, haut-parleur, microphone    Pour plus de fonctions de commande & de détails, veuillez consulter le manuel d'utilisation Comfion Pro.  Événements de la caméra - voir chapitre 3.4.5 Commande du NVR pour plus de détails  Paramètres pour cette caméra  Change l'angle de vue Mode Portrait / Paysage
--	---

	Nom de la caméra, adresse IP, port, nom d'utilisateur, mot de passe, protocole réseau, protocole de transmission • Voir 3.4.1 et 3.4.2 Intégration de caméras Zone • Si la caméra a été ajoutée à une partition (ici l'intérieur), le numéro de la zone s'affiche ici. Détection de mouvement configurée • Si elle est activée, la détection de mouvement de la caméra est évaluée par le Comfion Pro et peut être programmée comme événement déclencheur dans les automatisations.  Important L'activation de cette fonction nécessite que vous l'activiez dans la configuration directe de la caméra (interface Web ou ABUS IP-TOOL).  Remarque Pour utiliser la détection de mouvement de la caméra pour déclencher l'alarme, il faut en outre activer la fonction « MotionAlarm » dans les paramètres des composants de la caméra. Heure de synchronisation • Si elle est activée, la caméra prend en charge le réglage de l'heure de la centrale Comfion Pro Temps de mise en cache du réseau • Temps de tampon du NVR Comfion Pro pour la mise en mémoire tampon des données vidéo entrantes avant l'affichage. Supprimer la caméra Supprime la caméra de l'emplacement du canal et de la liste des composants.
	Cliquez sur l'icône en forme de roue dentée dans les paramètres de la caméra (individuellement) pour régler le mode d'enregistrement : Mode enregistrement • Enregistrement en continu ○ Enregistrement 24h/24 et 7j/7 ○ Nécessite un disque dur (par ex. mémoire de données SSD) • Enregistrement uniquement lorsque le système est activé ○ Enregistrement lorsque l'installation est armée (ou partition) ○ Nécessite un disque dur (par ex. mémoire de données SSD) • Enregistrement uniquement en cas d'événement ○ En fonction du type de zone défini pour la caméra, par ex. intrusion ou périmètre ○ Nécessite une carte micro-SD ou un disque dur • Pas d'enregistrement Enregistrement audio • Enregistrement avec flux audio (si la caméra le permet)

4.4.5. Fonctionnement du NVR

L'aperçu des caméras vous permet d'accéder à la vue parallèle de tous les canaux. Vous pouvez visualiser ici l'image en direct de toutes les caméras connectées. La fonction calendrier vous permet de visualiser les enregistrements existants dans le système, triés par date.

Vue d'ensemble des caméras 	 Événements de caméra par canal de caméra (enregistrement en continu et/ou événements)   Vue des canaux de caméra en grille ou en lignes.  Paramètres de la caméra  Image d'aperçu de la caméra déjà programmée - un clic permet de passer au flux en direct de la caméra. En fonction du type de caméra, d'autres fonctions / paramètres sont possibles. (par ex. PTZ, 2WayAudio, etc.)  Canal de caméra libre. Cliquer sur « + » pour lancer le processus d'apprentissage, c'est-à-dire rechercher les caméras sur le même réseau ou les intégrer manuellement.
Événements de la caméra 	Sélectionnez d'abord le canal de caméra pour accéder à cette vue.  Recherche d'enregistrements caméra dans le calendrier (les jours avec des événements sont marqués d'un point)   Télécharger les événements de la caméra • L'heure de début est fixée dans la ligne du temps • Durée d'enregistrement réglable de 10 sec. à 30 min.  Sélection des événements de la caméra dans la ligne du temps Enregistrement de l'événement → Rouge Enregistrement en continu → Gris

5. Utilisateurs et groupes d'autorisation

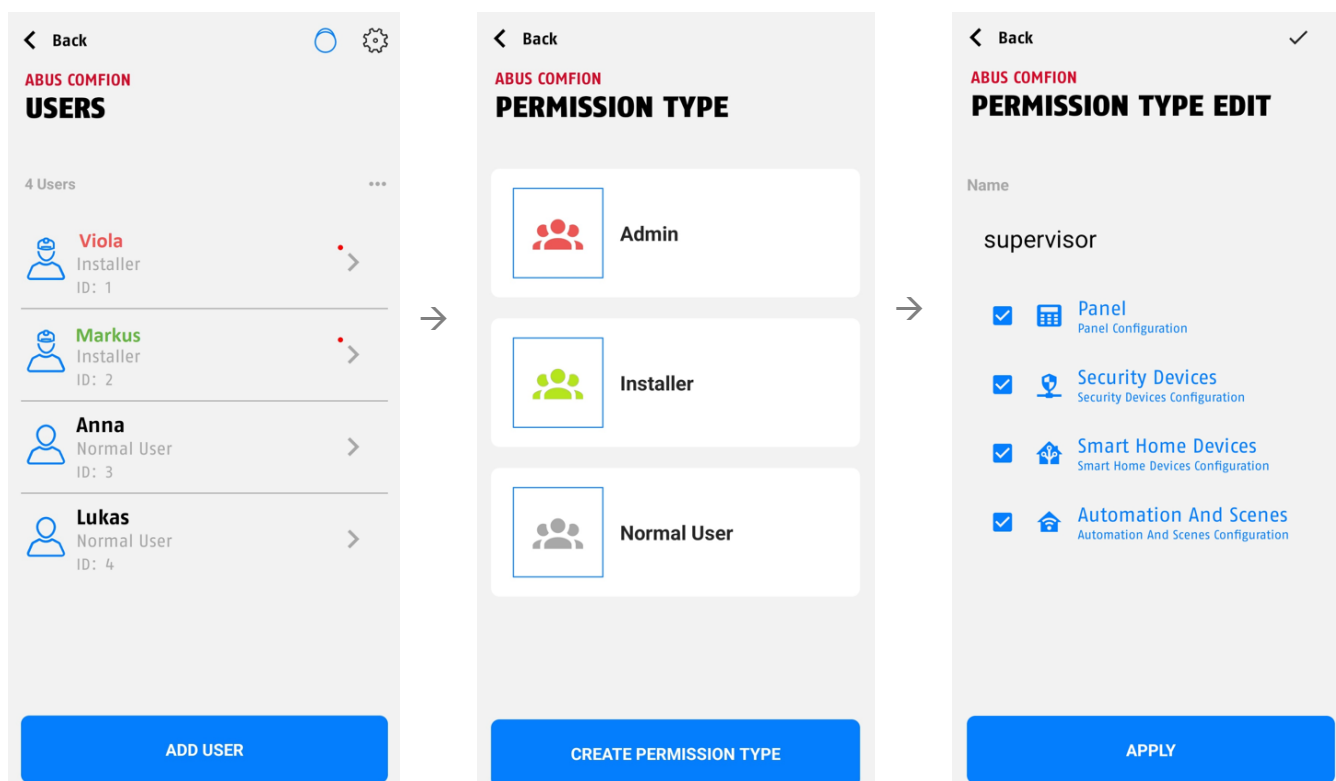
5.1. Explication des différents rôles

Installateur	L'installateur dispose de tous les droits d'utilisateur lors de la première mise en service. Après la remise de l'installation, l'installateur conserve tous les droits de configuration. Le propriétaire de l'installation peut retirer à l'installateur les droits sur l'image en direct de la caméra et lui interdire complètement l'accès à l'installation.
Admin	L'admin de l'installation dispose de tous les droits d'utilisateur pour l'installation. Si l'installateur attribue à l'admin des droits de configuration, l'admin peut obtenir les droits d'un installateur et ainsi créer et modifier des automatisations et des scènes par exemple.
Rôle propre (Personnalisé)	Vous avez la possibilité de créer vos propres groupes d'utilisateurs non administrateurs et de définir leurs autorisations (voir ci-dessous)
Propriétaire (rôle supplémentaire)	Le rôle de propriétaire est automatiquement attribué au premier admin existant sur l'installation. Le rôle de propriétaire ne peut pas être attribué manuellement. Le propriétaire de l'installation a, en plus des droits d'administrateur, le droit d'ajouter, d'inviter et de supprimer des utilisateurs. Le propriétaire de l'installation est marqué en rouge dans la liste des utilisateurs.

Les possibilités de réglage suivantes sont disponibles sous l'utilisateur installateur :

- Partager l'accès : Bloque/autorise l'accès au système et aux notifications push
- Installateur principal : Détermine le compte d'installateur avec lequel l'installation est connectée pour la télémaintenance (portail d'installateur spécialisé)

Création de groupes d'utilisateurs :



5.2. Mise en service

Dans l'état d'usine de la centrale, il existe actuellement les groupes d'autorisation « Installateur » et « Admin ». Si l'installation est mise en service par un installateur, celui-ci est autorisé au début à utiliser toutes les fonctions dans la centrale.

5.2.1. Remise au propriétaire

Une fois que vous, l'installateur, avez terminé la configuration de la centrale, l'installation doit être remise à l'utilisateur final. Le premier admin invité devient le **propriétaire de l'installation**. Vous le reconnaîtrez au fait que cet utilisateur est marqué en rouge.

Après avoir invité le propriétaire, l'installateur perd les droits de modification et d'ajout d'utilisateurs. D'autres utilisateurs doivent être ajoutés par le **propriétaire**.

5.3. Inviter/ajouter des utilisateurs

Les nouveaux utilisateurs ne peuvent être invités que par le propriétaire après le transfert. Lors de l'ajout d'un nouvel utilisateur, vous avez le choix entre les possibilités suivantes :

- Inviter un nouvel utilisateur
 - Inviter un utilisateur à partir de son adresse électronique.
- Sélection de mes membres
 - Inviter un membre. Les membres peuvent être ajoutés à la liste personnelle des membres dans l'aperçu central. (Voir **6.3.2 Membres**)
- Créer un utilisateur local
 - Création d'un utilisateur local sans compte Abus Cloud et sans utilisation d'applications. Il est possible d'attribuer à l'utilisateur local une télécommande, un code pour l'élément de commande et d'ajouter un tag/une carte NFC. Il est également possible d'enregistrer le numéro d'appel & l'e-mail pour les notifications.

En outre, il est possible de choisir l'autorisation de l'utilisateur à ajouter. On peut choisir ici entre Installateur, Admin et les groupes d'utilisateurs que l'on a créés soi-même.

5.4. Modifier les utilisateurs

Les données utilisateur se répartissent en 3 partitions, à savoir les droits d'accès, les notifications et les modes d'alarme autorisés lors du fonctionnement

5.4.1. Droits d'accès

Autorisation :

Le groupe d'autorisation (installateur, admin, utilisateur normal) peut être adapté ici pour chaque utilisateur

Code PIN :

Saisie du code PIN à 4 chiffres pour l'identification sur l'élément de commande radio Comfion

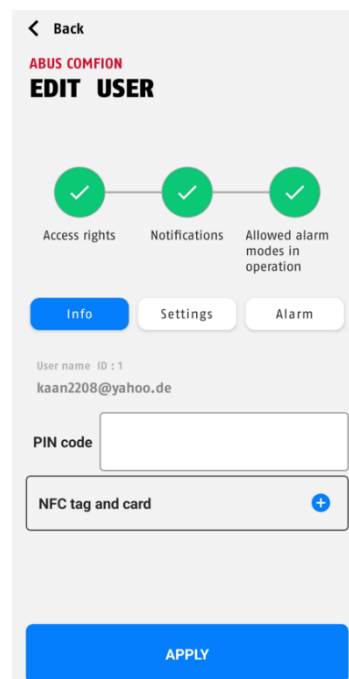
 Remarque	Chaque code à 4 chiffres ne peut être attribué qu'une seule fois. Si le même code est attribué à un deuxième utilisateur, un message d'erreur s'affiche.
---	---

Autoriser l'accès

En relation avec la saisie de l'adresse e-mail et du numéro de téléphone. Permet à cet utilisateur d'accéder

E-mail & téléphone (utilisateurs locaux uniquement)

Saisie de l'adresse e-mail et du numéro de téléphone pour recevoir des notifications par e-mail ou SMS



The screenshot shows the 'EDIT USER' screen for 'ABUS COMFION'. At the top, there's a 'Back' button. Below it, three status indicators with green checkmarks are shown: 'Access rights', 'Notifications', and 'Allowed alarm modes in operation'. There are three tabs: 'Info' (selected), 'Settings', and 'Alarm'. Under the 'Info' tab, the 'User name ID : 1' is displayed as 'kaan2208@yahoo.de'. Below this is a 'PIN code' field with a text input box. At the bottom of the input area is an 'NFC tag and card' section with a blue plus icon. A large blue 'APPLY' button is at the very bottom.

Tag NFC et carte

Jusqu'à 2 tags / cartes NFC peuvent être programmés et attribués par utilisateur.

Une pression sur « + » lance le processus de programmation

Une pression sur un média déjà appris ouvre les paramètres avec d'autres possibilités de configuration :

- Désactivé - (désactive le tag s'il est activé)
- Armement forcé - (Permet l'armement en cas de défaut)
- Support Fallback - (si activé, en cas de communication radio perturbée entre le cylindre/lecteur de mur et le module BUS-WLX, l'accès est contrôlé localement sur le cylindre/lecteur de mur).
- Nom - (désignation du tag - le nom apparaît également dans le journal de bord en cas d'événement d'accès)
- Utilisateur - (attribution à un utilisateur configuré dans le système Comfion Pro)

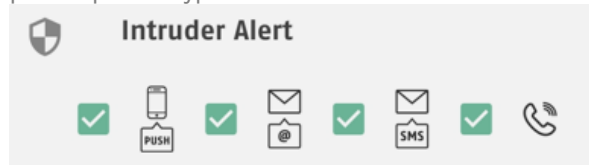
Les modifications doivent être confirmées par « Enregistrer » ou « Confirmer »

5.4.2. Notifications

Le système de sécurité Comfion Pro dispose des voies de communication suivantes : E-mail, push, SMS, appel & connexion à la station de contrôle

Sous l'option de menu « Utilisateurs → Modifier Utilisateurs → Notifications », vous pouvez choisir individuellement pour chaque utilisateur créé les notifications qui doivent être envoyées par événement.

par ex. pour le type d'événement « Alarme d'intrusion » (push/e-mail/SMS/appe)

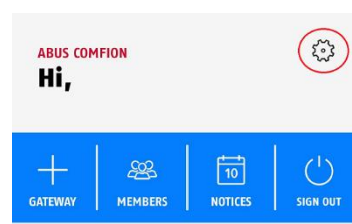
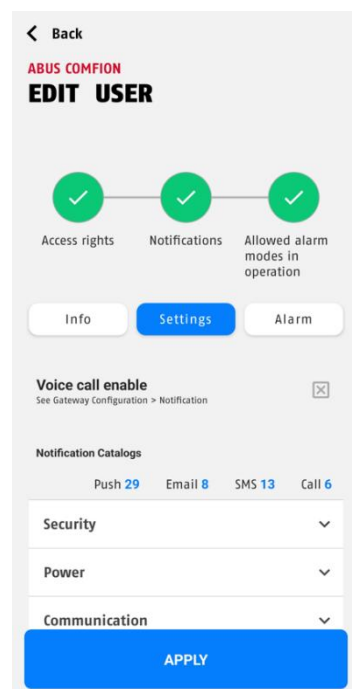


 Remarque	Certains événements sont limités à certains types de communication. Par exemple, pour certains événements, l'appel téléphonique n'est pas possible. Les notifications push ne sont disponibles que pour les utilisateurs de l'application Comfion, c'est-à-dire qu'elles ne peuvent pas être utilisées par les utilisateurs locaux.
---	---

Le numéro de téléphone pour les SMS et les appels téléphoniques, ainsi que l'adresse e-mail pour les notifications, sont enregistrés dans le compte de l'utilisateur. Vous pouvez les modifier à tout moment. Pour ce faire, allez dans votre aperçu des centrales et cliquez sur la roue dentée dans le coin supérieur droit. Vous pouvez maintenant attribuer le numéro d'appel de notification, ainsi que l'e-mail de notification.

Pour les utilisateurs locaux, la saisie de l'adresse e-mail / du numéro de téléphone s'effectue dans les paramètres utilisateur (droits d'accès).

 Remarque	Veuillez toujours saisir le numéro de téléphone avec l'indicatif du pays, par ex. +49.....
---	---

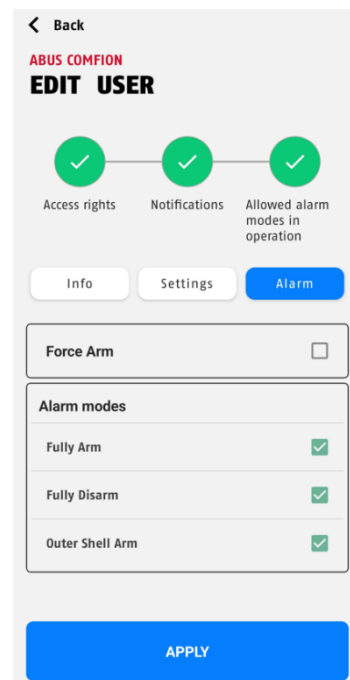


5.4.3. Modes d'alarme autorisés en fonctionnement

Vous définissez ici si l'utilisateur est autorisé à armer le système de force (dans ce cas, l'activation a lieu même si la zone est ouverte/déclenchée & sans la procédure de masquage). Vous trouverez plus de détails dans le **chapitre : 6.7.3**

En outre, vous définissez ici l'autorisation d'armement et de désarmement par partition. L'utilisateur doit posséder au moins une autorisation.

Toutes les modifications sont prises en compte en appuyant sur « Confirmer ».



5.5. Suppression d'utilisateurs

Il y a deux façons de supprimer des utilisateurs de la centrale :

1. Le propriétaire de l'installation (utilisateur marqué en rouge) peut supprimer tout autre utilisateur du système en cliquant sur celui-ci et sur le bouton « Supprimer l'utilisateur ».
2. Chaque utilisateur peut se supprimer lui-même de l'installation en cliquant longuement sur la centrale concernée dans l'aperçu des centrales et en confirmant ensuite la demande de suppression.

 Remarque	Le propriétaire de l'installation ne peut se retirer lui-même du système que par la deuxième voie (supprimer la centrale de l'aperçu des centrales). Après le retrait du propriétaire, le rôle revient à l'installateur. Celui-ci peut, en invitant un nouvel admin, le désigner comme nouveau propriétaire.
---	---

6. Communication

6.1. Module GSM

Le système de sécurité Comfion Pro dispose d'un module GSM intégré (2G/3G/4G). Il permet d'envoyer des SMS et d'effectuer des appels en cas d'alarme. Il offre également une voie de redondance pour toutes les communications du système. Cela signifie qu'en cas de panne de votre connexion Internet, toutes les communications avec le cloud, et donc l'accès à distance et les notifications push, sont effectuées via le module GSM.

 Remarque	Débloquez votre carte SIM avant de l'insérer dans le module GSM. En règle générale, vous pouvez désactiver le code PIN dans les paramètres de n'importe quel téléphone portable.
 Remarque	N'utilisez pas de cartes SIM provenant de l'étranger pour une utilisation permanente dans le Comfion Pro.

Une carte SIM est nécessaire pour le fonctionnement du mode mobile. Cette carte SIM peut être choisie librement (recommandation ABUS : Telekom, Vodafone, o2) et doit disposer des fonctionnalités que vous souhaitez utiliser sur la centrale. Si vous souhaitez utiliser toutes les fonctions, vous avez besoin d'une carte SIM avec SMS, d'un forfait voix et d'un volume de données.

 Remarque	ABUS déconseille l'utilisation de cartes prépayées dans le système de sécurité Comfion Pro pour des raisons de fiabilité. En outre, il n'est pas conseillé d'utiliser des cartes SIM multiples, car cela peut entraîner des problèmes de connexion.
 Remarque	La carte SIM doit posséder les caractéristiques suivantes, en fonction de l'utilisation prévue : • « SMS over IMS » - envoi de SMS via le réseau 4G • « Voice over LTE » - fonction d'appel via le réseau 4G

Valeur RSRP (dbm)	Signification	 Remarque
< -80	Très bon	RSRP est la puissance du signal utile (signal de référence LTE) qui arrive sur l'appareil depuis le pylône de téléphonie mobile. Le lieu d'installation peut affecter la force du signal, par exemple la distance par rapport à l'antenne de téléphonie mobile ou l'atténuation due à la structure du bâtiment. En cas de doute, nous recommandons d'utiliser une antenne externe.
-80 à -90	Bon	
-91 à -100	Moyen	
-101 à -110	Faible	
> -111	Très mauvais	

Pour l'envoi de SMS et la fonction d'appel, aucun autre réglage n'est nécessaire dans le module GSM lui-même. Si vous souhaitez bénéficier de la redondance des services réseau, il est nécessaire d'enregistrer les données APN de la carte SIM utilisée. Vous trouverez l'option de menu sous « Configuration centrale » → Roue dentée → « Module GSM ».

Si aucune carte SIM n'est insérée dans le Comfion Pro, veuillez désactiver la case « Activer ». Dans ce cas, il n'y a pas de vérification de la carte SIM ni, le cas échéant, de message d'erreur.

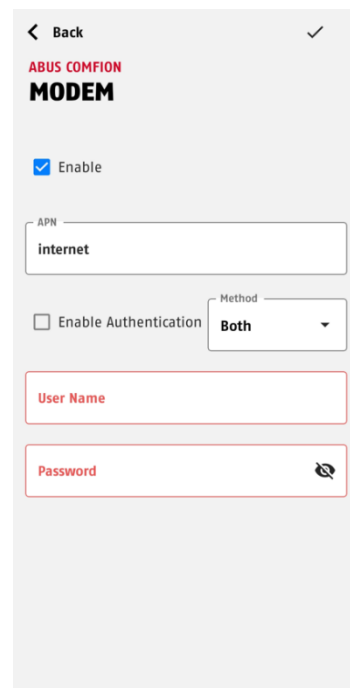
Les données APN de votre opérateur de téléphonie mobile sont jointes à votre carte SIM. Vous pouvez également les consulter en ligne. Les données ne sont pas spécifiques à la carte SIM, elles sont les mêmes pour chaque opérateur. Si le nom d'utilisateur & le mot de passe sont indiqués dans les données APN, cochez la case « Authentification ».

Exemple de Telekom :

- APN : internet.telekom
- Nom d'utilisateur : t-mobile
- Mot de passe : tm

Exemple de Vodafone :

- APN : web.vodafone.de
- Pas de nom d'utilisateur
- Pas de mot de passe



6.2. Courrier électronique

L'envoi d'e-mails de Comfion Pro fonctionne sans configuration et s'effectue via le cloud.

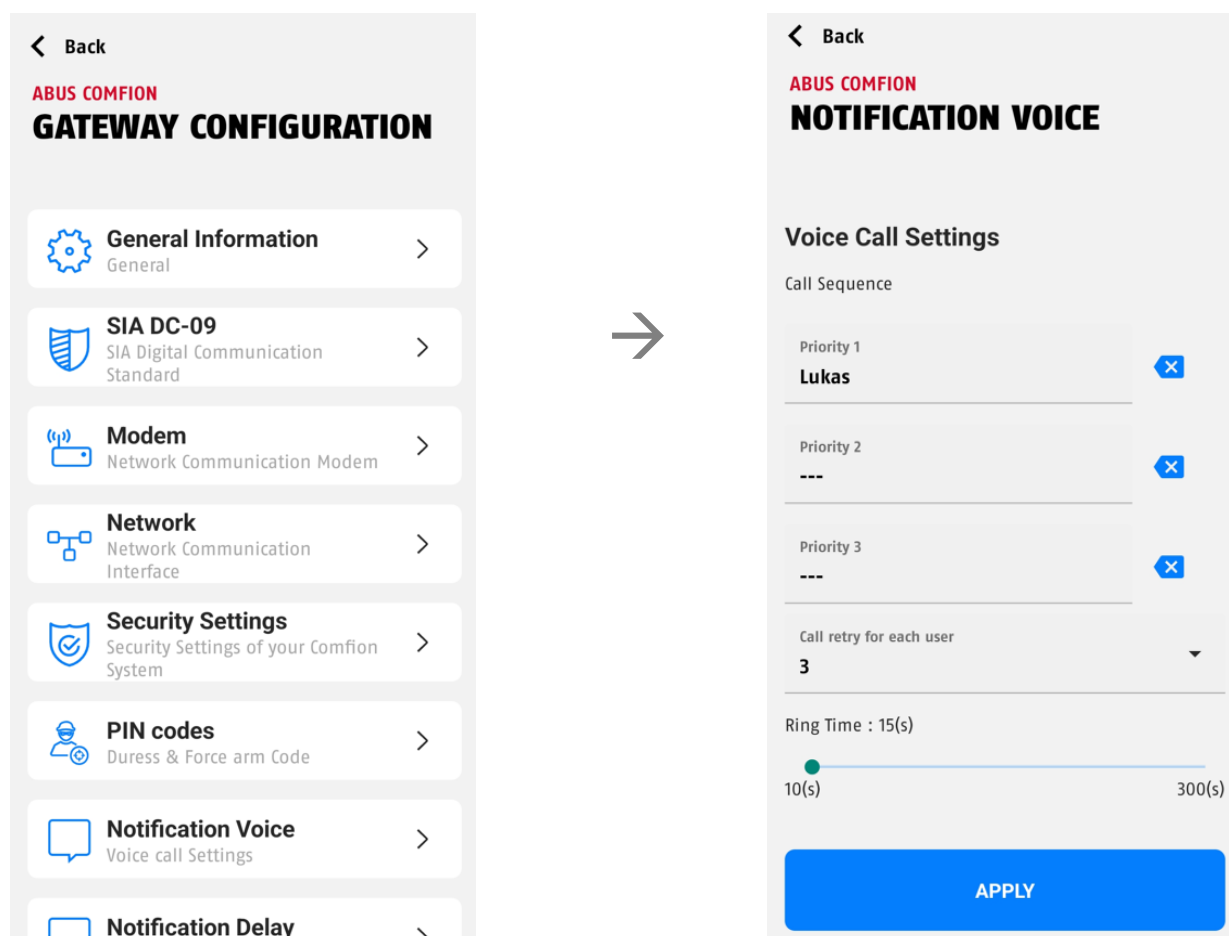
Si l'adresse e-mail à notifier doit être différente de celle du compte e-mail, vous pouvez enregistrer une adresse de notification dans votre compte (voir **4.4.2 Notifications**). Si vous n'enregistrez pas d'e-mail de notification, les e-mails seront envoyés à l'adresse e-mail de votre compte.

6.3. Appel téléphonique

Le système de sécurité Comfion Pro peut vous appeler en cas d'alarme. Le système n'est pas équipé d'un transmetteur vocal, ce qui signifie qu'aucun message vocal ne sera diffusé lors de cet appel. L'appel sert uniquement à donner l'alerte et doit aider à informer l'utilisateur appelé d'une alarme. La notification push envoyée simultanément indique de quel type d'alarme il s'agit.

La fonction d'appel nécessite l'insertion d'une carte SIM avec fonction d'appel. Pour plus d'informations sur le module GSM, voir **5.1 Module GSM**.

- Pour recevoir des appels, le numéro de téléphone du destinataire doit être enregistré dans le compte d'utilisateur (voir **5. Communication**).
- En outre, vous devez définir l'ordre des appels sous « Configuration centrale » - « Appel téléphonique ». Il est possible d'appeler au maximum 3 utilisateurs à la suite.



 Remarque	La répétition d'appel par utilisateur est réglée en usine sur 3. Cela signifie que chaque appelant reçoit trois appels. L'appel ne peut pas être confirmé.
---	--

6.4. SMS

Le système Comfion Pro peut envoyer des SMS à partir de la liste des événements (voir **5. Communication**). En outre, des automatisations permettent d'envoyer des SMS avec un texte librement définissable lors d'événements quelconques.

Pour que les SMS puissent être envoyés, il suffit qu'une carte SIM soit insérée dans le module et que le numéro d'appel de notification soit enregistré dans le compte (voir **5. Communication**).

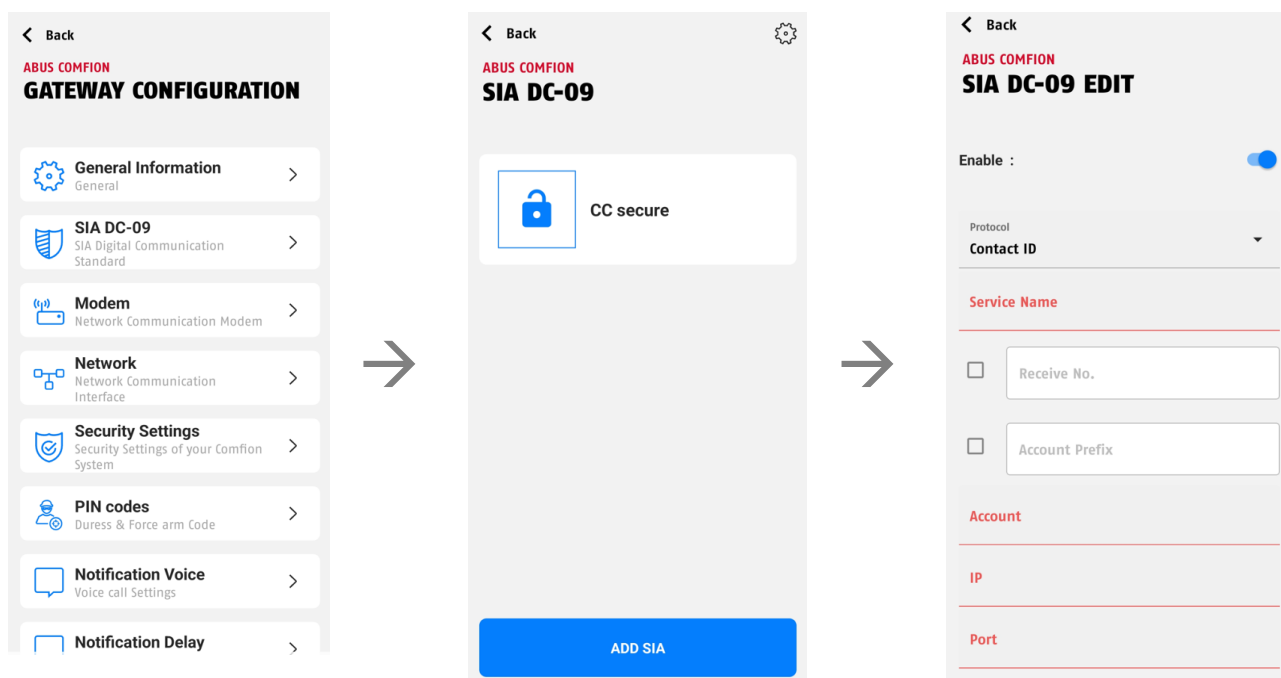
6.5. SIA CC-09 (connexion à la station de contrôle)

Le système de sécurité sans fil Comfion Pro dispose d'un composeur de station de contrôle numérique qui peut envoyer le protocole Contact ID via la norme SIA CC-09. Vous pouvez configurer plusieurs mises en ligne en même temps et ainsi communiquer avec différents services de gardiennage.

Inscrivez les données reçues de votre prestataire de services dans les champs concernés. Les deux champs grisés « Destinataire » ainsi que « Préfixe ID client » ne sont en général pas nécessaires et ne doivent être activés que si votre prestataire de services le demande explicitement.

Dans le champ « Message de test statique », vous pouvez choisir entre les options suivantes :

- **CC-09 Surveillance de ligne** -> Supervision intégrée dans le protocole de la station de contrôle (doit être pris en charge par la station de contrôle)
- **Message de test CID 602** -> Transmission du code CID de contact 602 selon l'intervalle défini
 - **Attention** : L'intervalle défini détermine le temps écoulé après le dernier événement envoyé à la station de contrôle. Si un événement est transmis à la station de contrôle dans l'intervalle, l'intervalle redémarre.



Le symbole de la roue dentée en haut à droite de l'écran permet d'accéder aux réglages avancés. Dans celui-ci, vous pouvez activer le message de test statique et régler l'intervalle

 Remarque	Vous trouverez une liste des codes Contact ID en annexe (chapitre 11.1)
---	--

7. Généralités, entretien et remarques

7.1. Configuration de la centrale

Sous l'option de menu Configuration de la centrale, vous trouverez d'une part toutes les informations importantes concernant votre centrale et pourrez d'autre part effectuer des réglages importants du système

Après avoir appelé l'option de menu Configuration des centrales, vous verrez les informations suivantes :

- Nom centrale → (champ de saisie)
- Symbole → (peut être remplacé par votre propre photo)
- Réseau → (affichage du type de connexion réseau)
- État de la téléphonie mobile → (Drop-Down)
 - Module de type → (puce GSM intégrée)
 - Carte SIM → (indique si elle est insérée)
 - IMEI → (numéro de série unique à 15 chiffres du module GSM)
 - Appel téléphonique → (indication si possible avec la SIM insérée)
 - Connexion LTE → (affichage de l'état de la connexion)
 - Force du signal (dBm) → (RSRP mesuré en -dbm, (force du signal recommandée voir **chapitre 5.1**)
- Alimentation électrique → (affichage bloc d'alimentation ou batterie)
- Firmware → (en cliquant dessus, la version et les notes de publication s'affichent)
- Module radio → (affichage du firmware du module radio)
- Référence

Confirmer

- Confirme les modifications dans ce menu.
- Les modifications sont ensuite également actualisées dans le cloud ABUS.

Supprimer la centrale d'alarme

- Supprime la centrale de l'application et du compte ABUS-Cloud !

Le symbole de la roue dentée en haut à droite permet d'ouvrir d'autres menus de réglage.

Pour les réglages concernant SIA CC-09, l'appel téléphonique et le module GSM, voir 5. Communication.

7.1.1. Informations générales

Sous le titre « Mémoire » s'affichent les informations relatives au support de stockage inséré (disque dur et/ou carte SD).

Le fuseau horaire utilisé ainsi que le serveur NTP s'affichent sous le titre « Date et heure ».

Le bouton « Redémarrage » permet de redémarrer la centrale.

7.1.2. Réseau

Dans ce menu, vous pouvez consulter les paramètres réseau et les adapter si nécessaire.

Vous avez le choix entre trois méthodes possibles :

DHCP (valeur par défaut) : Le protocole Dynamic Host Configuration Protocol est un protocole client/serveur par lequel le Comfion Pro reçoit automatiquement son adresse IP et d'autres informations connexes du routeur.

PPPoE : Point-to-Point Protocol over Ethernet est un protocole de réseau qui fournit une connexion directe dans le réseau interne. Pour ce faire, une authentification par nom d'utilisateur et mot de passe est nécessaire.

Statique : Si vous choisissez « statique », les données réseau du Comfion Pro sont attribuées manuellement. Consultez l'opérateur du réseau à ce sujet et n'attribuez pas d'adresse IP à partir du pool DHCP.

 Remarque	Des paramètres IP incorrects empêchent votre système de se connecter au réseau, ce qui le rend inaccessible à l'application. Dans ce cas, appuyez pendant 6 secondes sur la touche « Réinitialisation du réseau » (n° 14) située à l'arrière de l'appareil, puis relâchez-la. La centrale redémarrera alors et réinitialisera ses paramètres réseau sur les réglages par défaut DHCP.
---	--

7.1.3. Paramètres de sécurité

Mode mainten.	ON/OFF (Réglage par défaut OFF)	Le mode de maintenance est utilisé pour l'installation et la maintenance du système. Pendant que le mode de maintenance est actif, l'installation ne peut pas déclencher d'alarme.
Blocage de zone	3x-20x (par défaut 5x)	Si une zone se déclenche plus souvent que ce qui a été défini, cette zone ne se déclenchera plus jusqu'à ce que les alarmes soient supprimées de l'historique des alarmes
Répétition max. de la saisie au clavier	3x-20x (par défaut 5x)	Indique le nombre de saisies de PIN erronées sur l'élément de commande avant son blocage
Temporisation de l'élément de commande	5-180 sec (réglage par défaut 30 sec.)	Réglage du temps pendant lequel l'élément de commande est bloqué après X saisies erronées
Temporisation d'entrée	5-45 sec (réglage par défaut 10 sec.)	Si l'installation est armée, la temporisation d'entrée est affichée sur l'élément de commande radio.
temporisation de sortie	5-45 sec (réglage par défaut 30 sec.)	Temps de retard affiché sur l'élément de commande avant que la centrale ne passe à l'état armé.
Retard de transmission	5-180 sec (réglage par défaut 60 sec.)	Si cette propriété est activée dans la zone, la transmission d'un déclenchement est retardée de la durée définie.
Coupure de courant Retard	0-30 min (réglage par défaut 0 min)	Délai réglable de signalisation d'une perte de tension (12 V CC)
Activer la sirène anti-intrusion	ON/OFF (réglage par défaut ON)	Commande de la sirène en cas d'alarme anti-intrusion
Alarme d'intrusion Durée de la sirène	5-180 sec (réglage par défaut 60 sec.)	Durée de la signalisation acoustique par des sirènes connectées au système
Sabotage Activer la sirène	ON/OFF (réglage par défaut ON)	Commande de la sirène en cas d'alarme de sabotage
Alarme de sabotage Durée de la sirène	5-180 sec (réglage par défaut 60 sec.)	Durée de la signalisation acoustique par des sirènes connectées au système
Afficher la LED du logo : Sabotage	ON/OFF (réglage par défaut ON)	Indique visuellement le type d'alarme « sabotage » sur le logo ABUS éclairé. (rouge-clignotant)
Activer la sirène en cas d'agression	ON/OFF (réglage par défaut OFF)	Commande de la sirène en cas d'alarme agression
Alarme agression Durée de la sirène	5-180 sec (réglage par défaut 60 sec.)	Durée de la signalisation acoustique par des sirènes connectées au système
Afficher la LED du logo : Agression	ON/OFF (réglage par défaut ON)	Indique visuellement le type d'alarme « agression » par le logo ABUS éclairé. (clignoter en rouge)
Activer la sirène de l'eau	ON/OFF (réglage par défaut ON)	Commande de la sirène en cas d'alarme dégâts des eaux
Alarme dégâts des eaux Durée de la sirène	5-180 sec (réglage par défaut 60 sec.)	Durée de la signalisation acoustique par des sirènes connectées au système
Afficher la LED du logo : Inondation	ON/OFF (réglage par défaut ON)	Indique visuellement le type d'alarme « inondation » sur le logo ABUS éclairé. (clignoter en rouge)
Activer la sirène d'incendie	ON/OFF (réglage par défaut ON)	Commande de la sirène en cas d'alarme incendie
Alarme incendie Durée de la sirène	5-180 sec (réglage par défaut 60 sec.)	Durée de la signalisation acoustique par des sirènes connectées au système
Afficher la LED du logo : Alarme incendie	ON/OFF (réglage par défaut ON)	Indique visuellement le type d'alarme « incendie » sur le logo ABUS éclairé. (clignoter en rouge)
Activer la sirène de l'APP agression	ON/OFF (réglage par défaut OFF)	Commande de la sirène en cas d'alarme agression déclenchée via l'application
Aggression APP Durée de la sirène	5-180 sec (réglage par défaut 60 sec.)	Durée de la signalisation acoustique par des sirènes connectées au système

Afficher la LED du logo : Application d'agression	ON/OFF (réglage par défaut ON)	Indique visuellement le type d'alarme « app agression » par le logo ABUS éclairé. (clignoter en rouge)
Masquage Activer la sirène	ON/OFF (réglage par défaut ON)	Commande de la sirène en cas de masquage d'un détecteur (surveillance de la couverture)
Masquage Durée de la sirène	5-180 sec (réglage par défaut 30 sec.)	Durée de la signalisation acoustique par des sirènes connectées au système
Afficher la LED du logo : Masquage	ON/OFF (réglage par défaut ON)	Indique visuellement le type d'alarme « surveillance de couverture » au moyen du logo ABUS éclairé. (clignoter en rouge)
Masquer les erreurs de réseau	ON/OFF (réglage par défaut OFF)	Désactiver la prévention de l'armement d'une erreur de réseau
Masquer les erreurs de batterie	ON/OFF (réglage par défaut OFF)	Désactiver la prévention de l'armement d'un défaut de batterie
Masquer la perte de courant	ON/OFF (réglage par défaut OFF)	Désactiver la prévention de l'armement d'une perte de courant (12 V CC)
Activer la réinitialisation automatique	ON/OFF (réglage par défaut ON)	ON : La réinitialisation est effectuée lors du désarmement. Dès que tous les détecteurs déclenchés se trouvent à nouveau dans un état normal, l'aperçu des alertes disparaît du tableau de bord en cas de désarmement. OFF : Les alarmes et les erreurs doivent toujours être réinitialisées manuellement.
NFC mode ouvert	ON/OFF (réglage par défaut OFF)	OFF : Seuls les transpondeurs Mifare DESFire d'ABUS peuvent être utilisés, car ils sont contrôlés pour des raisons de sécurité sur l'application Comfion. Les transpondeurs d'autres fabricants ainsi que les transpondeurs Mifare Classic ne peuvent pas être utilisés. ON : Tous les transpondeurs Mifare Classic & Mifare DESFire peuvent être utilisés (restriction voir champ de remarque ci-dessous).
Autoriser la réinitialisation d'usine	ON/OFF (réglage par défaut ON)	OFF : La centrale ne peut pas être réinitialisée à l'aide du bouton de réinitialisation ON : La centrale peut être réinitialisée à l'aide du bouton de réinitialisation.
Désactiver la détection des sabotages	ON/OFF (réglage par défaut OFF)	ON : la détection de sabotage de tous les appareils programmés est désactivée.
Entrée-Suivant dans la même partition	ON/OFF (réglage par défaut OFF)	OFF : Entrée suivante Les zones réagissent à la temporisation d'entrée indépendamment de la partition ON : Entrée Les zones qui suivent ne réagissent qu'à la temporisation d'entrée déclenchée dans la même partition.



Remarque

Les transpondeurs Mifare DESFire d'autres fabricants ne fonctionnent que s'ils disposent d'un UID fixe. Aucun mécanisme d'identification aléatoire ne doit être activé sur les transpondeurs.

7.1.4. Codes PIN

Vous pouvez modifier le code de menace et le code d'armement forcé dans ce menu. Ces codes sont valables pour tous les utilisateurs de l'installation et sont composés de 3 chiffres
Les codes ne sont utilisables qu'en combinaison avec un élément de commande radio Comfion

 Remarque	Le code de menace et le code d'armement forcé sont saisis en même temps que le code utilisateur, à savoir Code utilisateur (4 chiffres) → Code de menace/forçage (3 chiffres) par ex. 1357999
---	---

Code de menace

- La saisie de ce code sur l'élément de commande radio Comfion permet de désarmer sous la contrainte
- Le Comfion Pro est désarmé, mais une communication a lieu vers les récepteurs configurés.

Code d'armement forcé

- Voir **chapitre 6.7.3**
- Permet d'activer une (ou plusieurs partitions) lorsque les zones sont ouvertes, sans opération de masquage.

7.1.5. Retards de notification

Vous pouvez régler les délais des **notifications de panne de réseau** dans ce menu.

Retard de notification du serveur :

Temps de retard en cas de défaillance de la connexion au cloud. Définit le délai, par exemple en cas de problèmes de cloud, avant qu'une notification ne soit envoyée. (réglage par défaut = 10 sec.) ; (Réglable de 10 à 600 sec.)

Retard de notification du client :

Délai de temporisation en cas de perte de connexion Internet sur la centrale Comfion Pro. Celle-ci peut survenir par exemple en raison d'une panne DSL, de l'absence de câble LAN ou d'une coupure de courant sur le routeur. (Réglage par défaut = 0 sec.) ; (Réglable de 0 à 600 sec.)

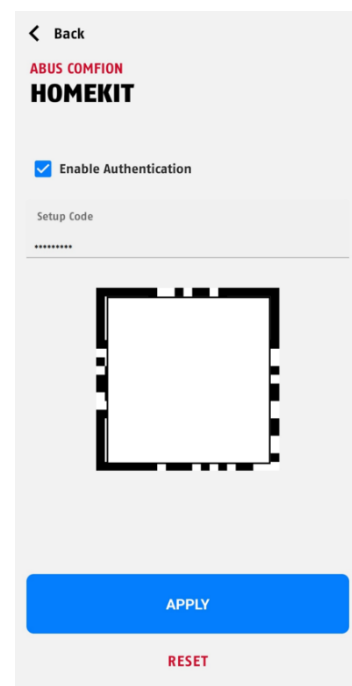
 Remarque	En fonction de l'infrastructure du réseau, il peut être conseillé d'augmenter légèrement le délai, en particulier si le routeur gère de nombreux clients IP.
---	--

En cliquant sur « **Confirmer** », les modifications sont prises en compte.

7.1.6. HomeKit

Ajouter un nouvel appareil dans l'interface utilisateur d'Apple HomeKit

- Au cours de la boîte de dialogue, il vous sera demandé de scanner le code QR présenté ici et/ou d'entrer le code de couplage à 8 chiffres.



7.1.7. Backup

 Remarque	Pour des raisons de sécurité, le fichier de sauvegarde de votre centrale est entièrement crypté et enregistré dans le Cloud d'Abus.
---	--

Créer une sauvegarde

Dans le menu Sauvegarde de la configuration de la centrale, vous pouvez créer une sauvegarde manuellement et activer la sauvegarde automatique. La sauvegarde automatique est effectuée chaque semaine.

Importer une sauvegarde

 Remarque	Veuillez noter que la nouvelle centrale a déjà été mise à jour avec la version firmware actuelle avant l'importation de la sauvegarde.
---	---

Pour importer la sauvegarde dans une nouvelle centrale, veuillez procéder comme suit :

1. Si ce n'est pas déjà fait, déconnectez du réseau la centrale d'où provient la sauvegarde et éteignez-la.
2. Dans l'aperçu des centrales de l'application, allez sur le symbole + pour ajouter une nouvelle centrale
3. Sélectionnez « Importer une sauvegarde »
4. Scannez le code QR au dos de votre nouvelle centrale
5. Sélectionnez la centrale à partir de laquelle vous souhaitez charger la sauvegarde
Remarque : Après l'importation, la sauvegarde est supprimée du cloud et les composants ne fonctionnent plus sur l'ancienne centrale.
6. Saisissez le nom de la centrale de votre nouvelle centrale
7. Après confirmation, un code de vérification est envoyé à l'adresse e-mail du propriétaire de l'installation. Saisissez ce code dans l'application et cliquez sur « Démarrer l'importation »
8. L'importation est maintenant effectuée. Vous pouvez maintenant fermer votre application et attendre de recevoir le message push indiquant que la centrale est en ligne et qu'elle est alimentée.

Pour restaurer une configuration sur le même matériel (centrale), veuillez procéder comme suit :

1. Réinitialisez la centrale concernée aux réglages d'usine (appuyez sur le bouton Reset pendant 10 secondes - > voir 6.5.1)
2. Dans l'aperçu des centrales de l'application, allez sur le symbole + pour ajouter une nouvelle centrale
3. Sélectionnez « Restauration »
4. Scannez le code QR au dos de votre centrale
5. Saisissez le nom souhaité de votre centrale
6. L'importation est maintenant effectuée. Vous pouvez maintenant fermer votre application et attendre de recevoir le message push indiquant que la centrale est en ligne et qu'elle est alimentée.

7.1.8. Informations sur WLX

Vous trouverez ici une liste des autorisations Fallback, y compris la carte de réinitialisation

Autorisation Fallback :

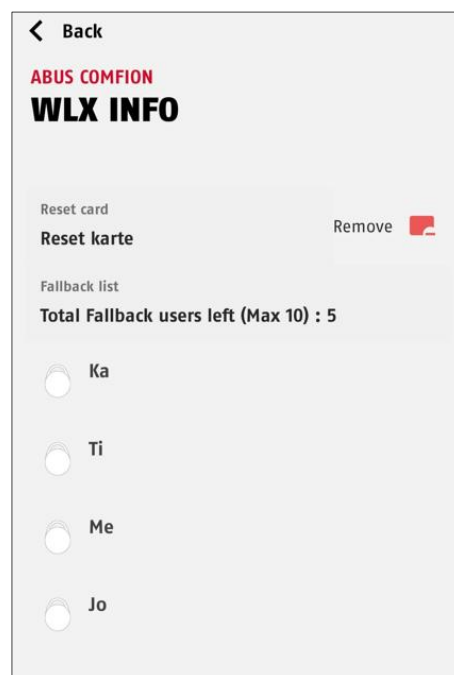
- L'autorisation Fallback est directement enregistrée dans le cylindre et permet l'accès lorsqu'il n'y a pas de liaison radio avec la centrale Comfion Pro & le module BUS-WLX. Dans le système Comfion Pro, il est possible d'attribuer jusqu'à 10 autorisations fallback (la carte de réinitialisation est toujours un support fallback).
- En cas d'interruption de la liaison radio, le support autorisé doit être présenté trois fois au cylindre wAppLoxx (attendre à chaque fois la signalisation)
- L'autorisation fallback est directement enregistrée dans les paramètres du NFC-Tag pour l'utilisateur, voir **chapitre 4.4** Modification des utilisateurs

Carte de réinitialisation

- La carte de réinitialisation est fournie avec le module Comfion Pro BUS-WLX.
- Après la programmation du premier composant wAppLoxx (cylindre ou lecteur mural), le processus d'apprentissage de la carte de réinitialisation est automatiquement lancé.
- La carte de réinitialisation est nécessaire pour réinitialiser un cylindre (en plus de la carte système)
- Si la carte de réinitialisation est perdue, elle peut être supprimée ici en la « retirant » et une nouvelle carte de réinitialisation peut ensuite être programmée. Après l'avoir retiré, le processus d'apprentissage démarre immédiatement !

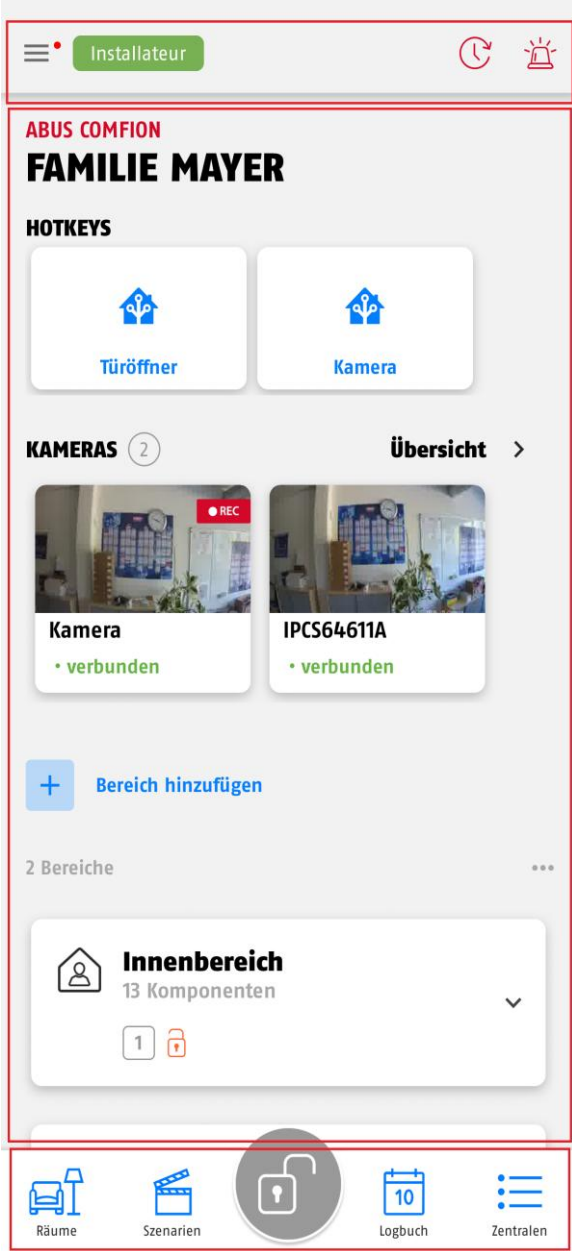
Liste Fallback

- Outre la carte de réinitialisation, jusqu'à 9 autres tags avec autorisation fallback apparaissent ici.



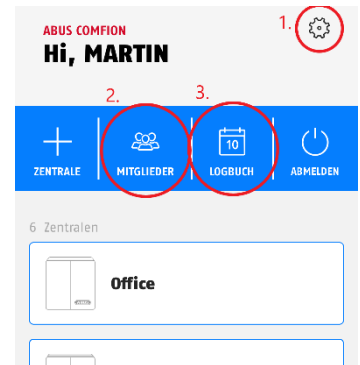
7.2. Tableau de bord (système configuré)

Le tableau de bord vous permet de contrôler l'installation et, même en tant qu'installateur, d'effectuer une grande partie de vos travaux.

	Barre de tête : •  Configuration et paramètres d'utilisation •  Rôle de l'utilisateur (installateur uniquement) •  Mise à jour du firmware (si disponible) •  Déclencher l'alarme de panique Tableau de bord / Domaine fonctionnel • Touches de raccourci clavier ○ Une courte pression sur la touche lance la scène & l'exécution est brièvement confirmée par  ○ Maintenir enfoncé pour configurer la scène • Aperçus de la caméra ○ Un clic sur l'image d'aperçu permet de passer au flux en direct ○ Un clic sur « Aperçu » permet d'accéder à la page des détails de la caméra et de poursuivre la configuration • Aperçu des partitions ○ Un clic sur  permet d'afficher les composants attribués et leur statut (si configuré). ○ Cliquer sur  pour ajuster le tri des partitions. Barre de navigation • Pièces (& liste des composants) voir 3.2.4 et 3.2.5 • Scénarios (scènes et automatisations) voir 6.4 • Modes d'alarme (symbole du cadenas) - voir 3.2.8 • Journal de bord (liste d'événements & fonction de filtrage) Centrales (aperçu) - voir 6.3
--	--

7.3. Aperçu des centrales

Dans l'aperçu des centrales de l'installation, vous pouvez, en plus de l'ajout de nouvelles centrales, voir les centrales existantes et y accéder, éditer les informations de votre compte (1), gérer vos membres (2) et voir le journal du compte (3).



7.3.1. Informations sur le compte

Vous y accédez dans l'aperçu de la centrale en cliquant sur la roue dentée.

Zurück

ABUS COMFION
ACCOUNT INFORMATIONEN

Face/Touch ID aktivieren : ☐

Name

E-Mail

Benachrichtigungssprache
Deutsch

Telefonnummer

Benachrichtigungs-Rufnummer

Benachrichtigungs-E-Mail

Erstellt am
2024-11-12 10:50:51

BESTÄTIGEN

ACCOUNT VERWALTUNG

- Activer Face/Touch ID
 - Sécurise l'application grâce à Face ou Fingerprint
- Nom du compte (affiché dans la centrale & le journal de bord)
- Compte e-mail
- Langue de notification
 - Définit la langue pour les notifications push, e-mail, SMS, le journal de bord, les partitions et les salles
- Numéro de téléphone
- Numéro d'appel de notification par SMS & appels téléphoniques
- E-mail de notification pour l'envoi d'e-mails de la centrale
- Date de création du compte
- Bouton de confirmation pour enregistrer les données
- Fonction de suppression du compte ABUS dans l'application

7.3.2. Membres

Dans l'application Comfion, vous avez la possibilité de tenir une liste des membres. Ceci est purement optionnel et n'est pas nécessaire au fonctionnement des systèmes Comfion Pro. Grâce à la liste des membres, lorsque vous ajoutez/invitez de nouveaux utilisateurs dans une centrale, vous pouvez facilement les sélectionner parmi vos membres.

7.3.3. Journal de bord du compte

Le journal de bord du compte répertorie tous les messages des installations autorisées à y accéder. Lorsque l'accès à une centrale est bloqué, les entrées du journal de cette centrale ne sont pas enregistrées dans le journal du compte.

7.4. Automations & scènes

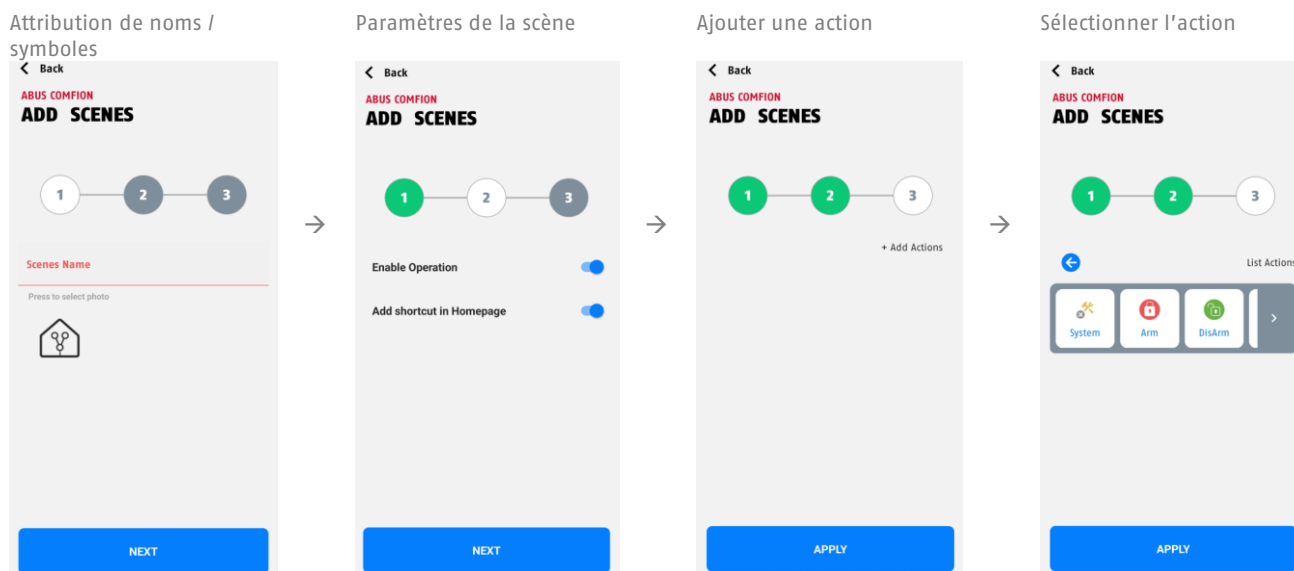
Le système Comfion Pro vous offre la possibilité de configurer jusqu'à 100 scénarios. Ces scènes ou automatisations sont entièrement paramétrables, ce qui vous offre une flexibilité maximale.

Sous l'onglet « Scénarios », vous pouvez ajouter aussi bien des scènes que des automatisations.

 Attention	Il est interdit de créer des automatisations qui se contredisent ou qui s'appellent de manière circulaire. Cela peut entraîner de graves problèmes de fonctionnement de la centrale.
 Remarque	Veuillez à laisser un intervalle d'au moins 5 secondes entre deux ordres de commutation pour le même appareil afin de pouvoir garantir un fonctionnement sans problème.

Scène = action déclenchée par un utilisateur via l'application (touche de raccourci). Peut être affiché dans le tableau de bord. Exemple : Prise de courant ON/OFF via l'application

Exemple de configuration d'une scène :



Étape 1 :

- Le nom de la scène est un champ obligatoire
- Changez le symbole en cliquant sur l'icône

Étape 2 :

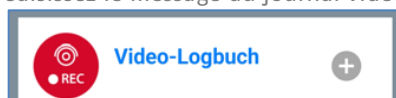
- Déterminez si la scène doit être active ou inactive (inactive = le nom de la scène est grisé)
- Afficher sur le tableau de bord affiche la scène du tableau de bord dans la partition « Touches de raccourci »

Étape 3 (ajouter une action) :

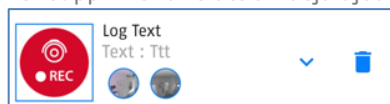
- Sélectionnez l'action dans la liste en cliquant dessus, en saisissant éventuellement d'autres données et enfin en cliquant sur le symbole « + » pour l'ajouter.

Exemple : Journal de bord vidéo :

- Saisissez le message du journal vidéo, sélectionnez les caméras, puis appuyez sur le symbole « + »



- Vous pouvez ajouter certaines actions directement en cliquant sur le symbole « + », puis en cliquant sur le  symbole pour ajouter d'autres paramètres.
- Vous pouvez supprimer une action déjà ajoutée en cliquant sur la poubelle



- Vous pouvez configurer plusieurs actions & elles seront exécutées l'une après l'autre. Vous pouvez changer l'ordre d'exécution en cliquant sur le symbole . Ensuite, vous pouvez glisser-déposer les actions. Une nouvelle pression sur  permet d'enregistrer la modification.
- Terminez la configuration de la scène en cliquant sur « Confirmer ».

Les actions suivantes peuvent être ajoutées :

Système	Journal de bord vidéo	Création d'une entrée de journal avec un message de journal et un extrait de l'enregistrement de la caméra (15 sec.) ou de l'image de la caméra PIR
	Redémarrage du système	Effectue un redémarrage de la centrale Comfion Pro.
	Vidéo de l'événement Push	Crée une notification push avec un texte de message, des images de caméra et les envoie aux destinataires sélectionnés
	Texte de l'événement Push	Crée une notification push avec un texte de message et l'envoie aux destinataires sélectionnés
	Délai	Exécute la scène avec un retard de la durée indiquée (secondes) ou retarde les actions successives.
Armée		Arme une partition du système Remarque : Après avoir ajouté cette action, il faut encore définir la partition en cliquant sur le symbole : 
Désarmée		Désarme une partition du système Remarque : Après avoir ajouté cette action, il faut encore définir la partition en cliquant sur le symbole : 
Scène		Exécute une scène déjà configurée. Remarque : Sélectionnez cette fonction pour exécuter plusieurs scènes simultanément (ou de manière décalée dans le temps à l'aide du délai).
Prise Comfion	Mise en marche	Allume la prise de courant
	Éteindre	Éteint la prise de courant
	Basculer	Commute la prise de courant (allumé → éteint, éteint → allumé)
Module relais Comfion	Mise en marche	Active le module relais
	Éteindre	Désactive le module relais
	Basculer	Commute le module relais (allumé → éteint, éteint → allumé)
Module de stores Comfion	Ouvert	Déplace les lamelles de store jusqu'à la position finale ouverte & haute
	Fermer	Déplace les lamelles du store jusqu'à la position finale fermée et vers le bas
	Arrêt	Arrête la commande d'ouverture ou de fermeture
	100 % vers le haut (50 % / 1/3 / 25 %)	Remonte les lamelles des stores de la valeur indiquée
	Fermer à 100 % (50 % / 1/3 / 25 %)	Descend les lamelles des stores de la valeur indiquée
	Ouverture des lamelles à 100 % (50 % / 1/3 / 25 %)	Ouvre les lamelles de store de la valeur indiquée
	Fermeture des lamelles à 100 % (50 % / 1/3 / 25 %)	Ferme les lamelles des stores de la valeur indiquée

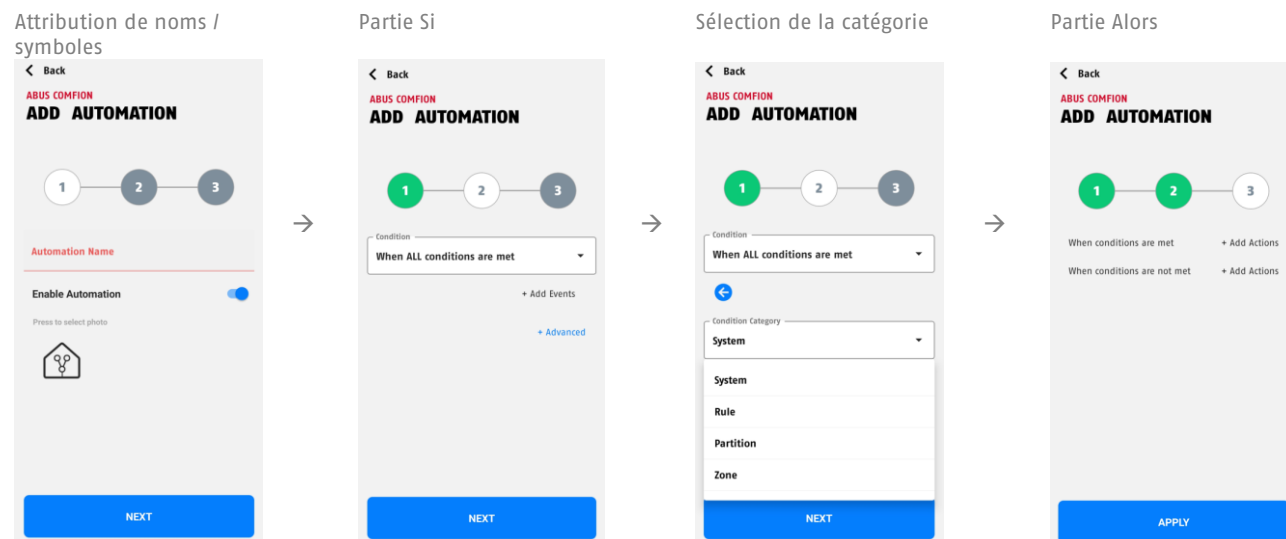
	Commande manuelle	Réglage individuel des lamelles des stores. En cliquant sur le symbole :  Le réglage de l'angle d'inclinaison (5 niveaux) et de la hauteur (10 niveaux) s'effectue à l'aide de la souris.
Centrale Comfion Pro	Sortie On	Active la sortie du relais de la centrale Comfion Pro
	Sortie OFF	Désactive la sortie relais de la centrale Comfion Pro
	Commutter la sortie	Permet de commuter la sortie du relais de la centrale Comfion Pro.
Sirène d'intérieur Comfion	Incendie	Exécute le message vocal « alarme incendie »
	Alarme	Active le son de la sirène (sous  Régler la durée max. 180 s)
	Arrêt	Désactive le son de la sirène
	Bip (signal sonore)	Active le son de confirmation (sous  Régler le nombre de répétitions (max. 30) ainsi que l'intervalle du piezo (max. 30 s)
	Échec	Active le son d'échec (sous  Régler le nombre de répétitions (max. 30) ainsi que l'intervalle du piezo (max. 30 s)
	Carillon de porte	Active le son du carillon de porte (sous  Régler le nombre de répétitions (max. 30) ainsi que l'intervalle du piezo (max. 30 s)
	Agression	Exécute le message vocal « alarme agression »
	Alarme dégâts des eaux	Effectue l'annonce vocale
Sirène extérieure Comfion	Alarme	Active le son de la sirène (sous  Régler la durée max. 180 s)
	Arrêt	Désactive le son de la sirène
	Bip (signal sonore)	Active le son de confirmation (sous  Régler le nombre de répétitions (max. 30) ainsi que l'intervalle du piezo (max. 30 s)
	Carillon	Active le son du carillon (sous  Régler le nombre de répétitions (max. 30) ainsi que l'intervalle du piezo (max. 30 s)
Détecteur de fumée Comfion	Arrêt de l'alarme	Désactive le signal d'alarme du détecteur de fumée Comfion. (le détecteur se déclenche à nouveau en cas de détection)
WLX-out (module hybride Comfion)	Sorties 1, 2, 3 allumées	Active la sortie 1 ou 2 ou 3 du module hybride Comfion
	Sortie 1, 2, 3, arrêt	Désactive la sortie 1 ou 2 ou 3 du module hybride Comfion
	Commutation des sorties 1, 2, 3	Commute la sortie 1 ou 2 ou 3 du module hybride Comfion
Comfion Caméra PIR / Caméra PIR extérieure	Instantané	Crée une capture d'image manuelle
Cylindre WLX Pro (accès/intrusion)	Mode bureau (accès permanent)	Complète le mode bureau (Permet l'accès sans tag NRC) En cliquant sur le symbole :  permet de choisir si le mode bureau doit être « activé » ou « désactivé ».
	Libération à distance (ouverture à distance)	Couple le cylindre de serrure via l'application et autorise ainsi l'accès. En cliquant sur le symbole :  définir le temps de couplage (max. 180 sec.)
WLX Pro Lecteur mural (accès/intrusion)	Libération à distance (ouverture à distance)	Commande l'ouverture de la porte (sortie sur le boîtier de pont) via l'application et autorise ainsi l'accès. En cliquant sur le symbole :  déterminez la durée de l'impulsion (6 ou 12 s)
Caméra IP (IPxxxxxxx)	Aller au préréglage	Orienté la caméra PTZ vers une position prédéfinie. En cliquant sur le symbole :  Sélection de la position 1, 2, 3 ou 4.

- Cliquez sur les scènes déjà configurées pour les modifier ou les supprimer.

Automation = se compose toujours de si et de alors. Librement configurable.

Exemple : Si l'installation est armée, alors la lumière est éteinte

Exemple de configuration d'une automation :



Étape 1 :

- Saisissez le nom de l'automation (champ obligatoire)
- Déterminez si l'automation est activée ou désactivée
- Changez le symbole en cliquant sur l'icône

Étape 2 : (Définir l'événement Si)

- Choisissez entre un lien « Et » ou un lien « Ou » :
 - Dans le cas de la liaison « Et », TOUTES les conditions doivent être remplies pour que l'action soit exécutée. Dans le cas de la liaison « ou », au moins UNE condition doit être remplie pour que l'action soit exécutée.
- Sélectionner l'événement « Si » :
 - Il est possible de configurer plusieurs événements, qui doivent être satisfaits soit TOUS (lien « et »), soit au moins UN (lien « ou »).
- Les événements suivants peuvent être sélectionnés :
 - Système -> Vous trouverez ici les événements système tels qu'une coupure de courant, mais aussi le planning
 - Règle -> Les automatisations existantes peuvent être connectées à une automation ...
 - Partition -> On trouve ici les événements de partition tels qu'armer/désarmer, intrusion, prêt à l'activation, etc.
 - Zone -> On trouve ici tous les événements liés à la zone (par ex. zone cambriolage)
 - Pièce -> On y trouve tous les composants et les événements qui y sont liés (par ex. détecteur d'ouverture contact ouvert ou bouton-poussoir mural appuyé)
- Sélectionnez en outre sous « Avancé », ...
 - ... combien de temps les conditions définies doivent s'appliquer avant que l'action ne soit exécutée. L'action ne sera exécutée que si les conditions s'appliquent à la période de temps définie et ne changent plus.
 - Exemple : Si la porte est ouverte pendant 30 secondes, alors... envoyer une notification push.

Étape 3 : (Définir l'événement Alors)

- L'action « Si, alors » -> est exécutée si les conditions définies dans la partie « Si » sont remplies
 - Les actions configurables ici sont les mêmes que celles du configurateur de scènes (étape 3)
- « Si passé, alors » -> l'action est exécutée lorsque les conditions définies dans la partie Si ne sont PLUS applicables

Modifier une scène/automation

Pour modifier, maintenez le symbole de la scène/de l'automation enfoncé pendant un peu plus de 2 secondes, puis relâchez-le

Suppression d'une scène/automation

Vous pouvez supprimer une scène/automation en passant en mode d'édition (voir « Édition d'une scène/automation ») et en cliquant ensuite sur le bouton « Supprimer une scène/automation » en bas de l'écran.

7.5. Réinitialisations



7.5.1. Réinitialisation d'usine

Pour réinitialiser la centrale aux réglages d'usine, maintenez la touche de réinitialisation (touche 12 voir 2.3 *Description de l'appareil*) enfoncée pendant >10 secondes et relâchez-la. Les LED de la centrale s'éteindront après quelques secondes et la centrale effectuera un redémarrage. Après le redémarrage, la centrale se trouve sur les réglages d'usine et peut être configurée à nouveau.

7.5.2. Redémarrage (reboot)

Maintenez la touche Reboot (touche 13) enfoncée pendant 2 secondes. Les LED de la centrale s'éteignent brièvement. La centrale effectue un redémarrage.

 Remarque	Lors du redémarrage décrit ici, l'alimentation électrique n'est pas interrompue. Si, par exemple, dans le cadre d'un redémarrage, la centrale est déconnectée manuellement de l'alimentation électrique, la centrale effectue un contrôle de tous les appareils connectés à la fin de l'opération de redémarrage & ce contrôle entraîne de nombreuses entrées dans le journal.
--	---

7.5.3. Réinitialisation de l'utilisateur

Pour réinitialiser les utilisateurs de l'installation ou supprimer tous les utilisateurs de l'installation, appuyez 5 fois sur la touche de réinitialisation du réseau (n° 14) en l'espace de 5 secondes. Après quelques secondes, la LED Internet passe brièvement au rouge. Vous devriez recevoir un message push sur les appareils connectés vous informant que la centrale concernée a été supprimée.

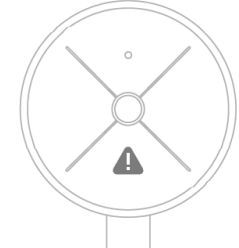
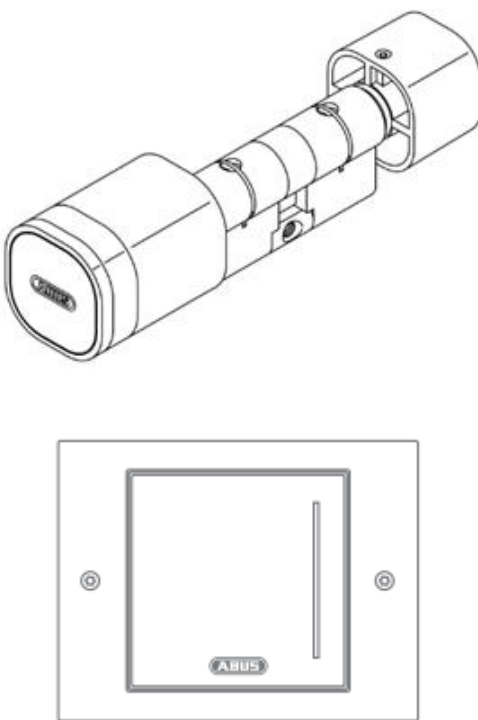
Lorsque tous les voyants sont à nouveau verts (le voyant Internet peut clignoter en vert), vous pouvez ajouter à nouveau l'installation en cliquant sur le symbole + dans votre application.

7.5.4. Réinitialisation du réseau

Si vous ne pouvez plus accéder à votre installation sur le réseau en raison d'un mauvais réglage IP, il est possible de réinitialiser la centrale sur DHCP. Pour ce faire, maintenir enfoncée pendant 6 secondes la touche de réinitialisation du réseau située au dos de la centrale (n° 14). Après quelques minutes, l'installation devrait être à nouveau accessible.

7.6. Utilisation

7.6.1. Armement / désarmement

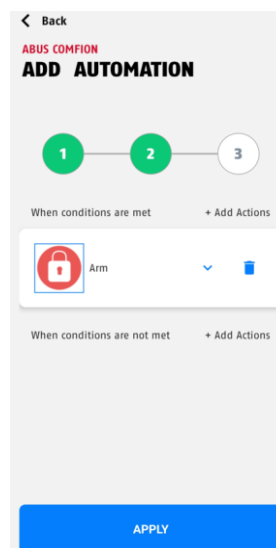
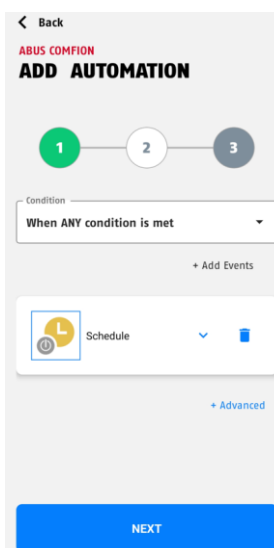
APP : L'armement/désarmement peut être effectué dans l'application en exécutant les modes d'alarme. Pour ce faire, cliquez dans le tableau de bord sur le bouton central en bas de l'écran (symbole du cadenas) et sélectionnez ensuite l'action (par ex. Entièrement armé).	
ELEMENT DE COMMANDE : Vous pouvez armer et désarmer le système à l'aide d'un élément de commande sans fil. Pour ce faire, saisissez votre code utilisateur ou présentez le NFC-Tag devant l'élément de commande et cliquez ensuite sur la surface d'action à exécuter (touches du cadenas). Vous trouverez des informations plus détaillées dans le guide de l'utilisateur ou dans le mode d'emploi de l'élément de commande	
TÉLÉCOMMANDE : Vous pouvez attribuer les modes d'alarme aux touches de votre télécommande sans fil et exécuter ainsi l'action correspondante en appuyant sur une touche. Vous trouverez ce réglage sous la télécommande.	
Cylindre WLX-Pro / WLX Pro Wall-Reader : se fait directement sur le lecteur Armement : • Présenter le tag RFID au lecteur • Verrouiller le cas échéant pendant le temps d'ouverture et présenter à nouveau le tag RFID • Armement réussi : LED rouge 1 x long • N'a pas réussi : LED rouge 6 x Désarmement : • Présenter le tag RFID au lecteur • Une fois désarmé avec succès, le cylindre se couple et la LED verte clignote 1 x longuement • Pas de succès : La LED rouge clignote 6 fois  Remarque Si la connexion radio est interrompue, la fonction Fallback est exécutée après le troisième processus de lecture infructueux. Pour plus de détails, voir chapitre 6.1.8	

AUTOMATION : Grâce à une automatisation, vous pouvez soumettre l'armement ou le désarmement de l'installation à des conditions. Cela permet par exemple de commuter selon un horaire ou lors de l'activation d'une entrée de fil.



Remarque

Selon EN 50131, le désarmement ne peut être effectué que par des personnes autorisées. Une activation temporisée ne peut être effectuée que dans le respect de la contrainte (par ex. l'utilisateur doit quitter le bâtiment et verrouiller la porte avant que l'armement ne puisse être effectué) et lorsque l'installation ne présente aucun dysfonctionnement. Dans ce cas, l'activation doit être indiquée par un signal acoustique et/ou visuel.



7.6.2. Réinitialisation des alarmes

La réinitialisation du système Comfion Pro peut se faire de la manière suivante, en fonction du réglage :

- Si l'option « Activer la réinitialisation automatique » est activée (sous Config. centrale), il est possible d'activer la réinitialisation automatique. - Paramètres de sécurité), la centrale réinitialise automatiquement l'alarme lors du désarmement, si les détecteurs concernés sont fermés.
- Si l'option « Réinitialisation automatique » est désactivée (sous Config. centrale - Paramètres de sécurité), le message s'affiche en haut de l'écran de l'application après une alarme et doit être réinitialisé manuellement par l'utilisateur.

Paramètres de sécurité	Tableau de bord	Réinitialiser l'alarme

7.6.3. Armement forcé

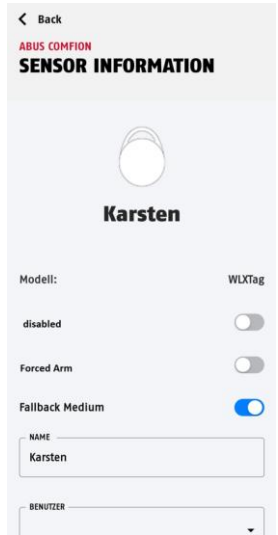
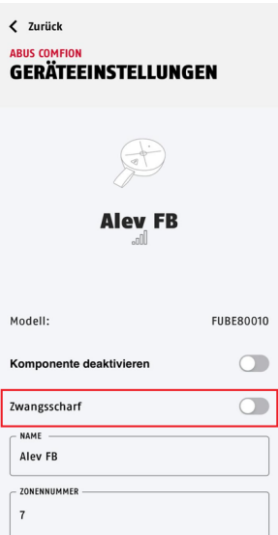
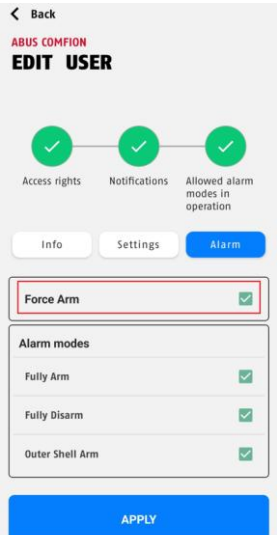
La fonction « Armement forcé » permet d'armer la centrale malgré une zone déclenchée/ouverte. La zone concernée est alors masquée sans autre intervention. Il n'est plus nécessaire de masquer manuellement le détecteur.

 Remarque	Veuillez noter que la fonction d'armement forcé ne peut être exécutée que si la zone déclenchée/ouverte possède le comportement de zone « Masquable ».
---	---

Pour l'armement forcé **via l'élément de commande**, le code d'armement forcé peut être défini dans la configuration de la centrale sous « Codes PIN » (voir **chapitre 6.1.4**). Ce code à 3 chiffres est saisi derrière le code utilisateur à 4 chiffres pour l'armement forcé via l'élément de commande.
En outre, il est possible d'attribuer l'attribut Armement forcé à un **transpondeur** afin de commuter avec celui-ci.

Pour l'armement forcé **via la télécommande sans fil**, il est possible de cocher la case « Armement forcé » dans les paramètres de la télécommande.

Pour l'armement forcé **via l'application**, il est possible de cocher la case « Armement forcé » sous l'onglet « Alarme » de chaque utilisateur.

			
Élément de commande & code d'armement forcé	Réglages du transpondeur	Télécommande	Paramètres utilisateur Alarme

7.7. Signification des symboles

Alimentation électrique	
	Niveau de charge de la pile (ou de l'accumulateur) 100 % / 75 % / 50 % / 25 % / pile vide
	Gauche : alimentation électrique externe (CC ou CA) connectée À droite : Alimentation de secours (batterie) en veille
Signal radio	
	4 barres = excellent 3 barres = très bon 2 barres = modéré 1 barre = mauvais
	Liaison radio interrompue. Se produit après la défaillance du signal de supervision du composant concerné, c'est-à-dire après > 1 heure (peut varier pour certains composants)
Comportement de l'appareil	
	Composant déclenché (par ex. détecteur d'ouverture ouvert, détecteur de secousses déclenché, détecteur de fumée déclenché, détecteur d'inondation déclenché)
	Mouvement détecté (détecteur de mouvement PIR / détecteur de mouvement micro-ondes)
	Appareil déclenché (p. ex. sirène activée, pression sur la touche)
	Zone fermée (par ex. détecteur d'ouverture fermé)
	Zone ouverte (par ex. détecteur d'ouverture ouvert) → Apparaît en plus du symbole « composant déclenché »

Défauts	
	Sabotage détecté (par ex. boîtier ouvert ou appareil retiré de la surface de montage) Symbole alternatif : 
	Rupture de câble détectée (par ex. détecteur 3en1)
Icônes d'action (une pression sur l'icône déclenche l'action décrite)	
	État de l'appareil OFF (par ex. prise sans fil désactivée) → Une pression sur le symbole met l'appareil en marche
	État de l'appareil ON (par ex. prise sans fil activée) → Une pression sur le symbole permet d'éteindre l'appareil
	Caméra PIR 1. Créer un enregistrement (appuyer sur le symbole pour déclencher l'enregistrement manuel) 2. Enregistrement en cours 3. L'enregistrement est transmis à la mémoire centrale.
Icônes WLX (contrôle d'accès)	
	Accès accordé Affichage pour le temps pendant lequel le cylindre est couplé (6/12 sec)
	L'accès permanent est activé (mode bureau activé)  Remarque L'accès permanent est une configuration dans la centrale. Pour l'exécution, le cylindre doit d'abord être réveillé (c'est-à-dire tourné) et établir une liaison radio avec la centrale. L'accès est ensuite autorisé.
	Partition armée Les partitions auxquelles le cylindre / Wall-Reader est assigné sont armées

7.8. ABUS-Cloud

Le système de sécurité sans fil Comfion Pro se connecte à l'Abus Cloud lors de sa première mise en service. L'installation est en outre enregistrée dans le compte de l'installateur Abus Cloud. Si cela n'est pas souhaité, il est possible de décocher la case « Installateur principal » sous l'utilisateur concerné dans l'installation, ou de la cocher pour un autre installateur.

7.9. Remarques sur le disque dur / le stockage de données SSD

- Les vis de fixation du disque dur ne doivent être serrées qu'à la main
- La durée de vie de la batterie de la centrale est influencée par le disque dur intégré et sa consommation électrique, ainsi que par le nombre d'abonnés BUS connectés.
 - La durée d'alimentation de secours exigée par la norme EN 50131 pour les centrales d'alarme anti-intrusion selon EN niveau 2 est garantie par l'utilisation d'une mémoire de données SSD et la connexion de jusqu'à 2 modules BUM080000 WLX Pro au Comfion Pro BUS !
- Le disque dur installé dans le Comfion Pro doit être formaté au format exFAT ou NTFS
- Ne remplacez le disque dur/la mémoire de données SSD que lorsque la centrale est hors tension

7.10. Maintenance et entretien par l'installateur

Testez le bon fonctionnement du système lors de l'entretien de routine :

- Vérifiez que le Comfion Pro ne présente pas de signes évidents de dommages au niveau du boîtier, du support mural ou du cache avant.
- Vérifiez l'action de l'interrupteur anti-sabotage
- Vérifiez l'état des batteries de secours
- Nettoyez le boîtier
 - Après le nettoyage, essuyez la surface à l'aide d'un chiffon doux et sec.
 - N'utilisez pas d'eau, de solvants ni de produits de nettoyage.
- Contrôlez la force du signal et l'état des piles/de la batterie de tous les composants
- Remplacez les piles ou les accumulateurs comme recommandé dans les instructions du fabricant
- Testez chaque composant.
- Nettoyez soigneusement les objectifs de tous les détecteurs PIR et de toutes les caméras à l'aide d'un chiffon doux et sec propre.
 - N'utilisez pas d'eau, de solvants ni de produits de nettoyage.
- Effectuez un test de détection de tous les détecteurs.
- Testez tous les générateurs de signaux
- Testez la transmission.

 Remarque	ABUS recommande de remplacer l'accumulateur central après 3 ans maximum. En cas de durée prolongée, une chute soudaine des performances ne peut être exclue.
---	--

Comment changer la batterie de la centrale :

- Mettez la centrale en mode maintenance (paramètres de sécurité)
- Retirez la centrale du support mural
- Mettez l'interrupteur de la batterie sur « OFF »
- Ouvrez le couvercle avant en desserrant les vis arrière et en faisant levier sur le couvercle (pour plus de détails, voir le **chapitre 3.1** Montage mural de la centrale)
- Débranchez l'alimentation électrique ainsi que l'ancienne batterie de la centrale
- Attendez 30 secondes
- Rebranchez la nouvelle batterie et l'alimentation électrique
- Fermez le couvercle de l'installation et quittez ensuite à nouveau le mode de maintenance

7.11. Tableau des forces du signal radio

Le tableau suivant décrit la signification des valeurs de signal des composants radio Comfion affichées en dBm.

Valeur RSSI (dBm)	Signification	Affichage sur le composant
<= -100	Faible	0 barre
<= -96	OK	1 barre
<= -91	Bon	2 barres
<= -86	Très bon	3 barres
> -86	Excellent	4 barres

8. Garantie

- Le plus grand soin est apporté à la conception et à la fabrication des produits ABUS en conformité avec les normes en vigueur.
- La garantie couvre uniquement les vices résultant de défauts matériels ou de fabrication présents au moment de la vente. En présence d'un défaut matériel ou de fabrication avéré, le module est réparé ou remplacé à la discrétion du donneur de garantie.
- La garantie se termine, dans de tels cas, à expiration de la durée d'origine de la garantie de 2 ans. Toute revendication dépassant ce cadre est expressément exclue.
- ABUS n'est pas responsable des défauts et dommages dus à des influences extérieures (par ex. transport, force, erreur de manipulation), à une utilisation non conforme, à l'usure normale ou au non-respect de ce mode d'emploi et des consignes d'entretien.
- En cas de réclamation au titre de la garantie, le produit en question doit être accompagné de la preuve d'achat originale avec la date d'achat et d'une brève description écrite du défaut.
- Si vous deviez constater un défaut déjà présent à l'achat sur le produit, nous vous prions de vous adresser directement à votre revendeur au cours des deux premières années.

9. Élimination



Éliminez l'appareil conformément à la directive européenne sur les déchets d'équipements électriques et électroniques 2012/19/UE - DEEE (déchets d'équipements électriques et électroniques). En cas de doute, veuillez vous adresser aux autorités communales compétentes en matière d'élimination. Vous recevrez les informations sur les points de reprise de vos vieux appareils par ex. auprès de l'administration communale ou municipale locale, des entreprises locales d'élimination des déchets ou auprès de votre revendeur.

10. Conformité

10.1. Déclaration de conformité UE

Par la présente, ABUS Security-Center GmbH & Co. KG déclare que l'appareil sans fil FUAA85000 est conforme à la directive 2014/53/UE et

2011/65/UE. Le texte complet de la déclaration de conformité UE est disponible à l'adresse Internet suivante :

abus.com > Recherche d'articles > FUAA85000 > Téléchargements

10.2. Conformité à la norme EN 50131

Le système de sécurité FUAA85000 est certifié conforme au niveau de sécurité 2 lorsqu'il est correctement installé, conformément aux normes EN 50131-1+A3:2020, EN 50131-3:2009, EN 50131-10:2014, EN 50136-1+A1:2018, EN 50136-2:2013 et EN 50131-5-3:2017.

11. Annexe

11.1. Contact ID Tableau de codes

Code	Classe de code	Données supplémentaires	Type	Description
111	Alarme incendie	Zone	Fumée	Un détecteur de fumée a déclenché une alarme incendie 24h/24
120	Alarme de panique	Zone	Panique	Une alarme panique a été déclenchée sur l'élément de commande
121	Alarme de panique	Utilisateur	Menace	Un utilisateur a saisi le code de menace
130	Alarme anti-intrusion	Zone	Effraction	Une zone d'intrusion a été déclenchée alors que le système était armé
131	Alarme anti-intrusion	Zone	Périmètre	Une zone périmétrique déclenche une pré-alarme

133	Alarme anti-intrusion	Zone	Zone 24 heures	Une zone d'alarme anti-intrusion de 24 heures a été déclenchée
134	Alarme anti-intrusion	Zone	Entrée/sortie	Une zone d'entrée/sortie a été déclenchée alors que le système était armé
135	Alarme anti-intrusion	Zone	Zone Immédiat (surveillé)	Une zone Immédiat (Surveillé) a été déclenchée alors que le système était armé
137	Alarme anti-intrusion	Zone	Sabotage	Le sabotage de la centrale a été déclenché
139	Alarme anti-intrusion	Zone	Bris de verre	Incursion confirmée par une zone
154	24 heures Alarme technique	Zone	Alarme dégâts des eaux	Le détecteur d'inondation signale une erreur
301	Défaut du système	Zone	Panne de tension du réseau AC	Perte de la tension secteur de la centrale ou du module d'extension lorsque l'installation est désarmée
302	Défaut du système	Zone	Batterie-Défaut	Batterie tampon vide de la centrale à l'état désarmé
305	Défaut du système	Zone	Réinitialisation	Le système a été réinitialisé et redémarré
306	Défaut du système	Zone	Redémarrage	Le système a effectué un redémarrage
308	Défaut du système	Zone	Arrêter	Le système a été arrêté et a cessé de fonctionner
311	Défaut du système	Zone	Batterie manquante / hors service	La batterie tampon de la centrale est absente ou complètement déchargée
338	Défaut périphérique	Zone	Élément de commande verrouillé	L'élément de commande est bloqué en raison de la saisie répétée d'un code erroné
344	Défaut périphérique	Zone	Détection de brouillage	Le récepteur radio a détecté un signal parasite (brouillage).
350	Communication Défaut	Zone	Erreur de comm.	Le système a détecté une erreur de communication.
381	Défaut du détecteur	Zone	Supervision	La zone indiquée ne s'est pas manifestée pendant l'intervalle de supervision.
383	Défaut du détecteur	Zone	Sabotage	Un sabotage a été déclenché dans la zone concernée
384	Défaut du détecteur	Zone	Batterie faible	Une pile vide a été déclenchée dans la zone concernée
393	Défaut du détecteur	Zone	Défaut maintenance	La zone concernée a signalé un défaut
400	Armer/désarmer/ Accès à distance	Utilisateur	Armée/ Désarmée	L'utilisateur concerné a armé ou désarmé le système via la télécommande
401	Armer/désarmer/ Accès à distance	Utilisateur	Armée/ désarmée via l'utilisateur	L'utilisateur concerné a armé ou désarmé le système via l'APP de son smartphone
406	Armer/désarmer/ Accès à distance	Utilisateur	Réinitialiser	L'utilisateur concerné a réinitialisé l'alarme précédemment déclenchée
407	Armer/désarmer/ Accès à distance	Utilisateur	Armée/ désarmée via l'élément de commande	L'utilisateur concerné a armé ou désarmé le système à l'aide d'un élément de commande radio
443	Armer/désarmer/ Accès à distance	Utilisateur	Armer avec masquage	L'utilisateur concerné a armé le système en masquant les défauts
454	Armer/désarmer/ Accès à distance	Utilisateur	Échec de l'armement	Le système n'a pas pu être armé après la temporisation de sortie
461	Armer/désarmer/ Accès à distance	Zone	Saisie du code erronée	Un code erroné a été saisi sur l'élément de commande.
570	Masquer	Zone	Masquer la zone	La zone concernée a été masquée
572	Masquer	Zone	Masquer la zone 24 heures	La zone 24 heures concernée a été masquée
602	Test	-	Message de test périodique	Un message de test périodique a été transmis à la station de contrôle.

ABUS I Security Center GmbH & Co. KG
abus.com

Linker Kreuthweg 5
86444 Affing
Allemagne

Tél. : +49 82 07 959 90-0



Security Tech Germany

FUAA85000

INSTALLATEURSHANDLEIDING

Comfion Pro draadloos beveiligingssysteem



1.	Updates	5
1.1.	Handleiding	5
1.2.	Comfion Pro-firmware en release-opmerkingen	5
2.	Algemeen	6
2.1.	Inleiding	6
2.2.	Beoogd gebruik / Wettelijk verplichte aanwijzingen	6
2.3.	Klantenservice / Customer Support	6
2.4.	Impressum	6
2.5.	Verklaring van symbolen	7
3.	Weringsprincipe en eigenschappen	7
3.1.	Productkenmerken	7
3.2.	Leveringsomvang	8
3.3.	Beschrijving van het apparaat	9
3.4.	Technische gegevens	11
4.	Montage en ingebruikname	12
4.1.	Wandmontage van de centrale	12
4.2.	Inbedrijfstelling van het systeem	15
4.2.1.	Installatie via de app & afronding van de hardwarevoorbereidingen	15
4.2.2.	Dashboard (na eerste aanmelding)	18
4.2.3.	Partities	18
4.2.4.	Ruimtes	19
4.2.5.	Componenten	20
4.2.6.	Instellingen voor componenten	22
4.2.7.	Aanwijzingen voor de bedrading (ingangen/uitgangen/BUS)	23
4.2.8.	Alarmmodi	24
4.3.	WLX Pro-installatie en programmering	25
4.3.1.	Installatie, configuratie en gebruik van de WLX Pro-cilinders en wandlezers	26
4.3.2.	WLX Pro-functies – Op afstand openen en kantoormodus	27
4.4.	Camera's (NVR)	28
4.4.1.	Camera's integreren via ONVIF	28
4.4.2.	Camera's integreren via RTSP	29
4.4.3.	Camera-instellingen (algemeen)	30
4.4.4.	Camera-instellingen (afzonderlijk)	30
4.4.5.	NVR-bediening	32

5. Gebruikers en autorisatiegroepen	33
5.1. Uitleg over de verschillende rollen	33
5.2. Inbedrijfstelling	34
5.2.1. Overdracht aan de eigenaar	34
5.3. Gebruikers uitnodigen/toevoegen	34
5.4. Gebruikers bewerken	34
5.4.1. Toegangsrechten	34
5.4.2. Notificaties	35
5.4.3. Toegestane alarmmodi tijdens bedrijf	36
5.5. Gebruikers verwijderen	36
6. Communicatie	36
6.1. Mobiele communicatiemodule	36
6.2. E-mail	37
6.3. Telefonische melding	38
6.4. SMS	38
6.5. SIA DC-09 (meldkamer bijschakelen)	39
7. Algemene informatie, onderhoud en opmerkingen	40
7.1. Centrale-configuratie	40
7.1.1. Algemene informatie	40
7.1.2. Netwerk	40
7.1.3. veiligheidsinstellingen	41
7.1.4. Pincodes	43
7.1.5. Vertragingen bij de kennisgeving	43
7.1.6. HomeKit	44
7.1.7. Backup	44
7.1.8. Informatie over WLX	45
7.2. Dashboard (systeem ingesteld)	46
7.3. Centrale-overzicht	47
7.3.1. Accountgegevens	47
7.3.2. Leden	48
7.3.3. Account-logboek	48
7.4. Automatiseringen & scènes	48
7.5. Resets	52
7.5.1. Fabrieksreset	52
7.5.2. Opnieuw opstarten (reboot)	52

7.5.3.	User-reset	52
7.5.4.	Netwerketset	52
7.6.	Bediening	53
7.6.1.	Inschakelen / uitschakelen	53
7.6.2.	Alarmen resetten	54
7.6.3.	Gedwongen ingeschakeld	55
7.7.	Verklaring van symbolen	56
7.8.	ABUS-cloud	57
7.9.	Opmerkingen over de harde schijf / SSD-geheugenopslag	58
7.10.	Onderhoud en service door installateurs	58
7.11.	Tabel met signaalsterktes van het draadloze netwerk	58
8.	Garantie	59
9.	Recyclen	59
10.	Conformiteit	59
10.1.	EU-conformiteitsverklaring	59
10.2.	Conformiteit aan EN 50131	59
11.	Bijlage	59
11.1.	Contact-ID-codetabel	59

1. Updates

1.1. Handleiding

Versie	Datum Publicatie	Wijzigingen
1.0	12.05.2026	Eerste versie
1.1	13.05.2026	Aanvullingen: - Nieuw: Hoofdstuk 1 Actualiseringen (voorheen hoofdstuk 7) - Hoofdstuk 3.2.6: Aanvulling: IP-camera's & MotionAlarm - Nieuw: Hoofdstuk 3.3 WLX Pro installatie & programmeren - Nieuw: Hoofdstuk 3.4.3 Camera-instellingen (globaal) - Nieuw: Hoofdstuk 3.4.4 Camera-instellingen (individueel) - Nieuw: Hoofdstuk 3.3.2 Camera's integreren via RTSP - Nieuw: Hoofdstuk 10.1 Contact-ID codetabel - Hoofdstuk 6.6.1: Ingeschakeld/uitgeschakeld WLX Pro-cilinder & wandlezer toegevoegd
1.2	30.06.2026	Aanvullingen: - Nieuw: Engelse, Franse en Nederlandse taalversies toegevoegd. - Release-opmerkingen voor Comfion Pro-firmware 1.0.2945 toegevoegd

1.2. Comfion Pro-firmware en release-opmerkingen

Firmware-versie	APP-Versie	Datum Publicatie	Wijzigingen
1.0.2864	2.1.96	12.05.2026	Eerste versie
1.0.2945	2.1.134	30.06.2026	Wijzigingen: - Aanpassing van de standaardwaarden van de FUBE80100 om de levensduur van de batterij te verlengen - Aanpassing van de ontwaaktijd van de FUBE80100 om de levensduur van de batterij te verlengen - Aanpassing van diverse logboekvermeldingen (toevoeging van gebruiker, gebied, enz.) - Aanpassing van de voorconfiguratie van de hybride module bij gebruik met wAppLoxx - Verbeteringen aan de H.265-videostream - Beveiligingsaanpassingen - Aanpassingen aan teksten en ontwerp Bugfixes: - Onvermijdelijkheid van WLX Access-componenten - Toestemmingsbericht „Toegang tot galerij“ bij het starten van de app - Correctie van beveiligingsinstellingen – sabotage van het alarmpaneel

De release-opmerkingen bij de huidige firmware-update vindt u in uw Comfion-app of via de volgende link:
<https://l.ead.me/bgjCEA>

2. Algemeen

2.1. Inleiding

Hartelijk dank dat u hebt gekozen voor het **Comfion Pro draadloze beveiligingssysteem**, een product van ABUS Security-Center (ook wel kortweg "ABUS" genoemd).

Deze handleiding bevat belangrijke beschrijvingen, technische gegevens, overzichten en meer informatie over de projectplanning, ingebruikname en bediening van het **Comfion Pro draadloze beveiligingssysteem**.

De hier beschreven producten/systemen mogen alleen worden geïnstalleerd en onderhouden door personen die gekwalificeerd zijn voor de betreffende taak. Gekwalificeerd personeel voor de installatie en het onderhoud van het systeem is in de regel een professionele ABUS-partner.

2.2. Beoogd gebruik / Wettelijk verplichte aanwijzingen

De verantwoordelijkheid voor het wettelijk conforme gebruik van het product ligt bij de koper of klant en de eindgebruiker. In overeenstemming met de aansprakelijkheid van de fabrikant voor zijn producten zoals gedefinieerd in de productaansprakelijkheidswetgeving, moet de bovenstaande informatie in acht worden genomen en worden doorgegeven aan exploitanten en gebruikers. Niet-naleving ontslaat ABUS Security Center van zijn wettelijke aansprakelijkheid.

Ongebruikelijk of ongewoon gebruik, reparatiewerkzaamheden of wijzigingen die niet uitdrukkelijk door ABUS zijn goedgekeurd en onjuist onderhoud kunnen storingen tot gevolg hebben en moeten worden vermeden. Wijzigingen die niet uitdrukkelijk door ABUS zijn toegestaan, leiden tot het verlies van aansprakelijkheid, garantie en speciaal overeengekomen garantie-aanspraken.

Architecten, technische gebouwplanners (TGA) en andere adviserende instellingen zijn verplicht alle benodigde productinformatie bij ABUS op te vragen om te voldoen aan de informatie- en instructieverplichtingen volgens de Wet Productaansprakelijkheid. Gespecialiseerde dealers en installateurs moeten de informatie in de ABUS-documentatie naleven en indien nodig doorgeven aan hun klanten.

Meer informatie is te vinden op www.abus.com op de algemene pagina of voor dealers en installateurs in het partnerportaal op <https://partner-asc.abus.com/>

2.3. Klantenservice / Customer Support

Neem voor verdere hulp contact op met ons Support-team: support@abus-sc.com

Algemene informatie over het **Comfion Pro draadloze beveiligingssysteem** is te vinden op onze homepage: <https://www.abus.com/de/Privat/Alarmsysteme/Comfion-Funk-System>

2.4. Impressum

Met de publicatie van nieuwere installatie-instructies verliest deze uitgave haar geldigheid.

Alle rechten voorbehouden. Niets uit deze installatiehandleiding mag in welke vorm dan ook gereproduceerd of vermenigvuldigd worden of verwerkt worden met elektronische, mechanische of chemische processen zonder schriftelijke toestemming van de uitgever.

ABUS Security Center aanvaardt geen aansprakelijkheid voor technische of druktechnische fouten en de gevolgen daarvan. De informatie in deze installatiehandleiding is naar eer en geweten samengesteld, rekening houdend met de huidige stand van de techniek. Zij worden regelmatig herzien en waar nodig bijgewerkt of gecorrigeerd.

Alle handelsmerken en industriële eigendomsrechten worden erkend, wijzigingen in het kader van de van technische vooruitgang kunnen zonder voorafgaande kennisgeving worden aangebracht.

2.5. Verklaring van symbolen

In deze installatiehandleiding worden de volgende symbolen gebruikt:

Symbol	Signaalwoord	Betekenis
	Opgelet	Duidt op een risico op letsel of gezondheidsrisico's door elektrische spanning
	Belangrijk	Duidt op mogelijke schade aan het apparaat/de accessoires of een risico op letsel of gevaren voor de gezondheid
	Aanwijzing	Geeft belangrijke informatie aan

3. Werkingsprincipe en eigenschappen

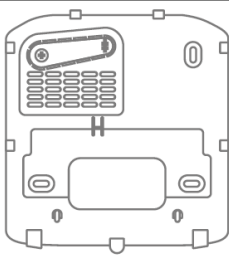
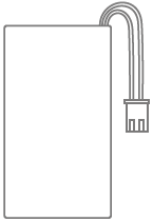
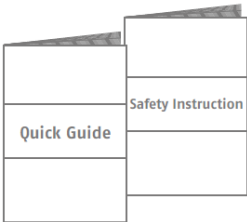
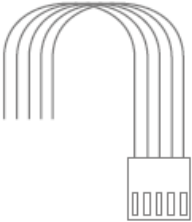
3.1. Productkenmerken

Het **FUAA85000 Comfion Pro draadloze veiligheidssysteem** is een inbraakalarmsysteem met EN-klasse 2-certificering en smart-home-functies. Het systeem kan worden ingesteld en bediend via de intuïtieve app of het ABUS Cloud-Portal.

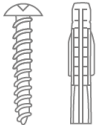
Belangrijkste kenmerken:

- Alles-in-één veiligheidssysteem: Alarmsysteem, video-NVR (tot 8 camera's) en toegangscontrole in één systeem - reduceert de diversiteit van apparaten en installatiekosten.
- Native integratie van wAppLoxx Pro: Direct in- en uitschakelen bij de deur – minder valse alarmen, betere acceptatie bij de eindklant.
- Perimeterwaarschuwing met buiten geïnstalleerde componenten: Vroegtijdige detectie van indringers - sneller ingrijpen en minder risico op inbraak.
- Geïntegreerde netwerkvideorecorder: Centrale opnames en beheer voor maximaal 8 camera's - videobeelden kunnen bij een alarm direct in de app worden bekeken en kunnen zonder extra NVR-recorder worden gerealiseerd.
- Besturing via apps en smart home-scenario's: Centrale bediening van alle componenten, flexibel configureerbare scenario's - ideaal voor individuele klanteneisen.
- Schaalbaar en sterk in projecten: Tot 160 draadloze componenten en 40 partities - met een grote draadloze reikwijdte tot 2.600 m in het open veld voor efficiënte planning van kleine objecten tot grotere projecten.
- Veilige 868-radio met AES128-bit encryptie: Dit zorgt voor een hoge mate van betrouwbaarheid van de transmissie, terwijl de bidirectionele radio veiligstelt dat het radiosignaal is aangekomen
- EN 50131 graad 2: Geschikt voor verzekeringsrelevante veiligheidseisen en professionele projecten.
- 4G mobiele-telefonie-back-up: Veilige alarmoverdracht, zelfs bij stroomuitval - verhoogde systeembeschikbaarheid.
- Bescherming tegen sabotage: Afbreekcontact & systeembewaking - betrouwbaar in het dagelijkse leven.
- Jamming-bewaking: Als een stoorzender wordt gedetecteerd, slaat Comfion Pro alarm.
- Een beveiligingsdienst inschakelen: Geïntegreerd meldkamerprotocol (SIA DC-09)
- Alle informatie altijd bij de hand: Meldingen optioneel via sms, e-mail of pushbericht

3.2. Leveringsomvang

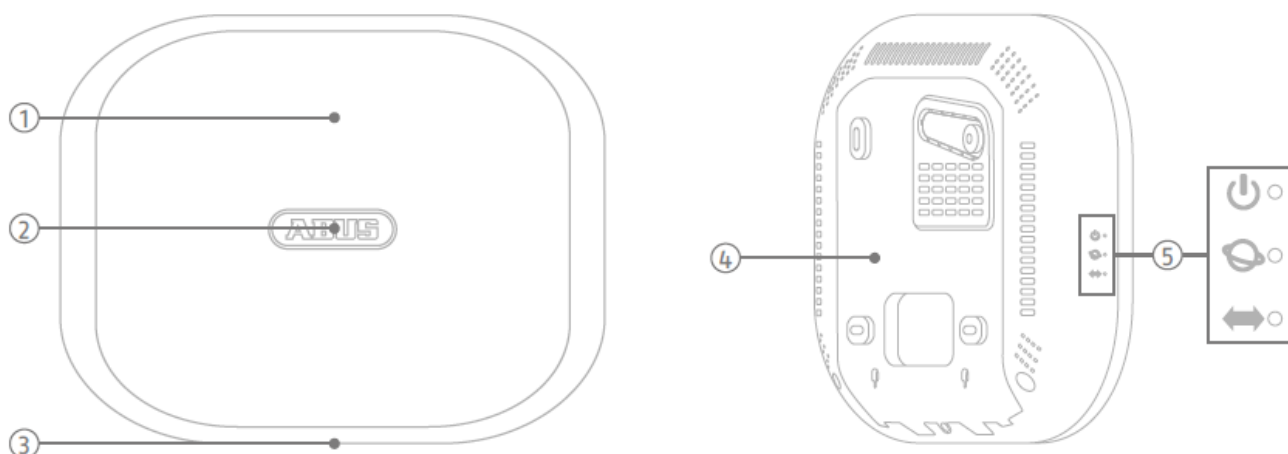
		
1 x centrale	1 x wandbeugel	1 x accu
		
Beknopte handleiding & veiligheidsinstructies	2 x kabel voor bedrade melders	4 x schroeven voor harde schijf
		
1 x openingsgereedschap		

Benodigd:


4 x schroeven / pluggen Ø 7,0 mm

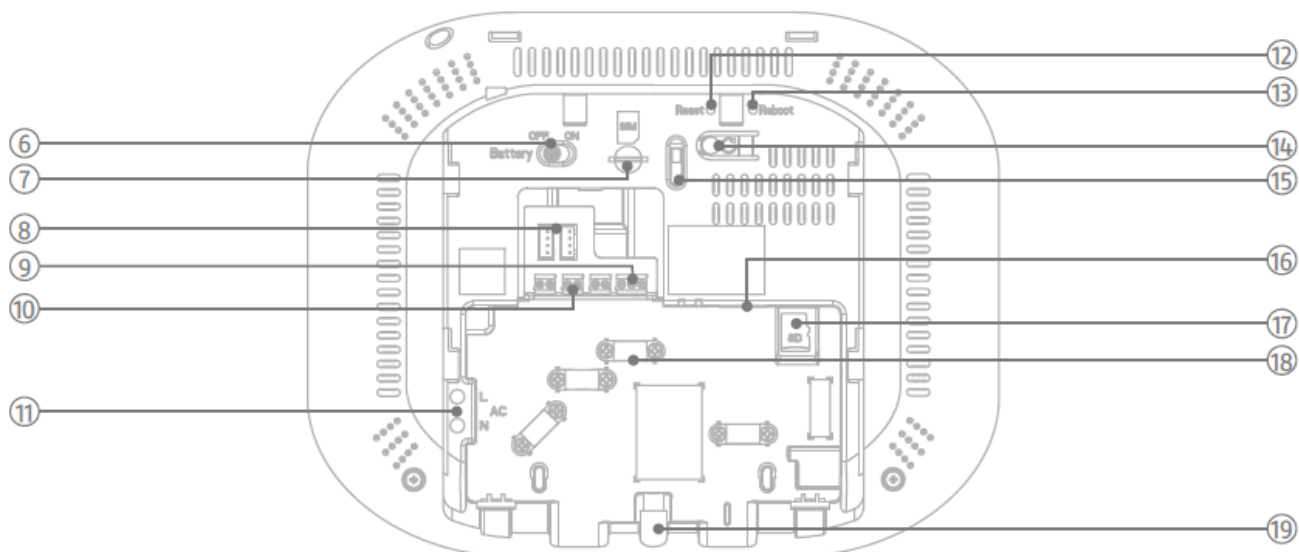
3.3. Beschrijving van het apparaat

Productopbouw (voorkant/achterkant)



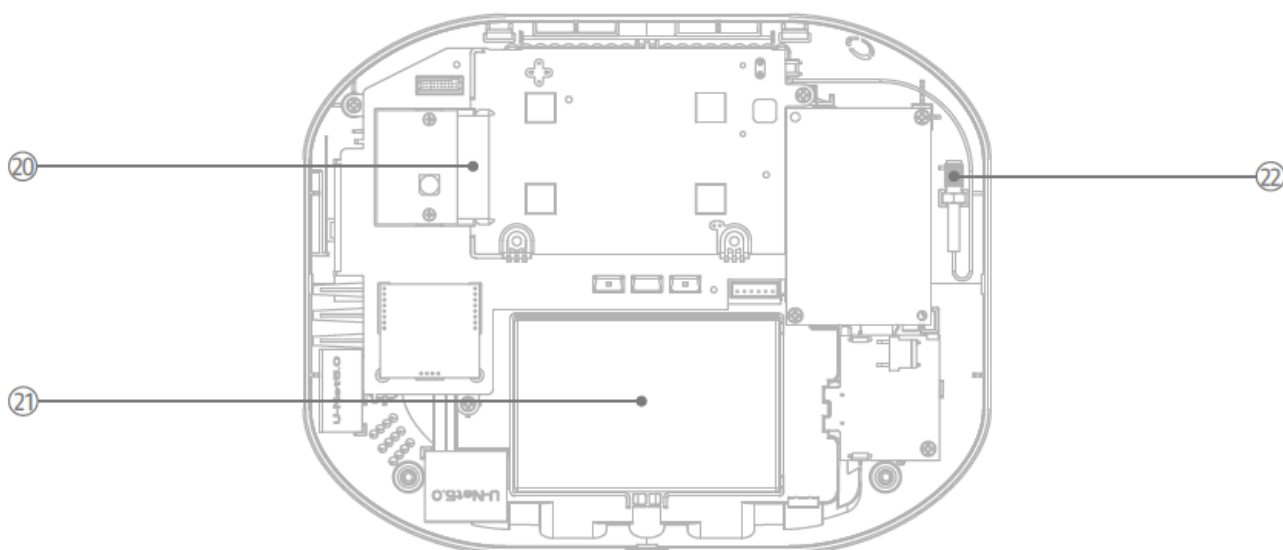
1 Deksel	2 Logo (alarmstatus)	3 Openingsmechanisme
4 Achterplaat	5 Status-LED's stroomvoorziening, internet, netwerk	

Achterkant (geopend)



6 Accuschakelaar	7 SIM-kaartsleuf (nano-SIM)	8 Bekabelde melderingangen
9 Relaisuitgang	10 BUS-klemmen	11 AC-aansluitklemmen (L/N)
12 Resettoets	13 Herstart-toets	14 Netwerkreset
15 Sabotageschakelaar	16 RJ45-aansluiting	17 MicroSD-sleuf
18 Trekontlasting	19 Bevestigingsschroef	

Voorzijde (geopend)



20 SATA-aansluiting voor SSD-schijf	21 Noodstroom-accu	22 Aansluiting externe antenne voor mobiele telefoon (SMA)
-------------------------------------	--------------------	--

Status-LED's

		  	
		Logo (alarmstatus) Status-leds	
Uitgeschakeld	Wit	Power-LED (boven)	
INGESCHAKELD	Blauw	Netspanning	Groen
Gedeeltelijk scherp	Blauw	Batterijvoeding	Rood
Alarm	Rood (knipperen)	Firmware-update	Geel (knipperen)
Sabotage centrale	Rood (knipperen)	Internet-LED (midden)	
Inleesprocedure	Groen (knipperen)	Online & Admin geregistreerd	Groen
Onderhoudsmodus	Violet	Online & Admin niet geregistreerd	Groen (knipperen)
Storing	Oranje (knipperen)	Offline	Rood
		Netwerk-LED (onder)	
		LAN	Groen
		3G/4G mobiele telefonie	Rood

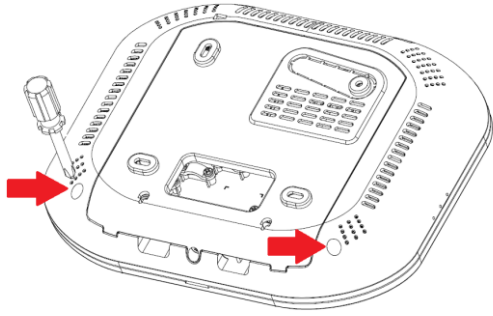
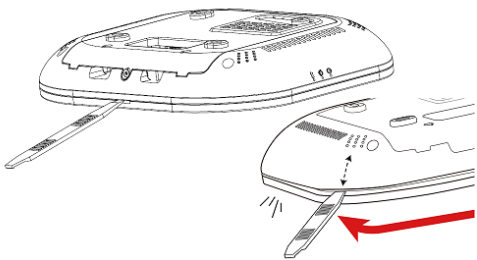
3.4. Technische gegevens

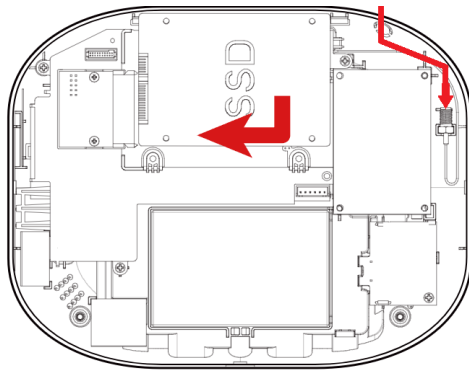
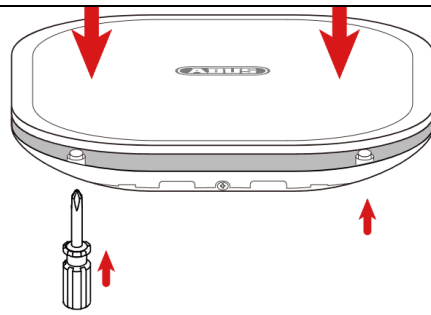
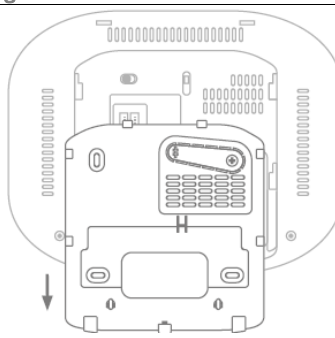
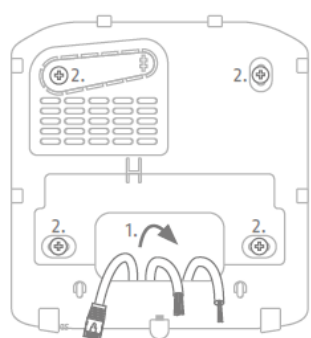
Afmetingen (bxhxd)	242 x 190 x 45 mm
Gewicht	950 g (inclusief back-up-accu)
Bedrijfstemperatuur	-10 °C tot +40 °C
Milieuklasse	II (EN 50131-1 + A3:2020)
Bescherming tegen omgevingsinvloeden	IP40 / IK06
Luchtvochtigheid	max. 85% RL (relatieve luchtvochtigheid)
Aansluitingen	L/N-aansluiting (230 volt), RJ45 (LAN), SATA 3.0-aansluiting (voor 2.5" SSD), SIM-kaartsleuf (nano-SIM), micro-SD-kaartsleuf
In-/uitgangen	4 ingangen voor meldergroepen (NO/NC), potentiaalvrij (Bedradingswijze: 2-draads CC, EOL, DEOL) 1 relaisuitgang (NO/NC/COM) max. 30 V DC / 1,6 A
BUS-interface	(GND / +V / B / A) 13,0 V kabellengte max. 200 m
Indicaties	Status-LED (voeding, internet, communicatie) ABUS-logo (systeemstatus)
Toetsen	Herstarttoets, resettoets, netwerkrestart, accu-schakelaar
Radiofrequentie / modulatie	868.0 - 868.6 MHz / GFSK
Vermogen, radio / bereik	max. 25 mW (14dBm) / 1000m, vrij veld
Aantal draadloze componenten	160
Aantal partities	40
Aantal gebruikers	51
Aantal gebeurtenissen	> 10.000
Netwerkrecorder	Max. 8 kanalen @ 2048 Kbps, bij gebruik van 4 kanalen @ 4096 Kbps Voorbeeld: 4 kanalen van 4K (3840 x 2160) + 4 kanalen van 1080p (1920 x 1080)
Communicatie	Ethernet 1 GbE LAN SSL/TLS Mobiel netwerk (back-up): 3G UMTS / 4G LTE SMS & spraak: 2G GSM / 4G LTE
AÜA-categorie	SP5 (LAN) SP2 (GSM) DP3 (LAN + GSM)
Stroomvoorziening	Primair: AC 230V / 50Hz Secundair: LiPo-accu 7,4V / 6.000mAh
Type voeding	Type A, voeding in overeenstemming met EN50131-1+A3:2020 en EN50131-6+A1:2021
Buffertijd - accubedrijf	> 12 uur volgens EN 50131-1+A3:2020, graad 2
Sabotagebescherming (herkenning / bescherming)	ja (1x wandafbreekcontact)
Supervisietijd	900 - 3600 s (standaardinstelling: 3.600 s)
Veiligheidsgraad	Klasse 2 (EN 50131-1 + A3:2020)
Conformiteit	Veiligheidsniveau 2 bij correcte installatie conform EN 50131-1+A3:2020, EN 50131-3:2009 en EN 50131-5-3:2017
EU-richtlijnen	RED: 2014/53/EU RoHS: 2011/65/EU + 2015/863 Algemene veiligheid: 2001/95/EG

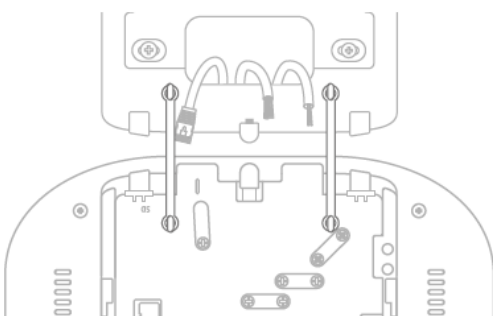
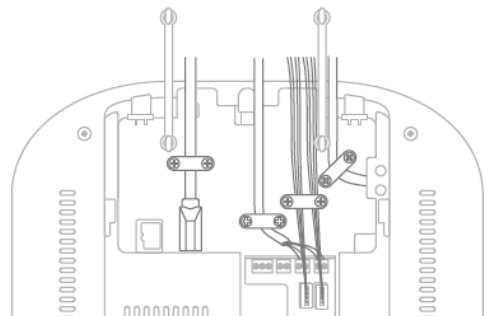
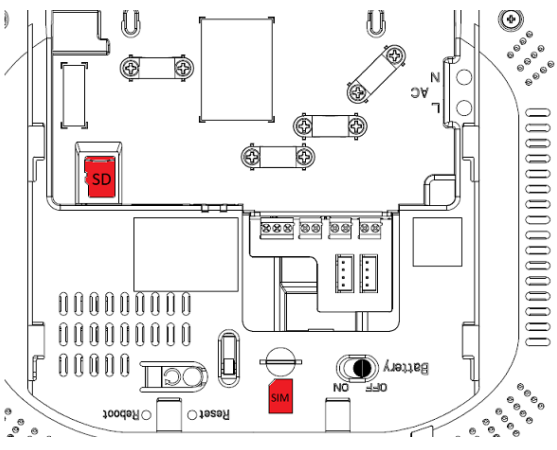
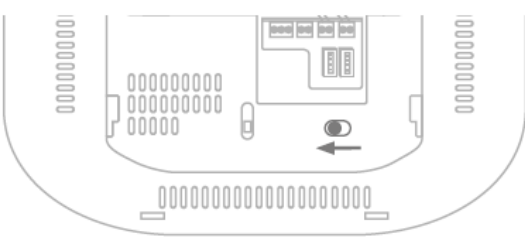
4. Montage en ingebruikname

4.1. Wandmontage van de centrale

 Opgelet	LET OP: VÓÓR INSTALLATIE VAN DIT SYSTEEM MOET U ERVOOR ZORGEN DAT DE STROOMTOEVOER NAAR DE ALARMCENTRALE GESCHIEDEN EN ONDERBROKEN IS. (Zorg er ook voor dat de accuschakelaar op "Off" staat.) Alle elektrische aansluitingen moeten worden uitgevoerd door een gekwalificeerde elektricien en moeten voldoen aan de geldende plaatselijke voorschriften.
 Opgelet	LET OP: Als het apparaat op het elektriciteitsnet wordt aangesloten terwijl er spanning op staat, staat de netspanning ook op de ommantelde koppen van de schroefklemmen van de netaansluiting. LET OP: Het netsnoer naar de alarmcentrale moet voorzien zijn van een tweepolige scheidingsinrichting conform EN 62368-1. Let op: Als u de printplaat in de alarmcentrale aanraakt, moet u de gebruikelijke voorzorgsmaatregelen nemen om schade door statische elektriciteit te voorkomen.
 Aanwijzing	- Monteer de centrale aan de wand op een hoogte van ongeveer 1,5m - Houd aan alle kanten een afstand van minimaal 1,5 m aan ten opzichte van de volgende apparaten: Elektrische apparaten, metalen voorwerpen of apparaten met radio-emissies (bijv. routers, magnetrons) - aangezien deze de radioprestaties van het systeem kunnen beïnvloeden.

Bevestiging van de harde schijf / SSD-opslag en externe mobiele antenne (niet meegeleverd)	
Open het deksel van de centrale. Draai hiervoor de 2 schroeven aan de achterkant los.	
Maak het deksel los met behulp van het meegeleverde gereedschap.	

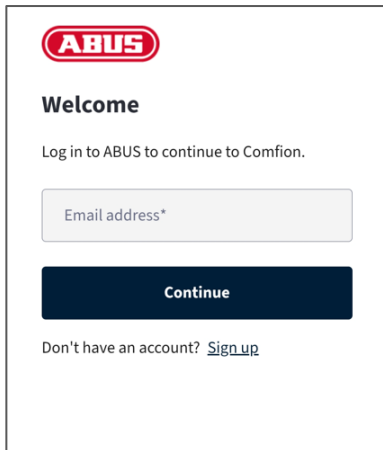
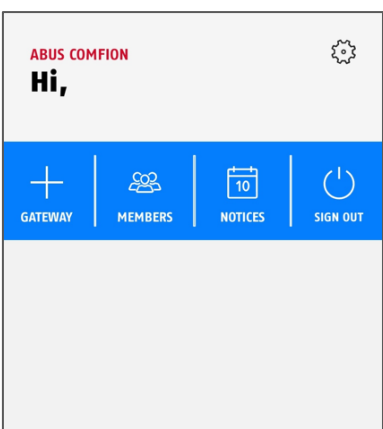
Harde schijf / SSD-schijf: (niet meegeleverd) Sluit de 2,5-inch SSD-schijf aan op de daarvoor bestemde insteekaansluiting (SATA 3.0) en fixeer de schijf met de meegeleverde schroeven. Externe mobiele antenne: (niet meegeleverd) Voer de aansluitkabel door de daarvoor bestemde opening en schroef deze vast op de SMA-bus. Aanbevolen accessoires bij ABUS: TVAC41210 - 1 TB 2,5-inch SSD-schijf SATA WD Red TVAC41220 - 2 TB 2,5-inch SSD-schijf SATA WD Red FUZU85000 - Ext. mobiele antenne voor Comfion Pro  Aanwijzing Formateer de harde schijf in het exFAT- of NTFS-formaat voordat u deze plaatst.  Aanwijzing De 2,5-inch harde-schijf-sleuf maakt het mogelijk om zowel HDD-schijven als SSD-schijven te gebruiken. Bij gebruik van een SSD-opslagmedium wordt voldaan aan de eisen van EN 50131 (noodstroomduur).	
Bevestig het deksel zodat het hoorbaar vastklikt en draai de schroeven aan de achterzijde vast.	
Wandmontage en bekabeling	
Draai de bevestigingsschroef (onderaan in het midden) los en trek de achterplaat van de centralebehuizing.	
 Let op: Zorg ervoor dat de stroomtoevoer (netsnoer) uitgeschakeld en geïsoleerd is! 1. Voer alle benodigde aansluitkabels door de kabeldoorvoer van de montageplaat van de centrale. 2. Bevestig vervolgens de montageplaat aan de muur.	

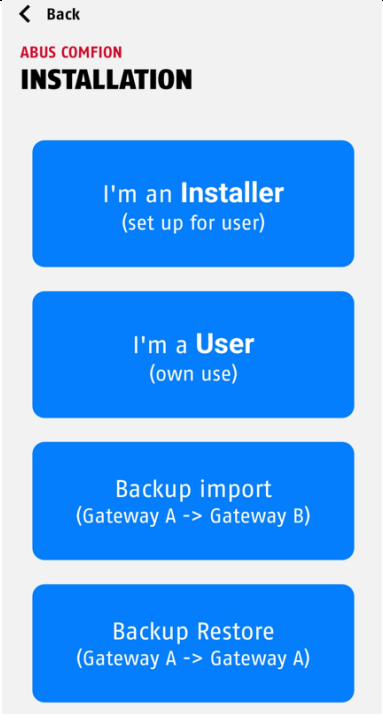
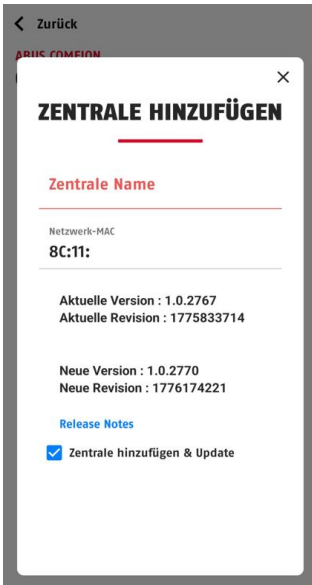
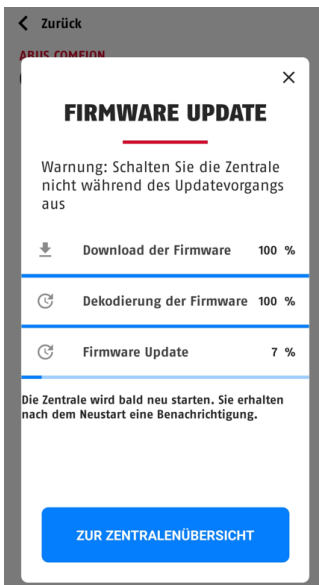
Hang de houderzekeringen van de centrale (2 houderkabels) in de voorzieningen aan de achterplaat in.							
Voer de aansluitkabels in de centrale in • Sluit het netsnoer aan op de L/N-klem. • Sluit de ethernet-kabel aan op de RJ45-aansluiting • Sluit indien nodig de buskabel en de bedrade melders enz. aan op de daarvoor bestemde klemmen. • Meer informatie over het aansluiten van bedrade melders en busapparaten vindt u in de hoofdstukken 3.2.5 en 3.2.6 Zet alle aansluitkabels vast met de trekcontlastingen.							
Steek indien nodig een micro-SD-kaart (max. capaciteit 512 GB) en/of een simkaart (nano-sim) in de daarvoor bestemde sleuven tot ze hoorbaar vastklikken. (Kaarten niet inbegrepen)  Aanwijzing Formateer uw SD-kaart in het exFAT- of NTFS-formaat voordat u deze plaatst.							
Schakel nu de stroomtoevoer in. De centrale voert nu het opstartproces uit.							
Zet de accuschakelaar op "ON" Nadat het opstarten is voltooid, branden de status-leds als volgt: <table border="0"> <tr> <td></td> <td>Voedings-LED: Groen (netspanning)</td> </tr> <tr> <td></td> <td>Internet-LED: Groen (knippert) (Online & admin niet geregistreerd)</td> </tr> <tr> <td></td> <td>Netwerk-LED: Groen (LAN)</td> </tr> </table>		Voedings-LED: Groen (netspanning)		Internet-LED: Groen (knippert) (Online & admin niet geregistreerd)		Netwerk-LED: Groen (LAN)	
	Voedings-LED: Groen (netspanning)						
	Internet-LED: Groen (knippert) (Online & admin niet geregistreerd)						
	Netwerk-LED: Groen (LAN)						

4.2. Inbedrijfstelling van het systeem

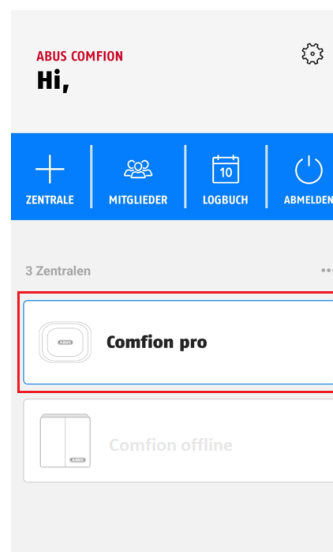
4.2.1. Installatie via de app & afronding van de hardwarevoorbereidingen

 Aanwijzing	De eerste inbedrijfstelling van de Comfion Pro-centrale en daarmee de koppeling met het partnerportaal en de bijbehorende installateur moet via de app plaatsvinden.
---	--

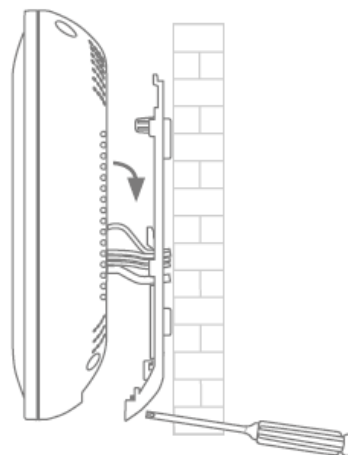
Download de Comfion-app vanuit uw app-store op uw smartphone of tablet (iOS of Android) Volg de instructies in de app tot u bij de inlogpagina komt	
Log in met uw ABUS Single Sign-On gegevens (partnertoegang) Als u nog geen toegang hebt, kunt u onder 'Registreren' een gratis account aanmaken.	
Na het inloggen ziet u het overzicht van het centrale. Voeg een nieuw centrale toe met de Plus-knop.	

Kies "Ik ben een installateur" wanneer u de installatie voor een klant in gebruik neemt. Hierdoor wordt de gebruiker aangemaakt in de rol van installateur. Als u de installatie zelf uitvoert, selecteert u 'Ik ben een gebruiker'. Hiermee wordt u geregistreerd in de rol van Admin met installateurs- en beheerdersrechten. Aanwijzing Als installateur kunt u gebruikers aanmaken, maar u verliest deze bevoegdheid zodra u een admin-gebruiker (eigenaar) uitnodigt. Meer informatie vindt u in hoofdstuk 4.1. (Gebruikersrollen) en hoofdstuk 4.2 (Inbedrijfstelling) Meer informatie over "Back-up importeren" en "Herstellen" vindt u in hoofdstuk 6.1.7 (Back-up)	
Aanwijzing Let erop dat de centrale met het internet is verbonden. Zodra de status-LED 'Internet' groen knippert, kunt u het koppelingsproces in de app starten. Scan hiervoor de QR-code met het opschrift "Pairing-code"	
Wijs een naam voor de centrale toe en bevestig deze. De installatie start nu een firmware-update voordat u toegang krijgt tot de installatie. De firmware-update kan enkele minuten duren en houdt in dat de centrale opnieuw wordt opgestart. Tijdens de update knippert de Power-LED geel.	 

Nadat de centrale opnieuw is opgestart, is deze in het centrale overzicht niet langer grijs weergegeven en kan deze worden geopend door erop te klikken.



Maak de mechanische vergrendeling los van de achterplaat en voer de houderkabel naar binnen. Plaats de centrale in de achterplaat, schuif deze naar beneden en schroef de centrale vast aan de achterplaat.



Aanwijzing

Na de installatie en inbedrijfstelling wordt er een sabotagealarm geactiveerd wanneer de centrale van de wandhouder wordt verwijderd of het deksel van de behuizing wordt geopend. Voer alleen noodzakelijke werkzaamheden aan de hardware uit als de onderhoudsmodus is geactiveerd (*Centrale-configuratie -> Beveiligingsinstellingen*)

4.2.2. Dashboard (na eerste aanmelding)

Kopbalk:

- Configuratie & gebruikersinstellingen
- **Installateur** Gebruikersrol (alleen installateur)
- Firmware-update (indien beschikbaar)
- Paniek-alarm activeren

Dashboard / Functiebereik

- Hotkey-knoppen (indien ingesteld)
- Previewbeelden van de camera (indien ingesteld)
- Overzicht van de partities (binnenruimte, buitenschil is standaard ingesteld en kan worden uitgebreid met andere partities, zie: 3.2.3 Partities)
 - Klik op ▼ om de toegewezen componenten en hun status weer te geven (indien geconfigureerd)

Navigatiebalk

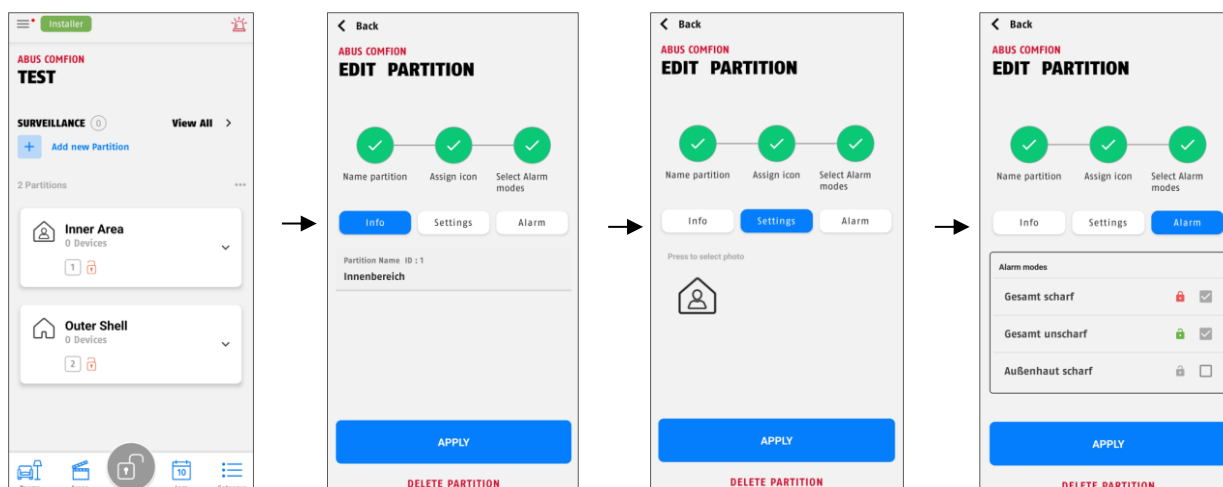
- Ruimtes (& componentenlijst) zie 3.2.4 en 3.2.5
- Scenario's (scènes en automatiseringen) zie 6.4
- Alarmmodi (slotpictogram) – zie 3.2.8
- Logboek (lijst van gebeurtenissen & filterfunctie)
- Centrales (overzicht) – zie 6.3

Een kant-en-klare dashboardweergave vindt u in **hoofdstuk 6.2 Dashboard**

4.2.3. Partities

Partities bieden u de mogelijkheid om het te bewaken object op te delen en om het gedifferentieerd in en uit te schakelen. In combinatie met de alarmmodi kunt u partities samen of afzonderlijk schakelen.

In de toestand af fabriek bestaat de installatie uit twee partities: de buitenschil en de binnenruimte. U kunt deze velden bewerken door hier lang op te drukken.

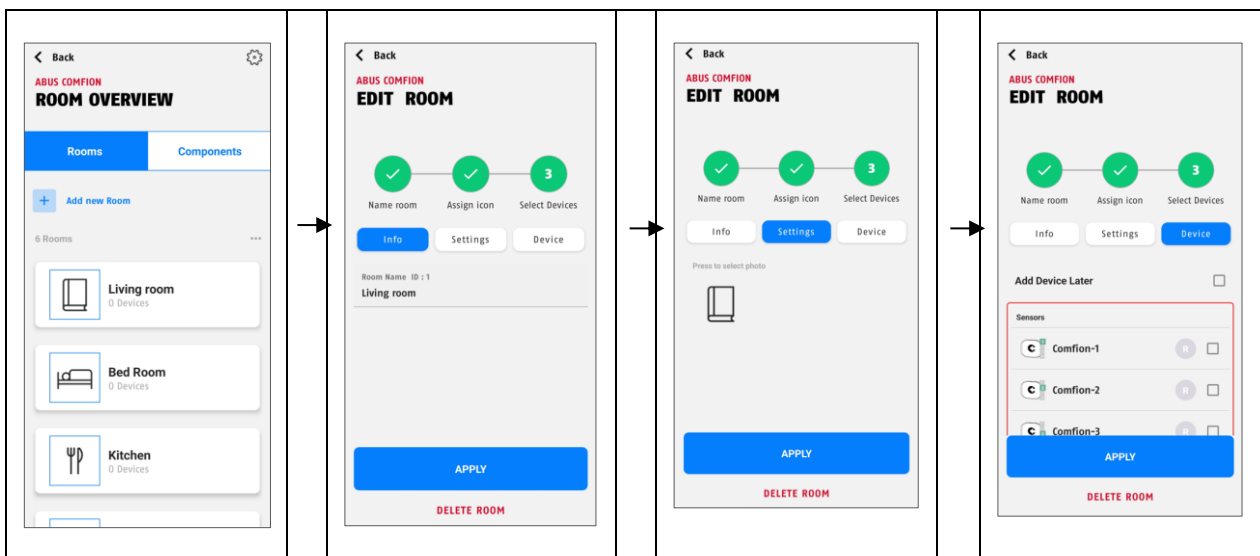


U kunt extra partities aanmaken door op de knop "Partitie toevoegen" te klikken.

4.2.4. Ruimtes

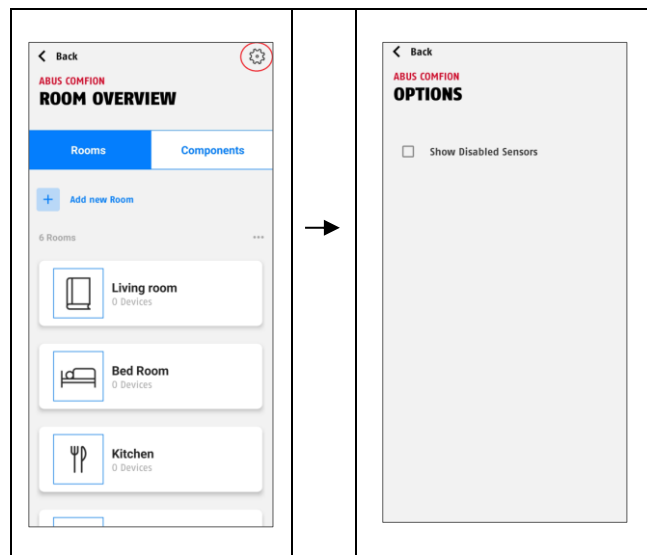
Vanuit het dashboard kunt u via de navigatiebalk naar het gedeelte "Ruimtes" gaan om de configuratie van ruimtes en componenten te verrichten. Met het draadloze Comfion Pro-beveiligingssysteem kunt u uw componenten aan ruimtes toewijzen. Dit dient om de identificatie van componenten te vereenvoudigen en heeft geen functionele eigenschappen. Ruimtes zijn niet toegewezen aan partities, wat betekent dat u componenten van verschillende partities in één ruimte kunt hebben.

In de fabrieksstatus heeft het systeem een aantal vooraf gedefinieerde ruimtes. U kunt deze ruimtes vrij bewerken of helemaal verwijderen. U kunt deze partitie bewerken door deze knop lang ingedrukt te houden.



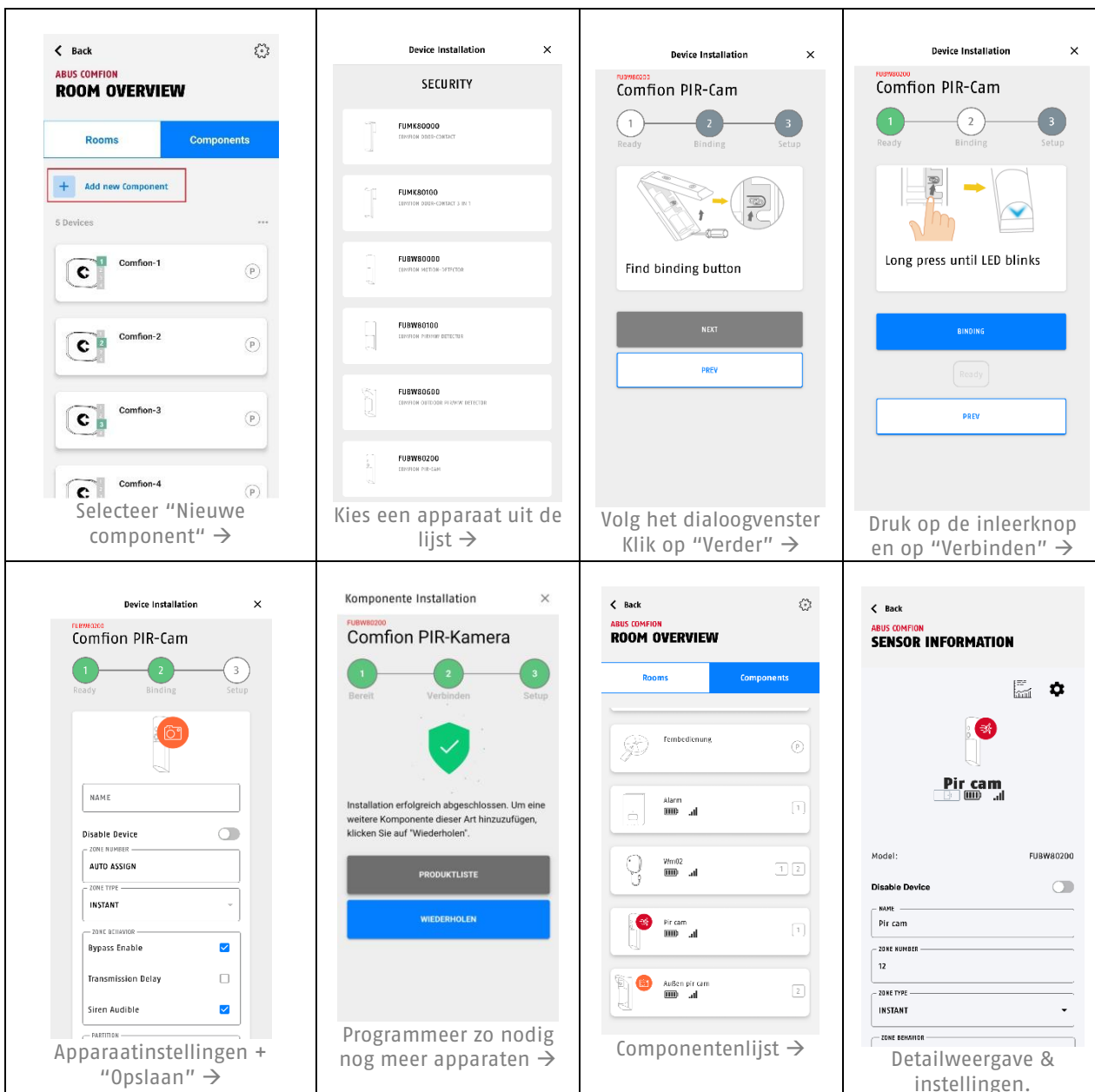
In het ruimteoverzicht kunt u via het tandwiel pictogram rechtsboven in het scherm de instelling "Gedeactiveerde componenten weergeven" in- of uitschakelen. (deze optie is standaard uitgeschakeld)

Als deze optie geactiveerd is, worden uitgeschakelde componenten in het dashboard onder de ruimtes en in de componentenlijst weergegeven.



4.2.5. Componenten

Vanuit het ruimteoverzicht gaat u naar het componentenoverzicht. Door op "Nieuwe component" te klikken, kunt u uw Comfion-componenten aan het systeem toevoegen.



Door op een reeds geprogrammeerde component te klikken, kunt u deze bewerken en de volgende apparaatinstellingen aanpassen:

Component deactiveren	UIT: (Voorinstelling): Het apparaat functioneert normaal AAN: Het apparaat wordt gedeactiveerd (werkt niet)
Naam	Toewijzing van een naam aan de component
Zonenummer	Toewijzing van het zonenummer (wordt automatisch gedaan door het systeem)
Zonetyp	- Ingang -> activeert een ingangsvertraging, waarna een inbraakalarm wordt geactiveerd - Uitgang -> kan open zijn tijdens de uitgangsvertraging, functioneert als een directe zone na inschakelen - Ingang/Uitgang -> gebruikt een ingangs- en uitgangsvertraging - Na de ingang -> Melder reageert als een directe partitie, tenzij daarvoor een ingangsvertraging is geactiveerd. Dit kan in de veiligheidsinstellingen

	<i>tot hetzelfde partitie worden beperkt.</i> • Direct (inbraak) -> <i>activeert een inbraakalarm wanneer het systeem ingeschakeld is</i> • Perimeterwaarschuwing -> <i>partitietype voor buitenmelders. Activeert het evenement, inclusief logboekvermelding en melding. Geen akoestische alarmering.</i> • Direct (bewaakt) -> <i>werkt als de directe zone wanneer het systeem ingeschakeld is; wanneer het systeem uitgeschakeld is, wordt een melding verzonden wanneer dit wordt geactiveerd</i> • 24-uurs inbraakalarm -> <i>Inbraakalarm, ongeacht de status van het systeem</i> • 24-uurs wateralarm -> <i>Wateralarm ongeacht de status van de installatie</i> • 24-uurs brand -> <i>Brandalarm ongeacht de status van de installatie</i> • 24 uur sabotage -> <i>Sabotagealarm, ongeacht de status van de installatie</i> • Sluitingsbewaking -> <i>Een open partitie voorkomt dat het systeem wordt ingeschakeld, maar activeert geen alarm</i>
Ingangstijd/uitgangstijd	• Voor de zonetypes 'Ingang', 'Uitgang' en 'Ingang/Uitgang' kan een vertragingstijd in seconden worden ingesteld (5 tot 180 seconden) • Standaardinstelling 10 s (ingangsvertraging) / 30 s (uitgangsvertraging)
Zonegedrag	• Kan worden overbrugd: <i>Als de partitie bij het inschakelen wordt geactiveerd, heeft u de mogelijkheid om dit te overbruggen</i> • Verzendingsvertraging: <i>Als deze optie is ingeschakeld, wordt de melding van zone-alarmen met de geprogrammeerde tijd vertraagd.</i> • Activering sirene: <i>Deze melder stuurt de in de partitie geïntegreerde sirenes aan</i>
Partitie	• Het apparaat kan aan één of meerdere partities worden toegewezen. -> Deze toewijzing zorgt er in combinatie met het zonetype voor dat er een alarm wordt geactiveerd.
Ruimte	• Het apparaat kan aan een ruimte worden toegewezen. • "Later toewijzen" betekent dat het apparaat nog niet aan een ruimte is toegewezen.
Looptest starten (bewegingsmelder)	• Als u op 'Looptest starten' klikt, begint een tijdvenster van 1 minuut waarin het apparaat moet worden geactiveerd. • De looptest kan worden afgebroken door op 'Stop' te klikken. • Bij activering begint het tijdvenster (de stilteperiode van de melder) opnieuw. • Bij combinatiesensoren (bijv. PIR + microgolf) kunnen de sensoren afzonderlijk of samen worden getest.
Start RF Signaalsterkte test (Draadloze componenten)	 Controleer de signaalsterkte voordat u de component monteert en gebruik bij twijfel een repeater. Een overzicht voor het beoordelen van de signaalsterkte vindt u in hoofdstuk 6.11 Aanwijzing • Klik op "Signaalsterketest starten" en activeer het apparaat. • Bij sensoren met meerdere functies (bijv. PIR + microgolf) kan elke sensor afzonderlijk worden getest.
Camerafuncties (alleen camera's)	• MotionAlarm Uit/Aan (standaardinstelling: Uit); "Aan" activeert een alarm als de camera aan een partitie is toegewezen.
Opslaan	• Klik op 'Opslaan' om de wijzigingen in de instellingen toe te passen.

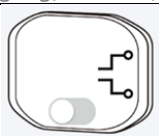
 Aanwijzing	Als een melder is geprogrammeerd voor het zonetype uitgang of ingang/uitgang, controleert het systeem de status van de melder pas nadat de vertragingstijd is verstreken bij ingeschakeld systeem. - Als de melder niet gereed is na het verstrijken van de tijd en "overbrugbaar" is geactiveerd, wordt de melder automatisch overbrugd na de vertragingstijd en wordt het systeem ingeschakeld. - Als de melder niet gereed is nadat de tijd is verstreken en "overbrugbaar" is gedeactiveerd, dan wordt het systeem niet ingeschakeld.
--	---

 Aanwijzing	Een gedetailleerd overzicht van de symbolen in de componentenlijst vindt u in hoofdstuk 6.7 (Uitleg bij de symbolen)
--	--

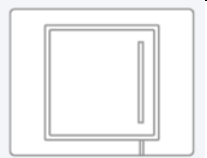
4.2.6. Instellingen voor componenten

In de component-instellingen & rechts boven het apparaatpictogram kunt u door te klikken op het tandwiel  gedetailleerde instellingen voor de component aanpassen. Raadpleeg de installatiehandleiding van de betreffende component voor meer informatie. Hieronder vindt u de instellingen voor de Comfion Pro-centrale FUAA85000, de Comfion Pro BUS-WLX-module BUM080000 en IP-camera's

Comfion Pro-centrale FUAA85000

Symbol	Benaming	instelmogelijkheid	Uitleg
 (per ingang, d.w.z. 1, 2, 3, 4)	Draadmodus	2-draads CC / EOL / DEOL (voorinstelling CC)	Bedradingswijze van de ingangen van de meldersgroepen
	NC of NO	Normally Open / Normally Closed (Voorinstelling: NO)	Rusttoestand van het relais, d.w.z. open of gesloten
	Logo display	Altijd uit / Altijd aan / Brandt (voorinstelling Aan)	Schakelt de verlichting van het logo permanent uit, permanent aan, of 10 sec. aan (flitst) bij een statuswijziging
	Ingeschakeld-kleur Uitgeschakeld-kleur Gedeeltelijk-ingeschakeld-Kleur	Kleurenmatrix	De kleur van de verlichting aanpassen door op het kleursymbool te klikken

Comfion Pro WLX Pro-module BUM080000 en WLX Pro-sluitmedia

Symbol	Benaming	instelmogelijkheid	Uitleg
 (BUS-WLX-module)	Resetten naar fabrieksinstellingen	Uitvoeren	Reset van de draadloze WLX-Pro-module. Let op: alle sluitcilinders en wandlezers moeten daarna opnieuw worden geprogrammeerd! (de BUS-WLX-module blijft geprogrammeerd!)
 Sluitcilinder (Access / Intrusion)	Supervisietijd	4 – 720 min (Voorinstelling: 720)	Regelmatige controle van de draadloze communicatie met het ingestelde interval.
	onvermijdelijkheid (alleen Access)	Uit / Aan (Voorinstelling: aan)	Als de schakelaar op "Aan" staat, wordt er geen toegang verleend wanneer de Comfion Pro is ingeschakeld.
	Openingstijd	6 sec. / 12 sec. (voorinstelling 6 sec.)	Definiëert de in- en uitschakelperiode van de cilinder voor het openen van de deursluis
 Wandlezer (Access / Intrusion)	Supervisietijd	4 – 720 min (Voorinstelling: 720)	Regelmatige controle van de draadloze communicatie met het ingestelde interval.
	onvermijdelijkheid (alleen Access)	Uit / Aan (Voorinstelling: aan)	Als de schakelaar op "Aan" staat, wordt er geen toegang verleend wanneer de Comfion Pro is ingeschakeld.
	Openingstijd	6 sec. / 12 sec. (voorinstelling 6 sec.)	Definiëert de in- en uitschakelperiode van de cilinder voor het openen van de deursluis

IP-camera's

Symbol	Benaming	instelmogelijkheid	Uitleg
 (IP-camera)	Camerafunctie "Bewegingsalarm"	Uit/Aan (Voorinstelling: Uit)	Bewegingsdetectie gebruiken om een alarm te activeren. Aanwijzing: Er zijn nog meer instellingen nodig, onder andere in de camera-configuratie. Zie hoofdstuk 3.4.4

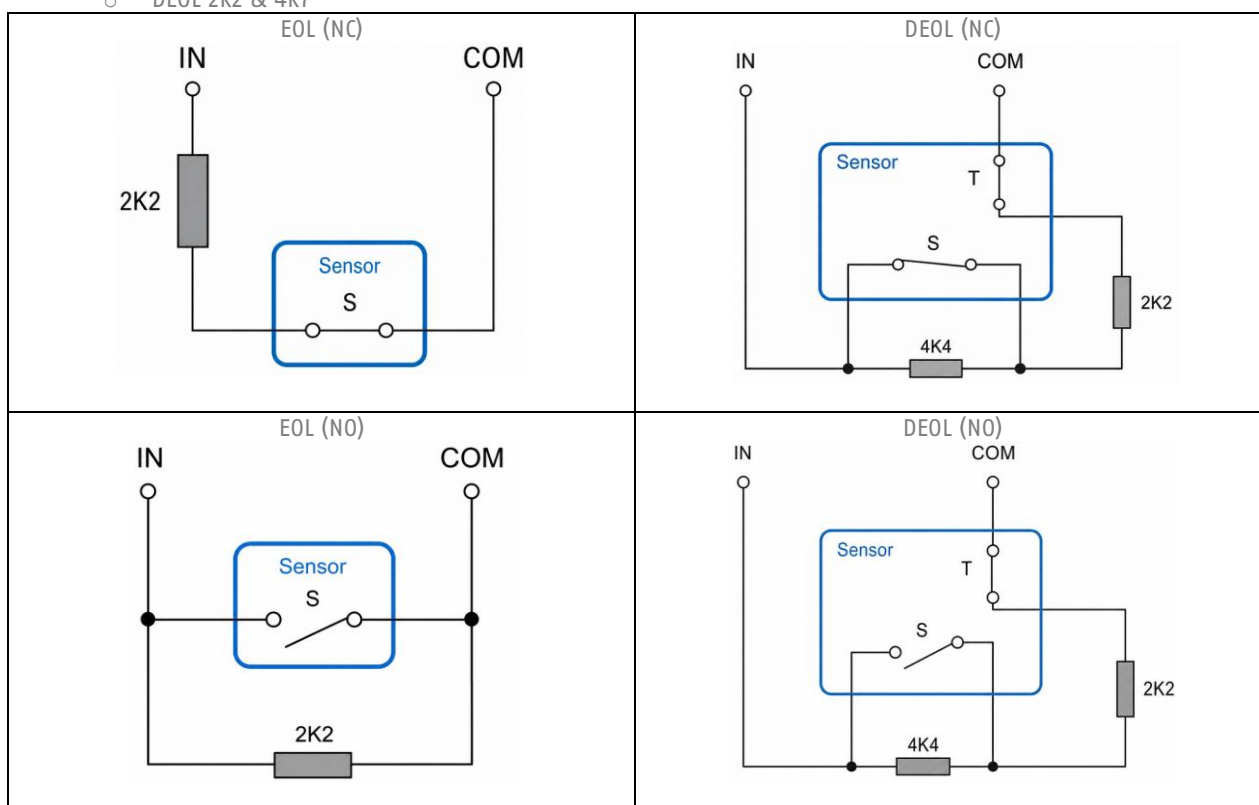
4.2.7. Aanwijzingen voor de bedrading (ingangen/uitgangen/BUS)



De Comfion Pro-centrale beschikt over verschillende aansluitmogelijkheden voor maximaal 4 bedrade melders (8), een relaisuitgang (9) en een RS485-businterface (10).

Bekabelde melderingangen

- Gebruik de meegeleverde adapterkabels van 30 cm met open uiteinden. De kabelparen zijn per ingang met een kleur gemarkeerd.
- In de apparaatinstellingen van de Comfion-app stelt u per ingang de bedradingsmodus (2-draads CC, EOL of DEOL) in, evenals de ruststand NO/NC.
- Voor de bewaakte weerstandsbedrading zijn de volgende weerstandswaarden vastgelegd:
 - EOL: 2k2
 - DEOL 2k2 & 4k7



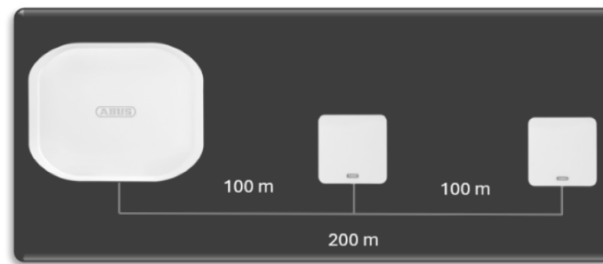
Relaisuitgang

- De relaisuitgang is spanningsvrij. Sluit de uitgang aan op massa en, indien nodig, op de klem NO (open contact) of NC (gesloten contact). max. 30 V DC & max. 1,6 A

RS485-businterface

- De Comfion Pro beschikt over een 4-draads RS485-businterface (GND / +V / B / A), 13,0 V, voor het aansluiten van maximaal 2 busdeelnemers (**Comfion Pro BUS-WLX-module BUM080000**)
- U kunt apparaten ofwel in serie ofwel parallel aansluiten op de Comfion Pro-centrale.
- De maximale kabellengte bedraagt 200 m en kan bij gebruik van 2 apparaten flexibel worden verdeeld:

- Voorbeeld:



- Aanbevolen kabel: Twisted-pair-kabels (afgeschermd en getwist), bijvoorbeeld: RS485/DMX-kabel of CAT5e- of CAT6-kabel.

 Belangrijk	Houd bij de installatie van de Comfion Pro-centrale en de BUS-WLX-module, en ook ten opzichte van andere elektrische apparaten, antennes en metalen, een minimale afstand van 1,5 meter aan om storingen in de draadloze communicatie (bijv. vertragingen of signaalverlies) te voorkomen!
--	---

4.2.8. Alarmmodi

Het Comfion Pro draadloze beveiligingssysteem werkt met zogenaamde "alarmmodi", die de kern van het systeem vormen. Dit zijn in- en uitschakelbare koppelingen tussen partities en gebruikers.

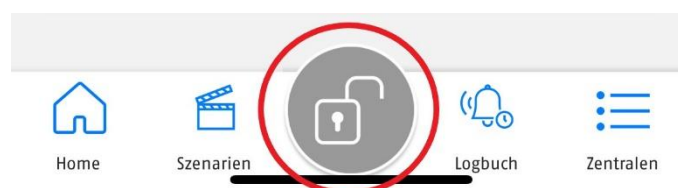
In een alarmmodus bepaalt u welke gebruiker welke partitie daarmee in- of uitschakelt. Dit kan worden gebruikt om alle mogelijke scenario's voor het inschakelen en uitschakelen af te beelden.

In de praktijk voert een gebruiker bij het in- of uitschakelen in werkelijkheid een alarmmodus uit.

 Aanwijzing	Het Comfion Pro draadloze beveiligingssysteem heeft in de fabrieksinstellingen drie vooraf geconfigureerde alarmmodi: "Volledig ingeschakeld", "buitenschil ingeschakeld" en "volledig uitgeschakeld".
--	---

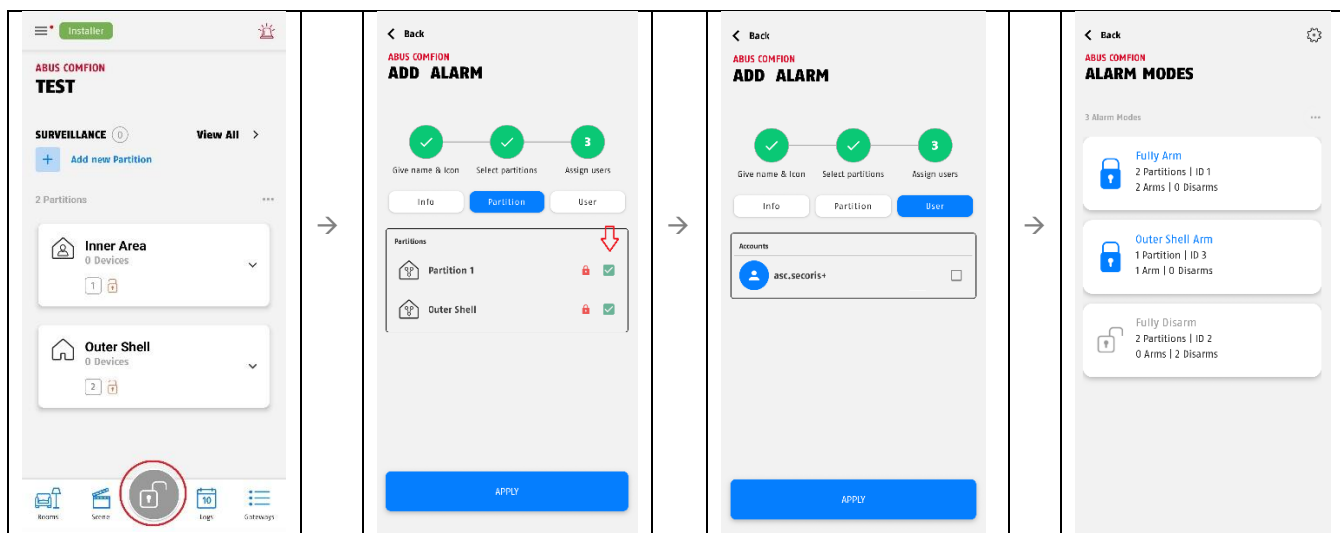
Uitvoering van een alarmmodus

- De knop in het midden van de onderste beeldrand toont de actuele status van het systeem (ingeschakeld, uitgeschakeld, gedeeltelijk ingeschakeld of onderhoudsmodus)
- Als u op de knop drukt, worden de beschikbare alarmmodi weergegeven en kunt u een van de daar getoonde schakelopdrachten uitvoeren.



Alarmmodi aanmaken of bewerken

1. U opent het beheer van de alarmmodi door in het dashboard op de statusknop te klikken en vervolgens op het instellingenpictogram (tandwiel) rechtsboven in het scherm.
2. Klik vervolgens op "Alarmmodus toevoegen" of bewerk een bestaande alarmmodus door er lang op te drukken.
3. Nadat u de naam voor de alarmmodus hebt toegewezen, selecteert u de partities EN de aard van de schakeling (ingeschakeld of uitgeschakeld). Klik op het symbool om de aard van de schakeling te wijzigen.
4. Selecteer in de volgende stap de gebruikers die geautoriseerd moeten worden om deze alarmmodus te schakelen.
5. Na voltooiing verschijnt de alarmmodus in uw overzicht en kunt u deze gebruiken.



4.3. WLX Pro-installatie en programmering

Voer de montage en bedrading van de **Comfion Pro BUS-WLX-module** uit zoals beschreven in de producthandleiding en in hoofdstuk 3.2.7.

Opmerking	Voor het instellen en uitvoeren van de configuratie van de Comfion Pro BUS-WLX-module en andere WLX Pro-sluitmedia hebt u de meegeleverde systeemkaart en resetkaart nodig. Bewaar deze kaarten zorgvuldig!
------------------	--

- Voeg de Comfion Pro BUS-WLX-module als "nieuw onderdeel" toe aan het systeem. Ga te werk zoals beschreven in **hoofdstuk 3.2.5** en volg de instructies voor het programmeren op.
- Programmeer vervolgens de WLX Pro-sluitcilinder of de WLX Pro-wandlezer.
- Tijdens het inleerproces (stap 2) wordt u gevraagd om de WLX Pro-sluitcilinder of WLX Pro-wandlezer toe te wijzen aan een Comfion Pro BUS-WLX-module. Kies de module die het dichtst bij de cilinder/wandlezer gepositioneerd is.

Opmerking	Nadat u de eerste sluitcilinder of wandlezer hebt geprogrammeerd, wordt u gevraagd om de meegeleverde resetkaart te programmeren. De geprogrammeerde resetkaart is in het Comfion-systeem vast opgeslagen als back-up-medium en is nodig om een cilinder te resetten. Meer informatie vindt u in hoofdstuk 6.1.8 WLX-informatie en in hoofdstuk 3.2.6 Instellingen voor componenten
------------------	--

Belangrijk	De volgende apparaten kunnen momenteel in de Comfion Pro worden geprogrammeerd: - WLX Pro-cilinder (Access/Intrusion) Type: LA-A, LA-I - WLX Pro-wandlezer (Access/Intrusion) Type: WR-A-S-O, WR-I-S-O De WLX Pro-repeater en andere sluitmedia worden momenteel niet ondersteund.
-------------------	---

- U kunt RFID-tags (NFC-tags) inlezen in de gebruikersinstellingen of dit kan direct na de overdracht door de eigenaar (administrator) worden gedaan. Meer informatie vindt u in **hoofdstuk 4.4.1 Toegangsrechten**.

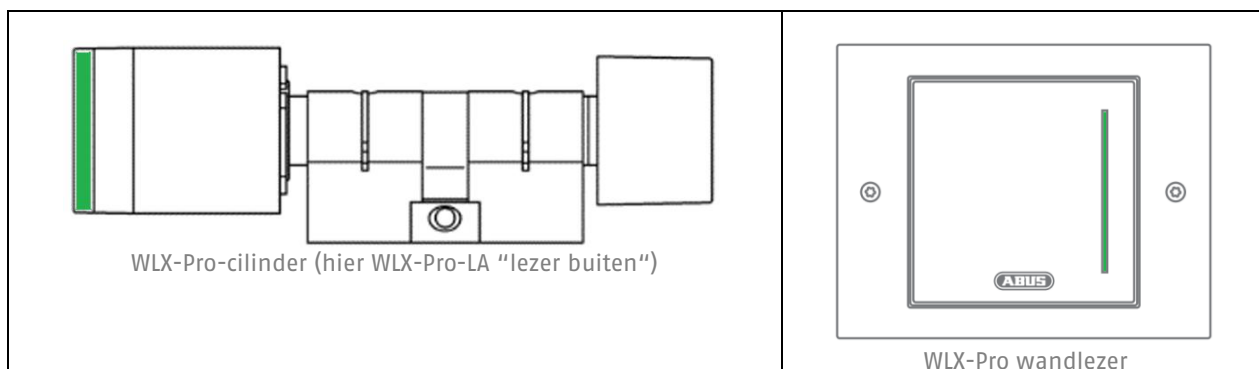
Belangrijk	Wij raden aan om ten minste één NFC-tag als noodoplossing in te stellen, zodat in geval van nood (bijvoorbeeld bij uitval van de draadloze verbinding of een langdurige stroomstoring) bevoegde personen toegang kunnen krijgen. Meer informatie vindt u in hoofdstuk 4.4.1 Toegangsrechten
-------------------	---

4.3.1. Installatie, configuratie en gebruik van de WLX Pro-cilinders en wandlezers

Meer informatie over de installatie van WLX-Pro-sluitcilinders / WLX-Pro-wandlezers vindt u in de bijbehorende installatiehandleidingen van de producten. Deze zijn online beschikbaar op abus.com in het downloadgedeelte van de productpagina:

- WLX-Pro-sluitcilinder: <https://abus.com/products/WLX-Pro-LA>
- WLX-Pro-wandlezer: <https://www.abus.com/products/ACSE00026>

De WLX-Pro-sluitcilinder en de WLX-Pro-wandlezer geven de volgende toestanden aan via een knipperpatroon van de LED's:



Signalen	Beschrijving	
Inbedrijfstelling en initialisatie		
	1 x groen, 1 x rood, 1 x groen, 1 x rood	Initialisatie na het plaatsen van de batterij
	1 x groen (lang)	De cilinder is niet geprogrammeerd (& permanent gekoppeld)
	2 x rood	Communicatie met buitenknop aanwezig
	2 x groen	Communicatie met Comfion Pro BUS WLX-module aanwezig.
Programmeren/Uitleren/Reset (tijdens het programmeerproces (vanaf firmware 2.01) knippert de cilinder met regelmatige tussenpozen groen)		
	2 x groen	Programmeren geslaagd
	3 x rood	Succesvol afmelden ('uitleren')
	1 x rood	Programmeren mislukt
	10 x rood	De systeemkaart is gepresenteerd (inleer-/afmeldmodus); als de resetkaart tijdens de knipperreeks wordt voorgehouden, wordt het apparaat gereset.
In bedrijf		
	1 x groen	Kort groen knipperen geeft aan dat het lees- en zendproces van het sluitmedium 1x groen is.
	1 x rood	Geen draadloze verbinding met de Comfion Pro BUS-WLX-module
	1 x rood (lang)	De Comfion Pro is ingeschakeld (bevestiging)
	1 x groen (lang)	De Comfion Pro is uitgeschakeld (bevestiging)
	1 x rood, 2x groen	Verlies van het radiosignaal / geautoriseerde fallback (herhaal deze procedure in totaal 3 keer)
	2 x groen	Toegang verleend
	3 x rood	Toegang geweigerd, geen geldige toegang

	3 x rood, 2 x groen	Batterijwaarschuwing (tot firmwareversie 2.07)
	5 x rood, 2 x groen	Batterijwaarschuwing (vanaf FW 2.09) De cilinder schakelt met een vertraging van ca. één seconde in
	1 x rood, 2 x groen	Batterijwaarschuwing niveau 2: geen signalering op de personentransponder, de Fallback kan nog 3x toegang verlenen → Gebruik het Fallback Medium zoals bij een storing in het draadloze netwerk
	4 x rood	Er is een storing in de draadloze communicatie en een onbevoegde Fallback-transponder werd gepresenteerd
	6 x rood	- Kan niet worden ingeschakeld, of - Uitschakelen is niet mogelijk

4.3.2. WLX Pro-functies – Op afstand openen en kantoormodus

Op afstand openen

Met behulp van de opening op afstand (ook wel 'remote-vrijgave' genoemd) kan de WLX-Pro-sluitcilinder voor een bepaalde periode (maximaal 180 seconden) worden ontgrendeld. De configuratie gebeurt in de Comfion-app (of via het webinterface) als scène of automatisering.

- o De scèneconfiguratie wordt aangevuld met een hotkey-knop in het dashboard van de Comfion-app
- o Meer informatie over de configuratie vindt u in **hoofdstuk 6.4 Automatiseringen & scènes**
- o Nadat de opening op afstand is uitgevoerd, moet de buitenknop op de WLX-Pro-sluitcilinder worden gedraaid om de deur te openen.

 Opmerking	Let op het verschil: - De duur van de remote vrijgave is de periode waarin de cilinder kan worden ingekoppeld - Nadat de buitenknop is gedraaid, wordt de cilinder gedurende de ingestelde openingsduur (6 of 12 seconden) ingekoppeld.
--	---

 Belangrijk	Op afstand openen is alleen mogelijk in de toestand waarin de Comfion Pro is uitgeschakeld.
---	---

Kantoormodus (permanente toegang)

Bij een cilinder waarop de kantoormodus is ingeschakeld, kan de deur zonder NFC-tag worden geopend door aan de cilinderknop te draaien. De configuratie gebeurt in de Comfion-app (of via het webinterface) als scène of automatisering.

- o De configuratie voor scènes wordt aangevuld met een hotkey-knop in het dashboard van de Comfion-app (u hebt 2 scènes nodig om de kantoormodus in en uit te schakelen)
- o Met de automatiseringsconfiguratie kunt u de kantoormodus in- en uitschakelen, bijvoorbeeld via een tijdschema: indien tijdstip x →, dan inschakelen ... als tijdstip Y →, dan uitschakelen
- o Meer informatie over de configuratie vindt u in **hoofdstuk 6.4 Automatiseringen & scènes**
- o Als de kantoormodus is geactiveerd, moet de buitenknop op de WLX-Pro-sluitcilinder worden gedraaid om de deur te openen.

 Belangrijk	Openen via de kantoormodus is alleen mogelijk in de toestand waarin de Comfion Pro uitgeschakeld is. Een geactiveerde kantoormodus wordt onderbroken voor de duur van de inschakeling! Programmeer deze functie alleen als de gebruiker op de hoogte is van de gevolgen en deze schriftelijk heeft bevestigd.
---	--

4.4. Camera's (NVR)

Met behulp van het ONVIF-integratieprotocol kunnen diverse camera's uit de ABUS Professional Line worden geïntegreerd in het draadloze Comfion Pro-beveiligingssysteem. Als alternatief is integratie via RTSP mogelijk. U kunt tot 8 camera's aansluiten op de Comfion Pro en deze laten opnemen bij een gebeurtenis, wanneer de installatie ingeschakeld is of continu (24/7) (op een micro-SD-kaart of SSD).



Opmerking

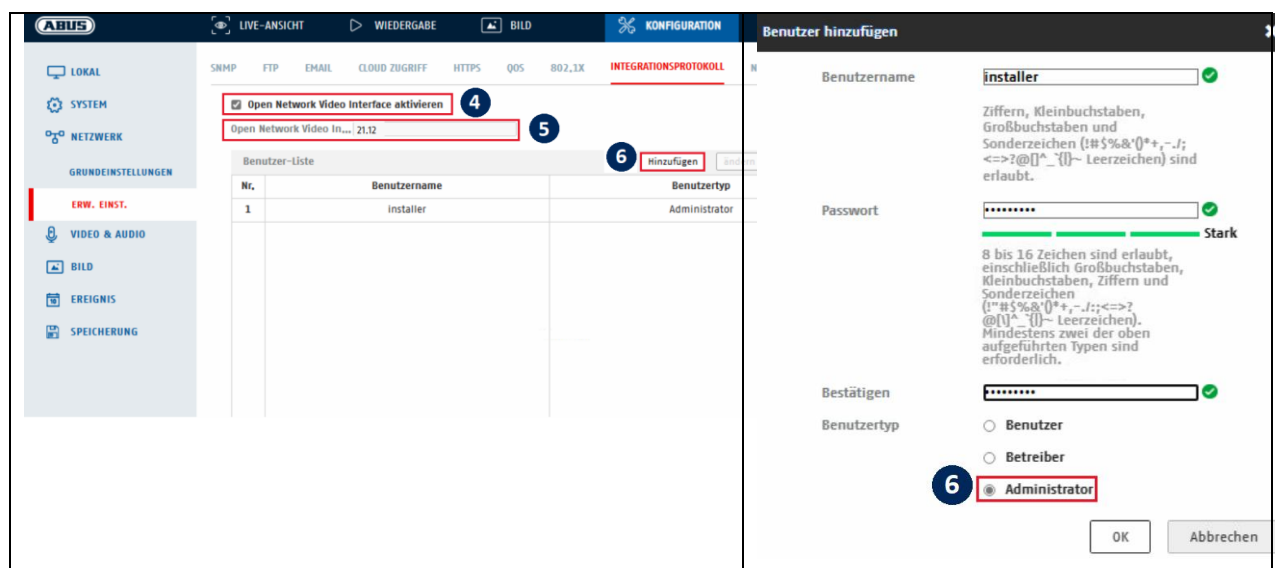
Voor continue opname (24/7) is een SSD-data-opslag in de centrale nodig.

4.4.1. Camera's integreren via ONVIF

In de fabriekinstellingen zoekt het Comfion Pro-systeem automatisch naar ONVIF-camera's in het netwerk en voegt deze toe aan het systeem. U kunt het Automatische camera zoeken deactiveren in het camera-overzicht in de camera-instellingen.

Ga als volgt te werk bij het integreren van de camera's:

1. Sluit de camera aan op hetzelfde netwerk als de Comfion Pro.
2. Open de software ABUS IP-Tool en activeer de camera.
3. Open de camera-interface, log in als de installateur en open de configuratie.
4. Schakel ONVIF in via de geavanceerde netwerkinstellingen van de camera onder het tabblad "Integratieprotocol" (Open Network Video Interface)
5. Hier ziet u ook de ONVIF-versie van de camera; voor Comfion Pro is versie 21.12 of hoger vereist. (Werk indien nodig de firmware van de camera bij – deze is beschikbaar op abus.com in het downloadgedeelte van het artikel)
6. Bovendien moet hier een nieuwe ONVIF-gebruiker worden toegevoegd. Selecteer hier het gebruikerstype "Administrator".
7. Verricht in de camera de video-instellingen die in het onderstaande aanwijzingenveld worden beschreven
8. Sla de ONVIF-gebruikersgegevens op in de Comfion Pro. (Selecteer in de Comfion Pro-app en de webinterface de gebruiker die onder (6.) is aangemaakt om verbinding te maken met de camera.)
9. Test de camerafuncties (livebeeld, enz.)



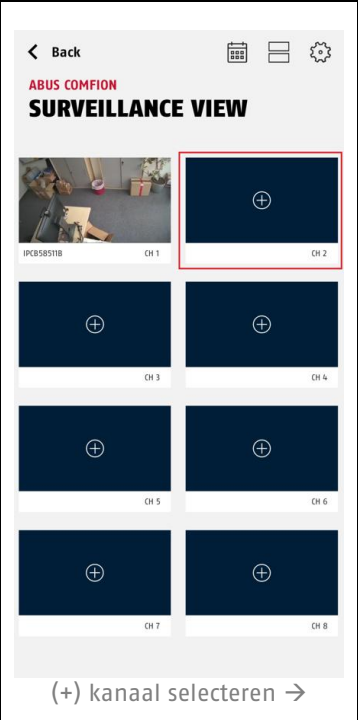
 Aanwijzing	Afhankelijk van het aantal aangesloten camera's (kanalen) worden de volgende instellingen voor videostreaming aanbevolen om ook bij het gelijktijdig bekijken en de continue opname van 8 kanalen een storingsvrije stream te kunnen garanderen. Primaire stream: 1 kanaal: Resolutie 4K; bitrate: 6 Mbps 8 kanalen: 4 x resolutie: 4K (3840 x 2160); bitrate: 2048kbps 4 x resolutie: 1080p (1920 x 1080); bitrate: 2048kbps Secundaire stream: 1-8 kanalen: Resolutie: 360p; bitrate 512kbps
 Aanwijzing	- De maximale resolutie van 4K (3840 x 2160) per kanaal mag niet worden overschreden - De maximale bitrate mag niet hoger zijn dan 8 x 2048kbps

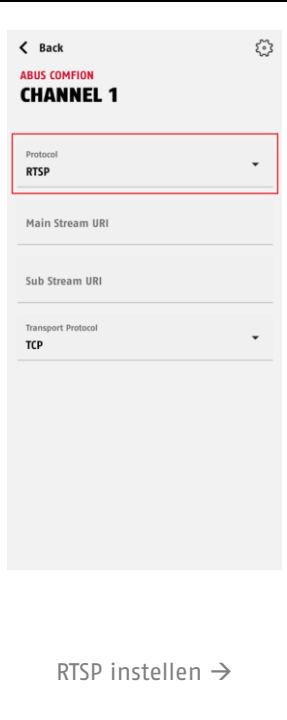
4.4.2. Camera's integreren via RTSP

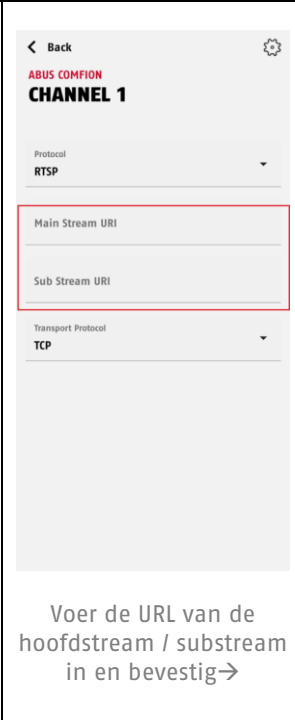
 Opmerking	De integratie via RTSP levert de videostream en audio-stream van de camera, maar biedt geen mogelijkheden voor verdere configuratie, PTZ-besturing of bewegingsdetectie.
--	---

Voer de volgende stappen uit om camera's via een RTSP-stream te integreren:

1. Sluit de camera aan op hetzelfde netwerk als de Comfion Pro.
2. Open de software ABUS IP-Tool en activeer de camera. Maak indien nodig een installateursaccount voor de camera aan.
3. Selecteer in de Comfion-app → Cameraoverzicht een (nog vrij) camerakanaal (+)
4. Selecteer in de configuratie onder "netwerkprotocol" de optie RTSP.
5. Voer de URL van de hoofdstream en de substream in. Compatibele ABUS-camera's gebruiken de volgende URL's:
 - **Aanwijzing:** Vervang "Gebruikersnaam" en "Wachtwoord" door de inloggegevens uit stap 2
 - Primaire stream: RTSP://gebruikersnaam:Passwort@192.168.0.27/ISAPI/Streaming/channels/101
 - Secundaire stream: RTSP://gebruikersnaam:Passwort@192.168.0.27/ISAPI/Streaming/channels/102







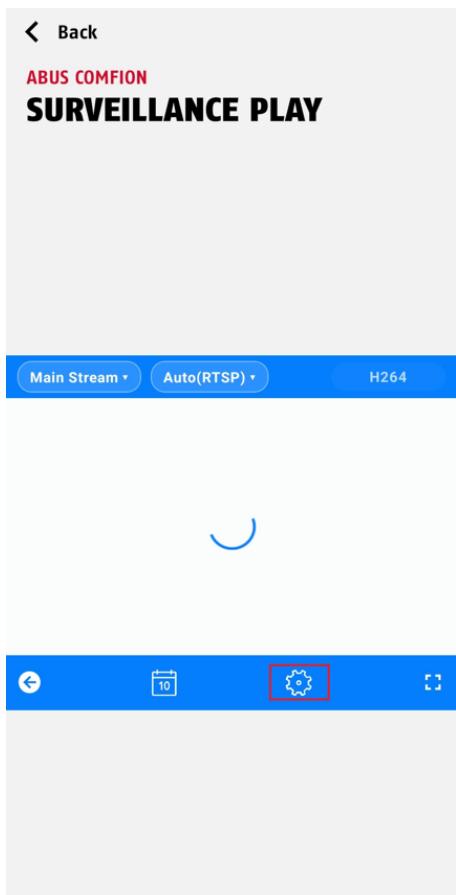
4.4.3. Camera-instellingen (algemeen)

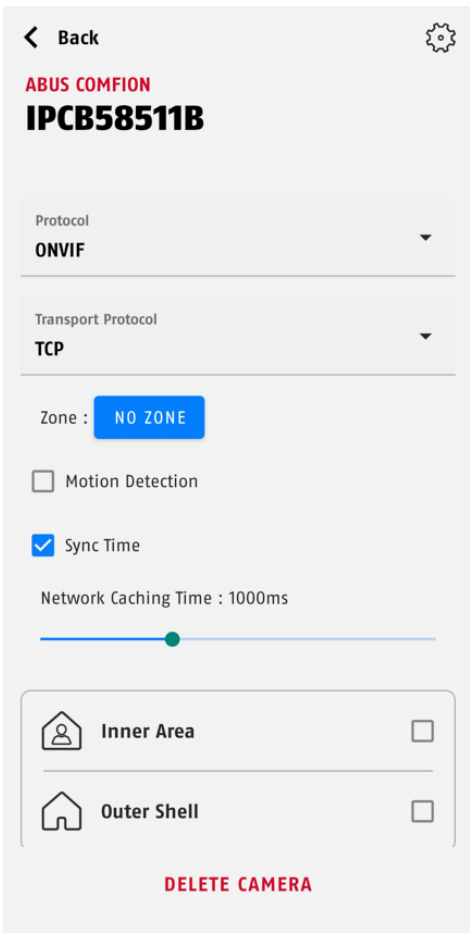
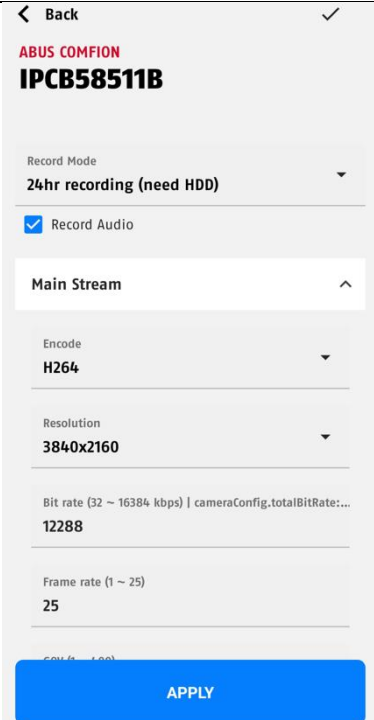
Via het cameraoverzicht kunt u door op het tandwielpictogram te klikken naar de camera-instellingen gaan . Deze gelden **op dezelfde manier voor alle aangesloten camera's**

Automatisch camera zoeken	UIT (voorinstelling) / AAN (uitgeschakeld) Automatisch zoeken naar ONVIF-camera's in hetzelfde netwerk
Gegevensopslag	UIT / AAN & 1 – 365 dagen Opnames worden na afloop van de opgegeven tijd van het opslagmedium gewist, mits de optie "AAN" is ingeschakeld.
Opname streamtype	Primaire stream (voorinstelling) / Secundaire stream Het type stream dat voor de opname wordt gebruikt.

In het detailscherm van de camera (live videostream) vindt u nog een tandwielpictogram  voor verdere configuraties **van deze camera**. Meer informatie vindt u in **hoofdstuk 3.4.4**.

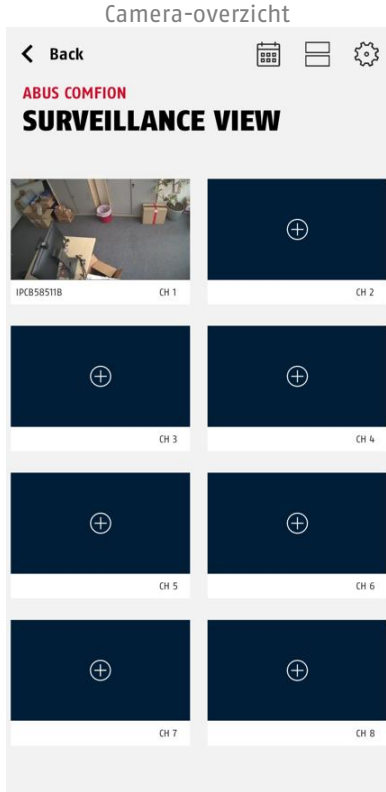
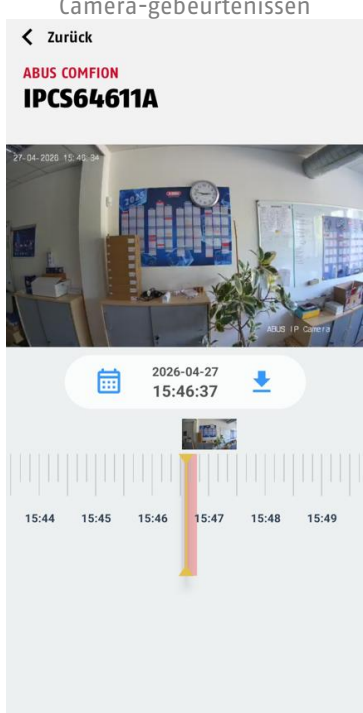
4.4.4. Camera-instellingen (afzonderlijk)

	Vanuit het camera-overzicht kunt u naar de livestream gaan door op de camerategel te klikken  terug naar het camera-overzicht Pannen/kantelen, luidspreker, microfoon    Raadpleeg de gebruikershandleiding van Comfion Pro voor meer besturingsfuncties en details.  Camera-gebeurtenissen – zie hoofdstuk 3.4.5 NVR-bediening voor meer informatie  Instellingen voor deze camera  Schakelt tussen staande en landscape-modus
--	---

	Naam camera, IP-adres, poort, gebruikersnaam, wachtwoord, netwerkprotocol, transmissieprotocol • Zie 3.4.1 en 3.4.2: Camera's aansluiten Zone • Als de camera aan een deelgebied is toegevoegd (in dit geval het binnendeelgebied), wordt hier het zonenummer weergegeven. Bewegingsdetectie • Indien ingeschakeld, wordt de bewegingsdetectie van de camera door de Comfion Pro geanalyseerd en kan deze in automatiseringen als triggergebeurtenis worden geprogrammeerd.  Belangrijk Om deze functie in te schakelen, moet u deze activeren in de directe configuratie van de camera (webinterface of ABUS-IP-Tool).  Aanwijzing Om de bewegingsdetectie van de camera te gebruiken voor het activeren van een alarm, moet bovendien in de componentinstellingen van de camera de functie "MotionAlarm" worden ingeschakeld. Synchronisatietijd • Indien deze functie is ingeschakeld, neemt de camera de tijdsinstelling van de Comfion Pro-centrale over Netwerk-caching-tijd • De buffertijd van de Comfion Pro NVR voor het tijdelijk opslaan van binnenkomende videogegevens voordat deze worden weergegeven. Camera wissen Verwijdert de camera uit de kanaalpositie en uit de componentenlijst.
	Klik op het tandwielpictogram in de camera-instellingen (afzonderlijk) om de opnamemodus in te stellen: Opnamemodus • Continue opname ○ 24/7 opname ○ Vereist een harde schijf (bijv. SSD-opslag) • Opname alleen mogelijk als het systeem is geactiveerd ○ Opname bij een in bedrijf zijnde installatie (of deelgebied) ○ Vereist een harde schijf (bijv. SSD-opslag) • Alleen opnemen tijdens gebeurtenis ○ Afhankelijk van het ingestelde zonetype van de camera, bijvoorbeeld inbraak of perimeter ○ Vereist een micro-SD-kaart of harde schijf • Geen opname Audio-opname • Opname inclusief audiostream (indien ondersteund door de camera)

4.4.5. NVR-bediening

Het camera-overzicht brengt u naar de parallelle weergave van alle kanalen. U kunt het livebeeld van alle geïntegreerde camera's hier bekijken. Via de kalenderfunctie kunt u de opnames die in het systeem aanwezig zijn op datum gesorteerd bekijken.

	 Camera-gebeurtenissen per camerakanaal (Continue opname en/of gebeurtenissen)   Weergave van de camerakanaal in een raster of in rijen.  Camera-instellingen  Previewbeeld van een reeds aangemelde camera – Een klik schakelt over naar de livestream van de camera. Afhankelijk van het cameratype zijn er nog meer functies/instellingen beschikbaar. (bijv. PTZ, 2-weg audio, enz.)  Vrij camerakanaal. Als u op "+" klikt, wordt het programmeerproces gestart, d.w.z. door te zoeken naar camera's in hetzelfde netwerk of door ze handmatig toe te voegen.
	Selecteer eerst het camerakanaal om naar dit scherm te gaan.  Zoeken naar camerabeelden in de kalender (dagen met gebeurtenissen zijn gemarkeerd met een stip)   Camera-gebeurtenissen downloaden - De starttijd wordt in de tijdlijn vastgelegd - Opnameduur instelbaar van 10 sec. tot 30 min.  Selectie van cameragebeurtenissen in de tijdlijn Opname van het evenement → rood Continue opname → grijs

5. Gebruikers en autorisatiegroepen

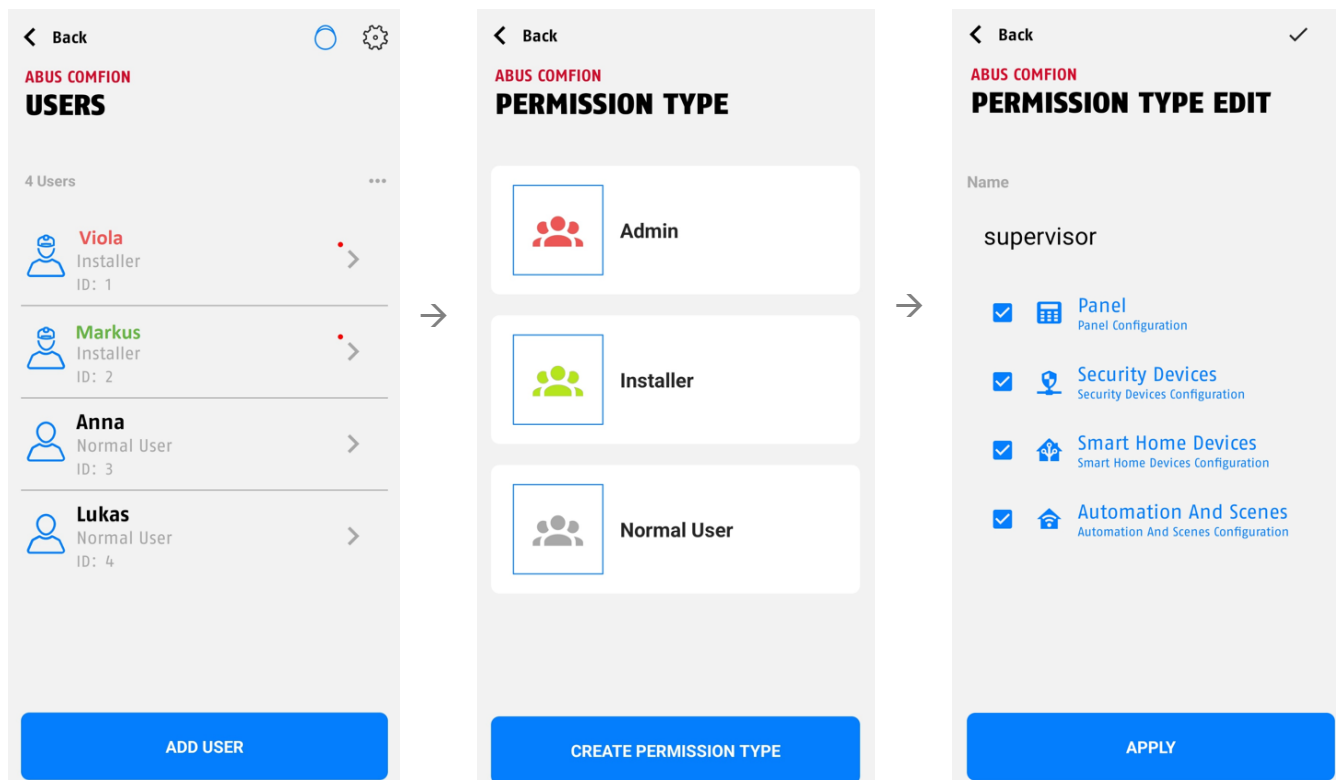
5.1. Uitleg over de verschillende rollen

Installateur	De installateur heeft alle gebruikersrechten tijdens de eerste inbedrijfstelling. Na overdracht van het systeem behoudt de installateur alle configuratierechten. De eigenaar van het systeem kan de rechten van de installateur voor het live camerabeeld intrekken en de toegang tot het systeem volledig blokkeren.
Admin	De administrator heeft alle gebruikersrechten voor het systeem. Als de installateur de beheerder configuratierechten toekent, kan de beheerder de rechten van een installateur krijgen en zo bijvoorbeeld automatiseringen en scènes aanmaken en bewerken.
Eigen rol (Door gebruiker gedefinieerd)	U hebt de mogelijkheid om uw eigen non-administrator gebruikersgroepen aan te maken en hun autorisaties vast te leggen (zie hieronder)
Eigenaar (extra rol)	De eigenaarsrol wordt automatisch toegewezen aan de eerste op het systeem bestaande administrator. De eigenaarsrol kan niet handmatig worden toegewezen. Naast de administrator-rechten heeft de eigenaar van het systeem de rechten om gebruikers toe te voegen, uit te nodigen en te verwijderen. De eigenaar van het systeem is rood gemarkeerd in de gebruikerslijst.

De volgende instelmogelijkheden zijn beschikbaar onder de installateur-gebruiker:

- Toegang vrijgeven: Blokkeert/verleent toegang tot het systeem en pushberichten
- Hoofdinstallateur: Bepaalt aan welk installateursaccount het systeem wordt gekoppeld voor onderhoud op afstand (portaal voor gespecialiseerde installateurs)

Gebruikersgroepen aanmaken:



5.2. Inbedrijfstelling

De autorisatietypes "Installateur" en "Administrator" zijn momenteel beschikbaar in de fabrieksinstellingen van de centrale. Als het systeem in bedrijf wordt gesteld door een installateur, dan is deze in eerste instantie geautoriseerd voor alle functies in de centrale.

5.2.1. Overdracht aan de eigenaar

Nadat u als installateur de installatie van de centrale hebt voltooid, moet het systeem worden overgedragen aan de eindgebruiker. De eerste uitgenodigde beheerder (admin) wordt **de eigenaar** van de installatie. U kunt dit herkennen aan het feit dat deze gebruiker rood gemarkeerd is.

Nadat de eigenaar is uitgenodigd, verliest de installateur de rechten om gebruikers te bewerken en toe te voegen. Andere gebruikers moeten door de **eigenaar** worden toegevoegd.

5.3. Gebruikers uitnodigen/toevoegen

Nieuwe gebruikers kunnen na de overdracht uitsluitend door de eigenaar worden uitgenodigd. De volgende mogelijkheden zijn beschikbaar bij het toevoegen van een nieuwe gebruiker:

- Nieuwe gebruiker uitnodigen
 - Een gebruiker uitnodigen via zijn e-mailadres.
- Het kiezen van mijn leden
 - Uitnodigen van een lid. Leden kunnen worden toegevoegd aan de persoonlijke ledenlijst in het overzicht van de centrale. (Zie **6.3.2 Leden**)
- Lokale gebruiker aanmaken
 - Maak een lokale gebruiker aan zonder Abus Cloud-account en zonder de app te gebruiken. Aan de lokale gebruiker kan een afstandsbediening of een code voor het bedieningspaneel worden toegewezen, en er kan een NFC-tag of -kaart worden toegevoegd. Bovendien kunnen een telefoonnummer en e-mailadres opgeslagen worden voor kennisgevingen.

De autorisatie van de toe te voegen gebruiker kan eveneens worden geselecteerd. U kunt kiezen tussen Installateur, Administrator en de gebruikersgroepen die u zelf hebt aangemaakt.

5.4. Gebruikers bewerken

De gebruikersgegevens zijn onderverdeeld in drie categorieën: toegangsrechten, meldingen en toegestane alarmmodi tijdens het gebruik

5.4.1. Toegangsrechten

Toegang:

Per gebruiker kan hier de machtigingsgroep (installateur, beheerder, gewone gebruiker) worden aangepast

PIN-code:

Voer de 4-cijferige pincode in voor identificatie op het Comfion draadloos bedieningspaneel

 Aanwijzing	Elke 4-cijferige code kan slechts één keer worden toegekend. Als dezelfde code aan een tweede gebruiker wordt toegewezen, verschijnt er een foutmelding.
---	---

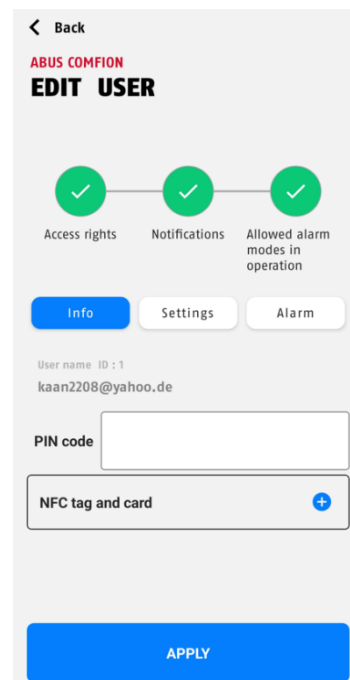
Bediening toestaan

In combinatie met het opgeven van het e-mailadres en het telefoonnummer. Biedt deze gebruiker toegang

E-mail & telefoon (alleen lokale gebruikers)

Invoer van het e-mailadres en telefoonnummer om meldingen via e-mail of SMS te ontvangen

NFC-tag en kaart



The screenshot shows the 'EDIT USER' interface for 'ABUS COMFION'. At the top, there's a 'Back' button and the title 'ABUS COMFION EDIT USER'. Below the title, three green checkmarks indicate that 'Access rights', 'Notifications', and 'Allowed alarm modes in operation' are all enabled. Underneath these, there are three buttons: 'Info', 'Settings', and 'Alarm'. Further down, the 'User name' is listed as 'ID : 1' and 'kaan2208@yahoo.de'. There is a 'PIN code' field with a text input box. Below that is an 'NFC tag and card' section with a blue plus icon. At the bottom, there is a large blue 'APPLY' button.

Per gebruiker kunnen maximaal 2 NFC-tags/kaarten geprogrammeerd en toegewezen worden.

Als u op "+" drukt, start het programmeerproces

Als u op de reeds aangeleerde media drukt, worden de instellingen geopend met meer configuratiemogelijkheden:

- Uit - (schakelt de tag uit als deze is ingeschakeld)
- Dwangschakeling - (Maakt het mogelijk om het systeem bij storingen in te schakelen)
- Fallback Medium - (indien ingeschakeld, wordt de toegang lokaal bij de cilinder/wandlezer gecontroleerd wanneer de radiocommunicatie tussen de cilinder/wandlezer en de BUS-WLX-module verstoord is.)
- Naam - (aanduiding van de tag - de naam verschijnt ook in het logboek bij een toegangsgebeurtenis)
- Gebruiker - (Toewijzing aan een aangemaakte gebruiker in het Comfion Pro-systeem)

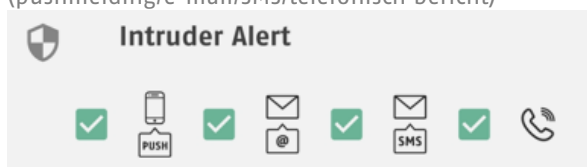
Wijzigingen moeten worden bevestigd door op "Opslaan" of "Bevestigen" te klikken

5.4.2. Notificaties

Het Comfion Pro-beveiligingssysteem beschikt over de volgende communicatiekanalen: E-mail, Push, SMS, Telefoon en Meldkamerbijschakeling

Onder het menupunt "Gebruikers → Gebruikers bewerken → Meldingen" kunt u voor elke aangemaakte gebruiker afzonderlijk instellen welke meldingen per gebeurtenis moeten worden verzonden.

Bijvoorbeeld voor het gebeurtenistype "inbraakalarm" (pushmelding/e-mail/SMS/telefonisch bericht)

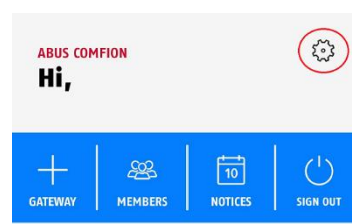
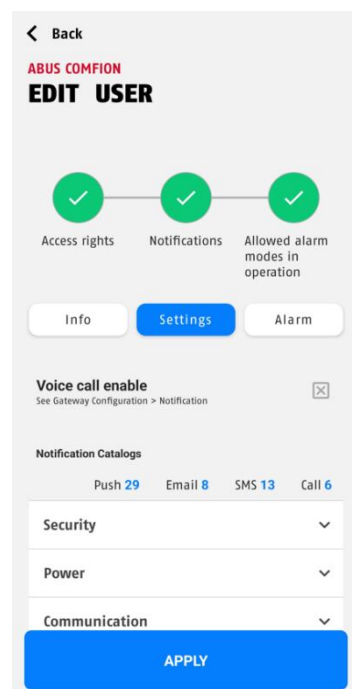


 Aanwijzing	Sommige gebeurtenissen zijn beperkt tot bepaalde communicatiemethoden. Bij sommige gebeurtenissen is het bijvoorbeeld niet mogelijk om te bellen. Pushmeldingen zijn alleen beschikbaar voor gebruikers van de Comfion-app; dit betekent dat ze niet kunnen worden gebruikt voor lokale gebruikers.
---	---

Het telefoonnummer voor SMS-berichten en telefoongesprekken, alsmede het e-mailadres voor meldingen, worden in het gebruikersaccount opgeslagen. U kunt deze op elk gewenst moment wijzigen. Ga hiervoor naar het overzicht van uw centrale en klik op het tandwielje in de rechter bovenhoek. U kunt nu het telefoonnummer voor de kennisgevingen en de e-mail voor kennisgevingen toewijzen.

Lokale gebruikers kunnen hun e-mailadres / telefoonnummer invoeren in de gebruikersinstellingen (toegangsrechten).

 Opmerking	Voer het telefoonnummer altijd in met het landnummer, bijvoorbeeld +49.....
--	---

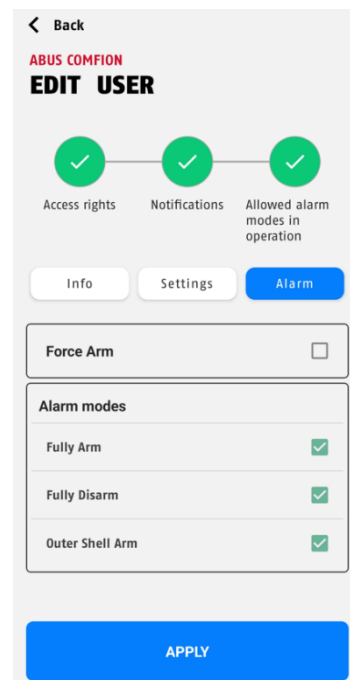


5.4.3. Toegestane alarmmodi tijdens bedrijf

Hier stelt u in of de gebruiker het systeem geforceerd mag inschakelen (in dat geval wordt het systeem ingeschakeld, zelfs als er een zone geopend of geactiveerd is en zonder de overbruggingsprocedure). Meer informatie vindt u in het **hoofdstuk: 6.7.3**

Bovendien stelt u hier de bevoegdheid in om elk deelgebied in of uit te schakelen. De gebruiker moet ten minste één machtiging hebben.

Alle wijzigingen worden doorgevoerd zodra u op 'Bevestigen' klikt.



5.5. Gebruikers verwijderen

Er zijn twee manieren om gebruikers uit de centrale te verwijderen:

1. De eigenaar van het systeem (de gebruiker die rood is gemarkeerd) kan elke andere gebruiker uit het systeem verwijderen door op die gebruiker te klikken en vervolgens op de knop 'Gebruiker verwijderen' te klikken.
2. Elke gebruiker kan zichzelf uit de installatie verwijderen door in het centrale overzicht lang op de betreffende centrale te klikken en vervolgens het verzoek tot verwijdering te bevestigen.

 Aanwijzing	De eigenaar van het systeem kan zichzelf alleen via de tweede methode (de centrale uit het centrale-overzicht verwijderen) uit het systeem verwijderen. Nadat de eigenaar is verwijderd, komt de taak bij de installateur te liggen. Deze kan door een nieuwe beheerder uit te nodigen, deze als nieuwe eigenaar aanwijzen.
---	--

6. Communicatie

6.1. Mobiele communicatiemodule

Het Comfion Pro-beveiligingssysteem beschikt over een geïntegreerde mobiele module (2G/3G/4G). Deze kan worden gebruikt om SMS-berichten te verzenden en te bellen in geval van een alarm. Zij biedt bovendien een redundante route voor alle communicatie binnen het systeem. Dit betekent dat bij uitval van uw internetverbinding alle communicatie met de cloud, en dus ook de toegang op afstand en de pushmeldingen, via de mobiele module verloopt.

 Opmerking	Schakel uw SIM-kaart pinnvrij voordat u deze in de GSM-module inlegt. U kunt de PIN in de regel uitschakelen in de instellingen van elke mobiele telefoon.
 Aanwijzing	Gebruik geen simkaarten uit het buitenland voor continu gebruik in de Comfion Pro.

Er is een SIM-kaart nodig om de GSM-module te gebruiken. Deze SIM-kaart is vrij te kiezen (aanbeveling ABUS: Telekom, Vodafone, o2) en moet beschikken over de functies die u wilt gebruiken bij de centrale. Als u alle functies wilt gebruiken, hebt u een SIM-kaart met sms, spraaktarief en datavolume nodig.

 Aanwijzing	ABUS raadt het gebruik van prepaidkaarten in het Comfion Pro-beveiligingssysteem af vanwege twijfels over de betrouwbaarheid ervan. Bovendien is het gebruik van Multi-SIM's niet aan te raden omdat dit kan leiden tot verbindingsproblemen.
 Opmerking	Afhankelijk van het gebruiksdoel moet de simkaart over de volgende eigenschappen beschikken: • "SMS via IMS" – SMS-verzending via het 4G-netwerk • "Voice over LTE" – belfunctie via het 4G-netwerk

RSRP-waarde (dBm)	Betekenis	 Aanwijzing
< -80 -80 tot -90 -91 tot -100 -101 tot -110 > -111	Zeer goed Goed Middel Zwak Zeer slecht	RSRP is de sterkte van het nuttige signaal (LTE-referentiesignaal) dat vanuit de zendmast bij het apparaat aankomt. De installatieplek kan de signaalsterkte beïnvloeden, bijvoorbeeld door de afstand tot de zendmast of door demping door het gebouwmateriaal. Bij twijfel raden wij aan een externe antenne te gebruiken.

In de GSM-module zelf hoeven geen verdere instellingen te worden verricht voor het verzenden van SMS-berichten of voor de belfunctie. Als u de redundantie van de netwerkdiensten wilt gebruiken, is het noodzakelijk om de APN-gegevens van de gebruikte SIM-kaart op te slaan. U vindt dit menupunt onder "Centrale-configuratie" → tandwiel → "Mobiele-communicatiemodule".

Als er geen simkaart in de Comfion Pro is geplaatst, schakel dan het keuzevakje 'Activeren' uit. In dat geval wordt de simkaart niet gecontroleerd en wordt er geen foutmelding weergegeven.

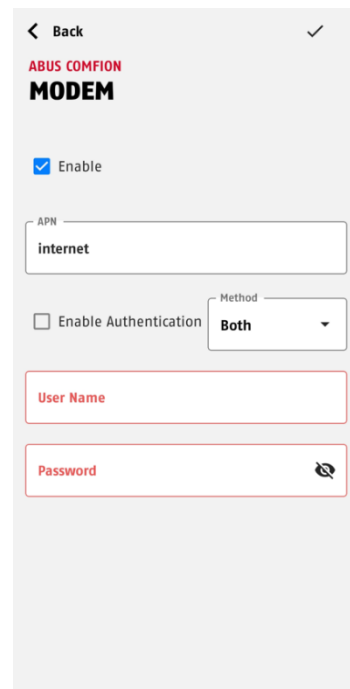
De APN-gegevens van uw mobiele telefonieprovider zijn bijgevoegd bij uw SIM-kaart. U kunt deze alternatief ook online opvragen. Deze gegevens zijn niet SIM-kaart-specifiek, maar zijn hetzelfde voor elke provider. Als een gebruikersnaam en wachtwoord zijn opgegeven in de APN-gegevens, vink dan het vakje "Authenticatie" aan.

Voorbeeld Telekom:

- APN: internet.telekom
- Gebruikersnaam: t-mobile
- Wachtwoord: tm

Voorbeeld Vodafone:

- APN: web.vodafone.de
- Geen gebruikersnaam
- Geen wachtwoord



6.2. E-mail

Het verzenden van e-mails via Comfion Pro werkt zonder configuratie en verloopt via de cloud.

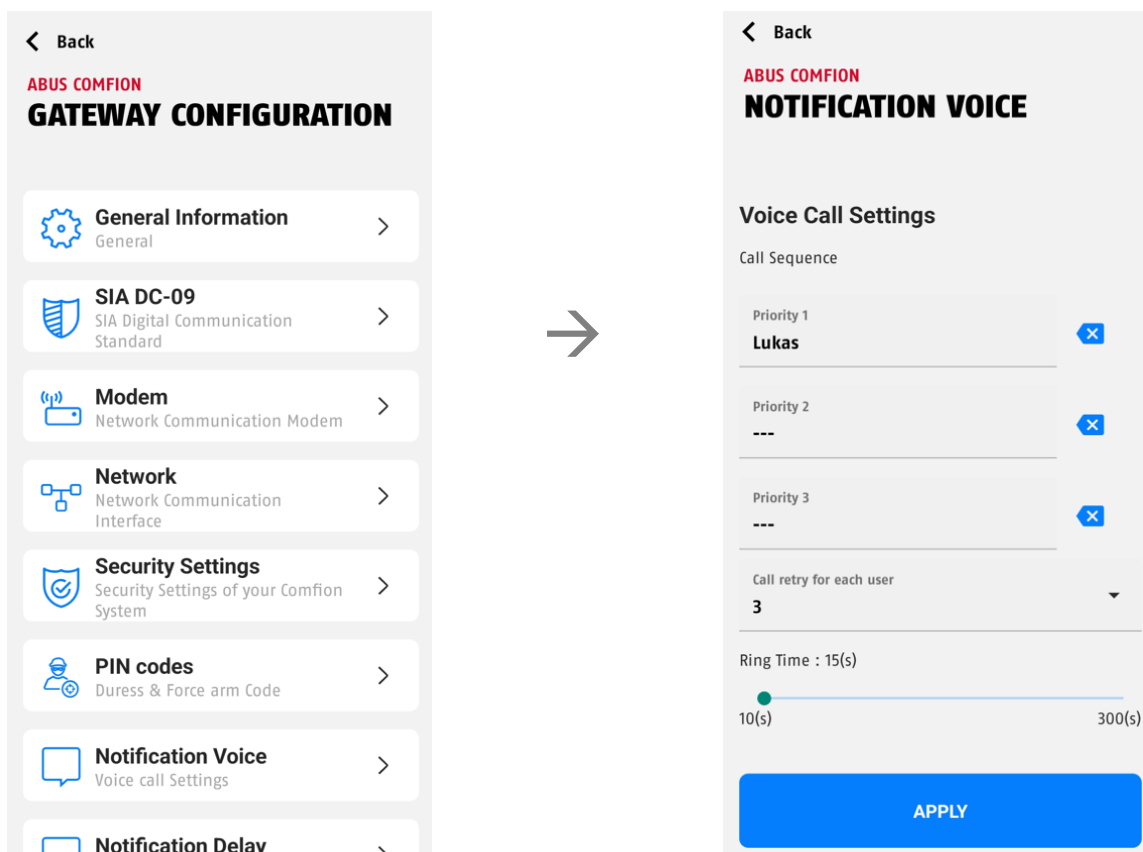
Als het e-mailadres waarnaar de meldingen moeten worden verzonden, afwijkt van het e-mailadres van uw account, kunt u een meldingsadres in uw account opgeven (zie **4.4.2 Meldingen**). Als u geen e-mailadres voor meldingen opgeeft, worden de e-mails naar het e-mailadres van uw account gestuurd.

6.3. Telefonische melding

Het Comfion Pro-beveiligingssysteem kan u bellen als er een alarm afgaat. Het systeem heeft geen spraakkiezer, wat betekent dat er geen spraakbericht wordt afgespeeld bij deze beloproep. De beloproep is alleen bedoeld als waarschuwing en moet de gebelde gebruiker op de hoogte brengen van een alarm. Het type alarm kan worden afgelezen aan de pushmelding die tegelijkertijd wordt verzonden.

Voor de belfunctie is een geplaatste simkaart met belfunctie vereist. Meer informatie over de GSM-module vindt u onder **5.1 GSM-module**.

- Om beloproepen te ontvangen, moet het telefoonnummer van de ontvanger opgeslagen zijn in het gebruikersaccount (zie **5. Communicatie**).
- U moet ook de oproepvolgorde definiëren onder "Centrale-configuratie" - "Telefoongesprek". Er kunnen maximaal 3 gebruikers achter elkaar worden gebeld.



 Aanwijzing	Het aantal herhalingen van oproepen per gebruiker is standaard ingesteld op 3. Dit betekent dat elke beller drie oproepen ontvangt. De oproep kan niet worden bevestigd.
---	---

6.4. SMS

Het Comfion Pro-systeem kan SMS-berichten versturen op basis van de gebeurtenissenlijst (zie **5. Communicatie**). U kunt ook automatiseringen gebruiken om sms-berichten te verzenden met vrij definieerbare tekst voor elke gebeurtenis.

Om sms-berichten te kunnen versturen, moet er een SIM-kaart in de module worden geplaatst en moet het kennisgevingsnummer in het account worden opgeslagen (zie **5. Communicatie**).

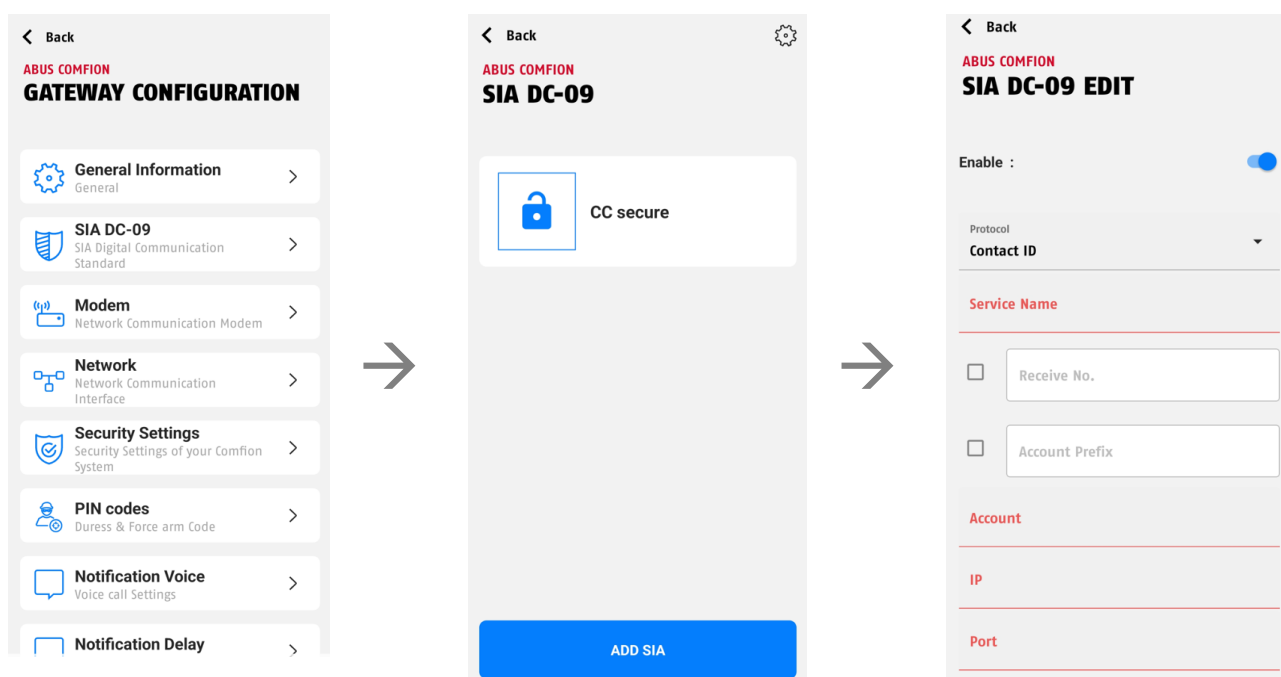
6.5. SIA DC-09 (meldkamer bijschakelen)

Het Comfion Pro draadloze beveiligingssysteem is voorzien van een digitale meldcentrale-koppeling die het Contact-ID-protocol via de SIA DC-09-standaard kan verzenden. U kunt meerdere bijschakelingen tegelijk configureren en zo communiceren met diverse beveiligingsdiensten.

Vul de gegevens die u van uw dienstverlener hebt ontvangen in de betreffende velden in. De twee grijze velden "Ontvanger" en "Klant-ID prefix" zijn over het algemeen niet vereist en hoeven alleen te worden geactiveerd als uw dienstverlener hier expliciet om vraagt.

In het veld "Statische testmelding" kunt u kiezen uit de volgende opties:

- **DC-09 Lijnbewaking** -> In het meldkamerprotocol geïntegreerde supervisie (moet door de meldkamer worden ondersteund)
- **CID-testbericht 602** -> Verzending van de Contact-ID-code 602 met het ingestelde interval
 - **Let op:** Het ingestelde interval bepaalt de tijd die verstrijkt sinds de laatste gebeurtenis naar de meldkamer is verzonden. Als er in de tussentijd een gebeurtenis naar de meldkamer wordt doorgestuurd, begint het interval opnieuw.



Via het tandwielpictogram rechtsboven in het scherm kunt u de geavanceerde instellingen openen. Hier kunt u het statische testbericht inschakelen en het interval instellen

 Aanwijzing	Een overzicht van de Contact-ID-codes vindt u in de bijlage (hoofdstuk 11.1)
---	---

7. Algemene informatie, onderhoud en opmerkingen

7.1. Centrale-configuratie

Onder het menu-item Centrale-configuratie vindt u alle belangrijke informatie over uw centrale en kunt u ook belangrijke instellingen voor het systeem verrichten

Nadat u het menu-item Centrale-configuratie hebt opgeroepen, ziet u de volgende informatie:

- Naam centrale → (invoerveld)
- Symbool → (kan worden vervangen door een eigen foto)
- Netwerk → (weergave van het type netwerkverbinding)
- Mob. netwerkstatus → (dropdownmenu)
 - Moduletype → (ingebouwde mobiele chip)
 - Simkaart → (indicatie of deze is geplaatst)
 - IMEI → (uniek 15-cijferig serienummer van de mobiele module)
 - Telefoongesprek → (kan worden weergegeven als er een simkaart is geplaatst)
 - LTE-verbinding → (weergave van de verbindingstatus)
 - Signaalsterkte (dBm) → (RSRP gemeten in -dBm, (aanbevolen signaalsterkte zie **hoofdstuk 5.1**)
- Stroomvoorziening → (indicatie netvoeding of accu)
- Firmware → (klik hierop om de firmwareversie en de release-opmerkingen te bekijken)
- Draadloze module → (weergave van de firmware van de draadloze module)
- Artikelnummer

Bevestigen

- Bevestigt de wijzigingen in dit menu.
- Daarna worden de wijzigingen ook in de ABUS-cloud bijgewerkt.

Centrale verwijderen

- Verwijdert de centrale uit de app en uit het ABUS-cloudaccount!

U kunt meer instellingenmenu's openen via het tandwielsymbool rechtsboven.

De instellingen voor SIA DC-09, telefoonoproep en de GSM-module zijn te vinden onder 5. Communicatie.

7.1.1. Algemene informatie

Onder het kopje "Opslag" wordt informatie weergegeven over het geplaatste opslagmedium (harde schijf en/of SD-kaart).

De gebruikte tijdzone en de NTP-server worden weergegeven onder de kop "Datum en tijd".

Met de knop 'Opnieuw opstarten' kunt u de centrale opnieuw opstarten.

7.1.2. Netwerk

In dit menu kunt u de netwerkinstellingen bekijken en indien nodig aanpassen.

U kunt kiezen uit drie methodes:

DHCP (standaardinstelling): Het Dynamic Host Configuration Protocol is een client-serverprotocol waarmee de Comfion Pro automatisch zijn IP-adres en andere bijbehorende gegevens van de router ontvangt.

PPPoE: Point-to-Point Protocol over Ethernet is een netwerkprotocol dat een directe verbinding binnen het interne netwerk beschikbaar stelt. Hiervoor is authenticatie met gebruikersnaam en wachtwoord vereist.

Statisch: Als u "statisch" selecteert, worden de netwerkgegevens van de Comfion Pro handmatig ingevoerd. Bespreek dit met de exploitant van het netwerk en wijs geen IP-adres toe uit de DHCP-pool.

 Aanwijzing	Onjuiste IP-instellingen betekenen dat uw systeem geen verbinding kan maken met het netwerk, waardoor het niet bereikbaar is voor de app. Druk in dat geval 6 seconden lang op de toets "Netwerk resetten" (nr. 14) aan de achterkant van de installatie en laat deze vervolgens los. De centrale zal dan opnieuw opstarten en de netwerkinstellingen terugzetten naar de standaard DHCP-instellingen.
---	---

7.1.3. veiligheidsinstellingen

Onderhoudsmodus	Aan/Uit (Voorinstelling: UIT)	De onderhoudsmodus is bedoeld voor de installatie en het onderhoud van het systeem. Zolang de onderhoudsmodus actief is, kan de installatie geen alarmen activeren.
Zoneblokkering	3x-20x (Voorinstelling 5x)	Als een partitie vaker wordt geactiveerd dan is ingesteld, zal deze partitie niet meer worden geactiveerd totdat de alarmen uit de alarmgeschiedenis zijn verwijderd
Max. aantal herhalingen van toetsenveldinvoer	3x-20x (Voorinstelling 5x)	Geeft aan na hoeveel keer een verkeerde pincode op het bedieningspaneel is ingevoerd, dit wordt geblokkeerd
Time-out bediendeel	5-180 sec (Voorinstelling : 30 sec.)	Instelling hoe lang het bedieningspaneel wordt geblokkeerd na X onjuiste invoer
Ingangsvertraging	5-45 sec (Voorinstelling : 10 sec.)	Bij een ingeschakelde installatie wordt de ingangsvertraging weergegeven op het draadloos bedieningspaneel.
Uitgangsvertraging	5-45 sec (Voorinstelling : 30 sec.)	De vertragingstijd die op het bedieningspaneel wordt weergegeven voordat de centrale in de ingeschakelde toestand gaat.
Verzendingvertraging	5-180 sec (voorinstelling 60 sec.)	Als deze eigenschap in de partitie is ingeschakeld, wordt de verzending van een triggering met de ingestelde tijd vertraagd.
Spanning lograpport vertraging	0-30 min (Voorinstelling : 0 min)	Instelbare vertraging bij de melding van een spanningsuitval (12 V DC)
Inbraaksirene activeren	Aan/Uit (Voorinstelling : AAN)	Aansturing van de sirene bij een inbraakalarm
Sireduur inbraakalarm	5-180 sec (voorinstelling 60 sec.)	Duur van de akoestische signalering via sirenes die in het systeem zijn geïntegreerd
Sabotagesirene activeren	Aan/Uit (Voorinstelling : AAN)	Aansturing van de sirenes bij een sabotagealarm
Sabotagealarm sireduur	5-180 sec (voorinstelling 60 sec.)	Duur van de akoestische signalering via sirenes die in het systeem zijn geïntegreerd
Logo-LED weergeven: Sabotage	Aan/Uit (Voorinstelling : AAN)	Geeft het alarmtype "sabotage" visueel weer via het verlichte ABUS-logo. (Rood knipperend)
Overval sirene activeren	Aan/Uit (Voorinstelling : UIT)	Aansturing van de sirenes bij een overvalalarm
Sireduur bij overvalalarm	5-180 sec (voorinstelling 60 sec.)	Duur van de akoestische signalering via sirenes die in het systeem zijn geïntegreerd
Logo-LED weergeven: Overval	Aan/Uit (Voorinstelling : AAN)	Geeft het alarmtype "Overval" visueel weer via het verlichte ABUS-logo. (Rood knipperend)
Sirene inschakelen	Aan/Uit (Voorinstelling : AAN)	Aansturing van de sirenes bij een watalarm
Watalarm - sireduur	5-180 sec (voorinstelling 60 sec.)	Duur van de akoestische signalering via sirenes die in het systeem zijn geïntegreerd
Logo-LED weergeven: Overstroming	Aan/Uit (Voorinstelling : AAN)	Geeft het alarmtype "Overstroming" visueel weer via het verlichte ABUS-logo. (Rood knipperend)
Sirene brand activeren	Aan/Uit (Voorinstelling : AAN)	Aansturing van de sirenes bij een brandalarm
Duur van brandalarmsirene	5-180 sec (voorinstelling 60 sec.)	Duur van de akoestische signalering via sirenes die in het systeem zijn geïntegreerd
Logo-LED weergeven: brandalarm	Aan/Uit (Voorinstelling : AAN)	Geeft het alarmtype "Brand" visueel weer via het verlichte ABUS-logo. (Rood knipperend)
Overval-app: sirene activeren	Aan/Uit (Voorinstelling : UIT)	Aansturing van de sirenes bij een via de app geactiveerd overvalalarm
Overval-app: sireduur	5-180 sec (voorinstelling 60 sec.)	Duur van de akoestische signalering via sirenes die in het systeem zijn geïntegreerd
Logo-LED weergeven: Overval-app	Aan/Uit (Voorinstelling : AAN)	Geeft het alarmtype "Overval-app" visueel weer via het verlichte ABUS-logo. (Rood knipperend)
Sirene maskeren activeren	Aan/Uit (Voorinstelling : AAN)	Aansturing van sirenes bij het afdekken van een melder (afdekbewaking)

Maskering van de sireneduur	5-180 sec (Voorinstelling : 30 sec.)	Duur van de akoestische signalering via sirenes die in het systeem zijn geïntegreerd
Logo-LED weergeven: Maskering	Aan/Uit (Voorinstelling : AAN)	Geeft het alarmtype "Dekselbewaking" visueel weer via het verlichte ABUS-logo. (Rood knipperend)
Intruder Network	Aan/Uit (Voorinstelling : UIT)	Inschakelblokkering door een netwerkfout deactiveren
Intruder Battery	Aan/Uit (Voorinstelling : UIT)	Inschakelblokkering door een accufout deactiveren
Intruder Ac Lost	Aan/Uit (Voorinstelling : UIT)	De beveiliging tegen stroomuitval (12 V DC) uitschakelen
Automatische reset inschakelen	AAN/UIT (Voorinstelling : AAN)	AAN: De reset wordt uitgevoerd bij het uitschakelen. Zodra alle geactiveerde melders zich weer in de normale toestand bevinden, verdwijnt het waarschuwingsoverzicht uit het dashboard wanneer het systeem wordt uitgeschakeld. UIT: Alarmen en fouten moeten altijd handmatig worden gereset.
NFC-modus (open)	AAN/UIT (Voorinstelling : UIT)	UIT: Er kunnen uitsluitend Mifare DESFire-transponders van ABUS worden gebruikt, omdat deze om veiligheidsredenen worden gecontroleerd voor de Comfion-applicatie. Transponders van derden en Mifare Classic-transponders kunnen niet worden gebruikt. AAN: Alle Mifare Classic- en Mifare Desfire-transponders kunnen worden gebruikt (zie het opmerkingenveld hieronder voor beperkingen).
Fabrieksinstellingen herstellen toestaan	AAN/UIT (Voorinstelling : AAN)	UIT: De centrale kan niet met de reset-toets worden gereset AAN: De centrale kan met de reset-toets worden gereset.
Sabotagedetectie deactiveren	AAN/UIT (Voorinstelling : UIT)	OPMERKING: de sabotageherkenning van alle geprogrammeerde apparaten is gedeactiveerd.
Vervolg op de ingang in hetzelfde gebied	AAN/UIT (Voorinstelling : UIT)	UIT: De partities die op de ingang volgen, reageren op de ingangsvertraging, ongeacht het bereik AAN: Zones die op een ingang zijn aangesloten, reageren alleen op de ingangsvertraging die in hetzelfde gebied is geactiveerd.



Aanwijzing

Mifare DESfire-transponder van andere fabrikanten werken alleen als ze een vaste UID hebben. Er mag geen random ID-mechanisme geactiveerd zijn op de transponders.

7.1.4. Pincodes

In dit menu kunt u de bedreigingscode en de code voor het geforceerde inschakelen wijzigen. Deze codes gelden voor alle gebruikers van het systeem en bestaan uit 3 cijfers

De codes kunnen alleen worden gebruikt in combinatie met een Comfion-draadloos bedieningspaneel

 Aanwijzing	De dreigingscode en de noodcode worden samen met de gebruikerscode ingevoerd, d.w.z.: Gebruikerscode (4 cijfers) → Code voor dreigings-/noodactivering (3 cijfers), bijv. 1357999
---	--

Bedreigingscode

- Door deze code in te voeren op het draadloos bedieningspaneel van Comfion kan het systeem geforceerd worden uitgeschakeld
- De Comfion Pro wordt uitgeschakeld, maar er wordt wel een melding verzonden naar de ontvangers die zijn geconfigureerd.

Code voor geforceerd inschakelen

- Zie **hoofdstuk 6.7.3**
- Maakt het mogelijk om één of meerdere deelgebieden in te schakelen bij geopende zones, zonder dat er een overbruggingsprocedure plaatsvindt.

7.1.5. Vertragingen bij de kennisgeving

In dit menu kunt u de vertragingstijden voor **meldingen bij netwerkuitval** instellen.

Vertraging bij servermelding:

Vertragingstijd bij uitval van de cloudverbinding. Definiëert de vertraging, bijvoorbeeld bij cloudproblemen, voordat er een melding wordt verzonden. (Standaardinstelling = 10 sec.); (Instelbaar van 10 tot 600 sec.)

Vertraging bij de melding aan de client:

Vertragingstijd bij verlies van de internetverbinding op de Comfion Pro-centrale. Dit kan bijvoorbeeld worden veroorzaakt door uitval in de DSL-verbinding, een ontbrekende LAN-kabel of uitval bij de router. (Standaardinstelling = 0 sec.); (Instelbaar van 0 tot 600 sec.)

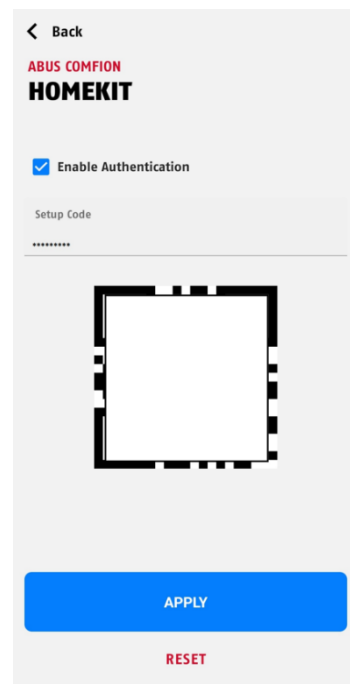
 Aanwijzing	Afhankelijk van de netwerkinfrastructuur kan het raadzaam zijn om de vertragingstijd iets te verhogen, vooral wanneer de router veel IP-clients beheert.
---	--

Als u op '**Bevestigen**' klikt, worden de wijzigingen doorgevoerd.

7.1.6. HomeKit

Voeg een nieuw apparaat toe in de Apple HomeKit-gebruikersinterface

- Tijdens het dialoogvenster wordt u gevraagd de hier getoonde QR-code te scannen en/of de 8-cijferige koppelingscode in te voeren.



7.1.7. Backup

 Aanwijzing	Het back-up-bestand van uw centrale wordt om veiligheidsredenen volledig versleuteld opgeslagen in de ABUS Cloud.
---	--

Een back-up maken

In het menu Back-up van de configuratie van de centrale kunt u handmatig een back-up maken en de automatische back-up inschakelen. Er wordt wekelijks een automatische back-up gemaakt.

Back-up terugzetten

 Aanwijzing	Houd er rekening mee dat de nieuwe centrale al is geüpdated naar de huidige firmwareversie voordat de back-up wordt geïmporteerd.
---	--

Ga als volgt te werk om de back-up in een nieuwe centrale te importeren:

1. Koppel de centrale waarvan de back-up afkomstig is, indien dat nog niet is gebeurd, los van het netwerk en schakel deze uit.
2. Tik in het centrale-overzicht in de app op het +-symbool om een nieuwe centrale toe te voegen
3. Selecteer 'Back-up importeren'
4. Scan de QR-code op de achterkant van uw nieuwe centrale
5. Selecteer de centrale waarvan u de back-up wilt laden
Opmerking: Na het importeren wordt de back-up uit de cloud verwijderd en werken de componenten niet meer op de oude centrale.
6. Voer de gewenste naam van uw nieuwe centrale in
7. Na bevestiging wordt er een verificatiecode naar het e-mailadres van de eigenaar van de installatie gestuurd. Voer deze code in de app in en klik op 'Importeren starten'
8. De import wordt nu uitgevoerd. U kunt uw app nu sluiten en wachten tot u de pushmelding ontvangt dat de centrale online is en er stroom is.

Om een configuratie op dezelfde hardware (centrale) te herstellen, gaat u als volgt te werk:

1. Zet de betreffende centrale terug op de fabrieksinstellingen (houd de resetknop 10 seconden ingedrukt -> zie 6.5.1)
2. Tik in het centrale-overzicht in de app op het +-symbool om een nieuwe centrale toe te voegen
3. Selecteer 'Herstellen'
4. Scan de QR-code op de achterkant van uw centrale
5. Voer de gewenste naam van uw centrale in
6. De import wordt nu uitgevoerd. U kunt uw app nu sluiten en wachten tot u de pushmelding ontvangt dat de centrale online is en er stroom is.

7.1.8. Informatie over WLX

Hier vindt u een overzicht van de Fallback-machtigingen, incl. de resetkaart

Fallback-machtiging:

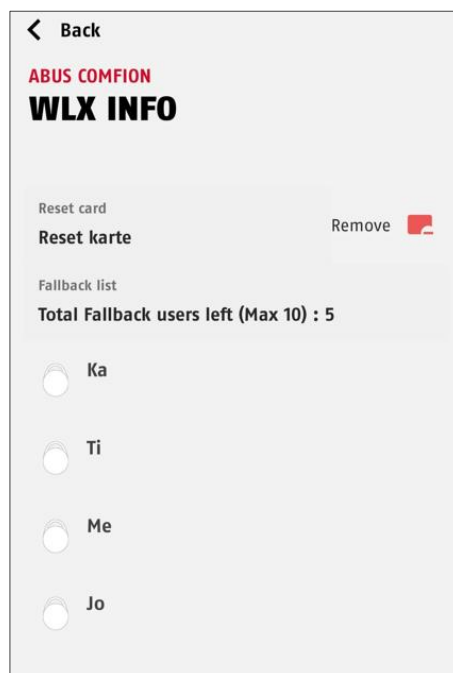
- De Fallback-toegangsbevoegdheid is direct in de cilinder opgeslagen en geeft toegang wanneer er geen draadloze verbinding is met de Comfion Pro-centrale en de BUS-WLX-module. In het Comfion Pro-systeem kunnen maximaal 10 fallback-toegangsrechten worden toegekend (de resetkaart is altijd een fallback-medium).
- Als de draadloze verbinding wordt onderbroken, moet het geautoriseerde medium drie keer tegen de wAppLoxx-cilinder worden gehouden (telkens wachten tot het signaal klinkt)
- De Fallback-machtiging wordt direct in de NFC-tag-instellingen van de gebruiker opgeslagen; zie **hoofdstuk 4.4** Gebruikers bewerken

Resetkaart

- De resetkaart wordt meegeleverd bij de Comfion Pro BUS-WLX-module.
- Nadat de eerste wAppLoxx-component (cilinder of wandlezer) is geprogrammeerd, wordt het proces voor het programmeren van de resetkaart automatisch gestart.
- De resetkaart is nodig om een cilinder te resetten (in aanvulling op de systeemkaart)
- Mocht de resetkaart kwijtraken, dan kunt u deze hier via 'Verwijderen' wissen en daarna een nieuwe resetkaart programmeren. Na het verwijderen begint het programmeerproces onmiddellijk!

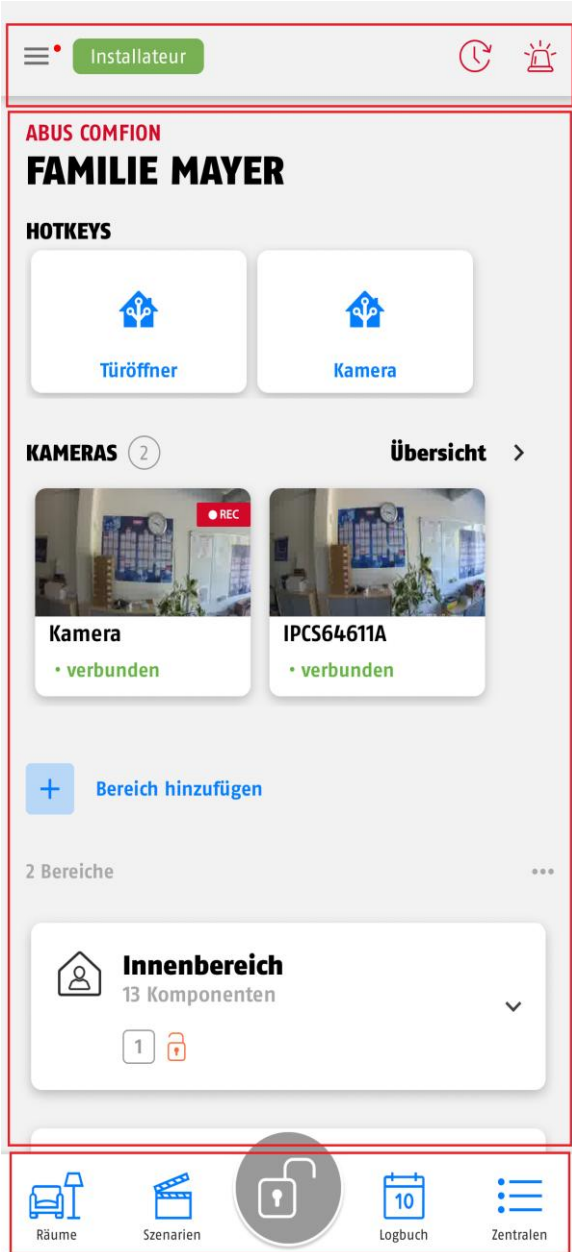
Fallback-lijst

- Naast de resetkaart verschijnen hier maximaal 9 andere tags met Fallback-autorisatie.



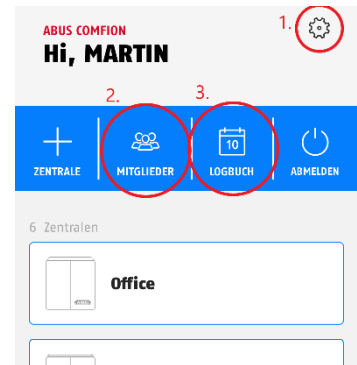
7.2. Dashboard (systeem ingesteld)

U kunt het systeem bedienen via het Dashboard en ook een groot deel van uw werk als installateur uitvoeren.

	Kopbalk: •  Configuratie en gebruikersinstellingen •  Gebruikersrol (alleen installateur) •  Firmware-update (indien beschikbaar) •  Paniek-alarm activeren Dashboard / Functiebereik • Hotkey-knoppen ○ Een korte druk op de toets start de scène en de uitvoering wordt kort bevestigd met  ○ ingedrukt houden om de scène te configureren • Previewbeelden van de camera ○ Klik op de miniatuurafbeelding om naar de stream te gaan ○ Als u op 'Overzicht' klikt, gaat u naar de detailpagina van de camera en kunt u de configuratie aanpassen • Overzicht van de deelgebieden ○ Klik op  om de toegewezen componenten en hun status weer te geven (indien ingesteld) ○ Klik op  om de sortering van de partities aan te passen. Navigatiebalk • Ruimtes (& componentenlijst) zie 3.2.4 en 3.2.5 • Scenario's (scènes en automatiseringen) zie 6.4 • Alarmmodi (slotpictogram) – zie 3.2.8 • Logboek (lijst van gebeurtenissen & filterfunctie) Centrales (overzicht) – zie 6.3
--	---

7.3. Centrale-overzicht

In het centrale-overzicht van het systeem kunt u naast het toevoegen van nieuwe centrales de bestaande centrales bekijken en openen, uw accountgegevens bewerken (1), uw leden beheren (2) en het account-logboek bekijken (3).



7.3.1. Accountgegevens

Ga naar het centrale-overzicht via het tandwielpictogram.

Zurück

ABUS COMFION
ACCOUNT INFORMATIONEN

Face/Touch ID aktivieren : ☐

Name

E-Mail

Benachrichtigungssprache
Deutsch

Telefonnummer

Benachrichtigungs-Rufnummer

Benachrichtigungs-E-Mail

Erstellt am
2024-11-12 10:50:51

BESTÄTIGEN

ACCOUNT VERWALTUNG

- Face ID/Touch ID activeren
 - Beveiligt de app met gezichtsherkenning of vingerafdruk
- Accountnaam (weergegeven in centrale & logboek)
- Account-e-mail
- Taal voor berichten
 - Definiëert de taal voor pushmeldingen, e-mail- en SMS-meldingen, het logboek, partities en ruimtes
- Telefoonnummer
- Kennisgevingstelefoonnummer voor sms & beloproepen
- Kennisgevingsmail voor verzending per e-mail vanuit de centrale
- Tijdstip waarop het account is aangemaakt
- Bevestigingsknop om de invoer op te slaan
- In-app verwijderfunctie van het ABUS-account

7.3.2. Leden

In de Comfion-app kunt u een ledenlijst bijhouden. Dit is puur optioneel en is niet nodig voor het gebruik van de Comfion Pro-systemen. Met de ledenlijst kunt u bij het toevoegen/uitnodigen van nieuwe gebruikers in een centrale deze heel eenvoudig uit uw leden selecteren.

7.3.3. Account-logboek

Alle berichten van systemen met geautoriseerde toegang worden vermeld in het account-logboek. Als de toegang tot een systeem is geblokkeerd, worden logboekvermeldingen van die centrale niet opgeslagen in het accountlogboek.

7.4. Automatiseringen & scènes

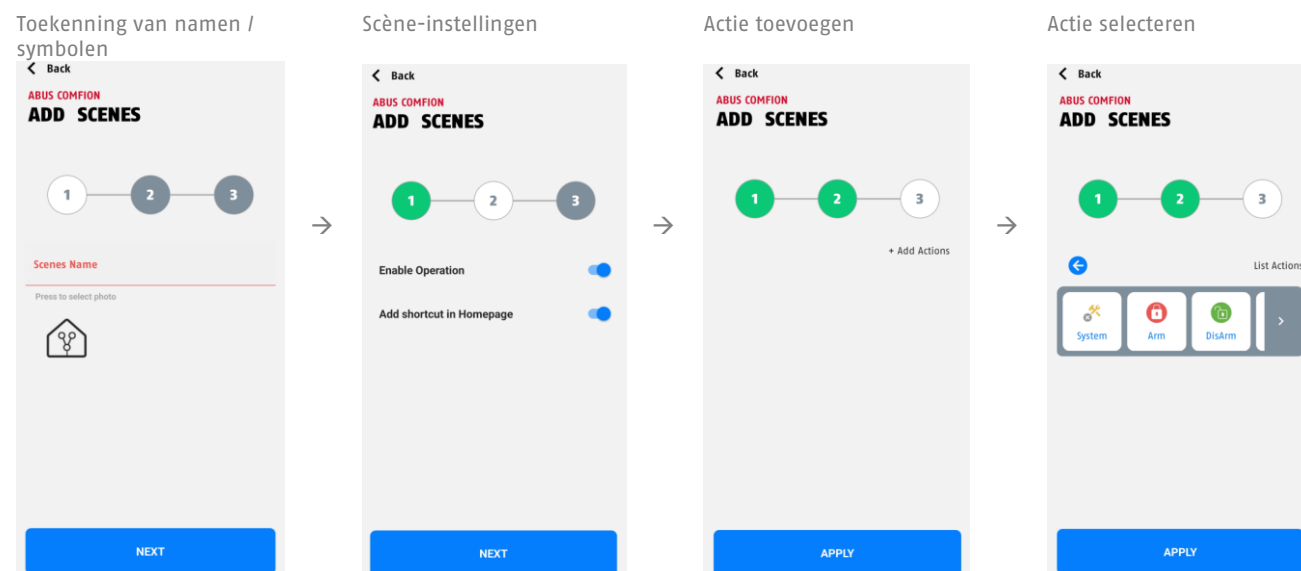
Met het Comfion Pro-systeem kunt u tot 100 scenario's configureren. Deze scènes of automatiseringen kunnen volledig vrij worden ingesteld, waardoor u maximale flexibiliteit hebt.

Onder het tabblad 'Scenario's' kunt u zowel scènes als automatiseringen toevoegen.

 Let op	Er mogen geen automatiseringen worden aangemaakt die elkaar tegenspreken of in een cirkel oproepen plegen. Dit kan leiden tot ernstige werkingsproblemen bij de centrale.
 Aanwijzing	Zorg ervoor dat u een interval van minstens 5 seconden laat tussen twee schakelcommando's voor hetzelfde apparaat om een vlotte werking te garanderen.

Scène = actie die door een gebruiker via de app wordt geactiveerd (hotkey). Kan worden weergegeven in het dashboard. Voorbeeld: Contactdoos AAN/UIT via app

Voorbeeldconfiguratie van een scène:



Stap 1:

- De naam van de scène is een verplicht veld
- Wijzig het symbool door op het pictogram te klikken

Stap 2:

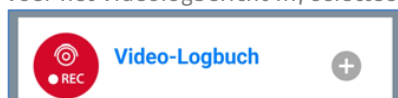
- Geef aan of de scène actief of inactief moet zijn (inactief = de naam van de scène is grijs weergegeven)
- Met 'Weergeven op dashboard' wordt de scène weergegeven in het gedeelte 'Hotkeys' van het dashboard

Stap 3 (actie toevoegen):

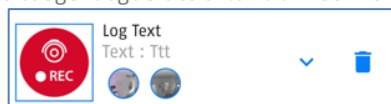
- Selecteer de actie uit de lijst door erop te klikken, voer indien nodig aanvullende gegevens in en voeg deze vervolgens toe door op het "+"-symbool te klikken.

Voorbeeld: Videologboek:

- Voer het videologbericht in, selecteer de camera's en druk vervolgens op het "+"-symbool



- Sommige acties kunt u direct toevoegen door op het "+"-symbool te klikken en daarna door op het pictogram te klikken om verdere instellingen toe te voegen.
- Een reeds toegevoegde actie kunt u weer verwijderen door op de prullenbak te klikken



- U kunt meerdere acties configureren; deze worden vervolgens achter elkaar uitgevoerd. U kunt de volgorde van uitvoering wijzigen door op het pictogram  te klikken. Daarna kunt u de acties met drag & drop verplaatsen. Druk nogmaals op  om de wijziging op te slaan.
- Rond de configuratie van de scène af door op 'Bevestigen' te klikken.

De volgende acties kunnen worden toegevoegd:

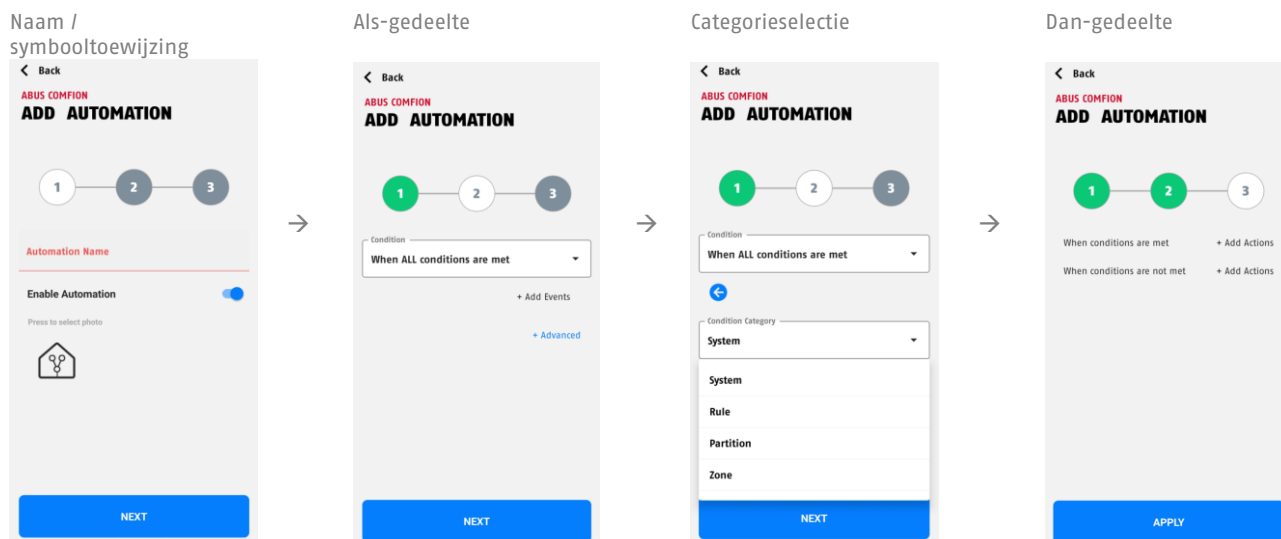
Systeem	Videologboek	Een logboekvermelding aanmaken met een logbericht en een fragment van de camerabeelden (15 sec.) of van het PIR-Cam-beeld
	Systeem opnieuw opstarten	Voer een herstart van de Comfion Pro-centrale uit.
	Push-evenement-video	Maakt een pushmelding aan met berichttekst en camerabeelden en verzendt deze naar de geselecteerde ontvangers
	Tekst van push-melding	Maak een pushmelding aan met de tekst van het bericht en verstuur deze naar de geselecteerde ontvangers
	Vertraging	Voert de scène uit met een vertraging van het opgegeven aantal seconden, of vertraagt opeenvolgende acties.
INGESCHAKELD		Schakelt een deelgebied van het systeem in Opmerking: Nadat u deze actie hebt toegevoegd, moet u het deelgebied nog instellen door op het pictogram te klikken: 
Uitgeschakeld		Schakelt een partitie van het systeem uit Opmerking: Nadat u deze actie hebt toegevoegd, moet u het deelgebied nog instellen door op het pictogram te klikken: 
Scène		Voert een reeds geconfigureerde scène uit. Opmerking: Kies deze functie om meerdere scènes tegelijkertijd (of met behulp van de vertraging op verschillende tijdstippen) uit te voeren.
Comfion-wandcontactdoos	Uitschakelen	Schakelt de contactdoos in
	Inschakelen	Schakelt de contactdoos uit
	Schakelen	Voert een omschakeling van het stopcontact uit (aan → uit, uit → aan)
Comfion-relais-module	Uitschakelen	Schakelt de relaismodule in
	Inschakelen	Schakelt de relaismodule uit
	Schakelen	Schakelt de relaismodule om (aan via → , uit via →)
Comfion-jaloezie-module	Open	Brengt de lamellen van de jaloezieën naar de eindpositie: open en omhoog
	Sluiten	Brengt de lamellen van de jaloezieën naar de eindpositie gesloten en omlaag
	Stop	Stop de opdracht Openen of Sluiten
	100% omhoog (50% / 1/3 / 25%)	Brengt de lamellen van de jaloezieën met de opgegeven waarde omhoog
	100% sluiten (50% / 1/3 / 25%)	Laat de lamellen van de jaloezieën met de opgegeven waarde naar beneden gaan
	Lamellen 100% openen (50% / 1/3 / 25%)	Opent de lamellen van de jaloezieën met de opgegeven waarde

	Lamellen sluiten 100% (50% / 1/3 / 25%)	Sluit de lamellen van de jaloezieën met de opgegeven waarde
	Handmatige besturing	Individuele instelling van de lamellen van de jaloezieën. Door te klikken op het pictogram:  Kunnen de hellingshoek (5 standen) en de hoogte (10 standen) kunnen worden ingesteld.
Comfion Pro-centrale	Uitgang Aan	Schakelt de relaisuitgang van de Comfion Pro-centrale in
	Uitgang uit	Schakelt de relaisuitgang van de Comfion Pro-centrale uit
	Uitgang omschakelen	Schakelt de relaisuitgang van de Comfion Pro-centrale om.
Comfion binnensirene	Brand	Speelt de gesproken melding "brandalarm" af
	Alarm	Schakelt het sirenegeluid in (onder  duur instellen, max. 180 s)
	Stop	Schakelt het sirenegeluid uit
	Piep (signaaltoon)	Schakelt het bevestigingsgeluid in (onder  het aantal herhalingen (max. 30) en het interval van de piëzo (max. 30 s) instellen
	Mislukt	Schakelt het geluidssignaal bij een mislukking in (onder  het aantal herhalingen (max. 30) en het interval van de piëzo (max. 30 s) instellen
	Deurbel	Schakelt het deurbelgeluid in (onder  het aantal herhalingen (max. 30) en het interval van de piëzo (max. 30 s) instellen
	Overval	Speelt de gesproken melding "Overvalalarm" af
	waterniveau alarm	Geeft de gesproken mededeling weer
Comfion-buitensirene	Alarm	Schakelt het sirenegeluid in (onder  duur instellen, max. 180 s)
	Stop	Schakelt het sirenegeluid uit
	Piep (signaaltoon)	Schakelt het bevestigingsgeluid in (onder  het aantal herhalingen (max. 30) en het interval van de piëzo (max. 30 s) instellen
	Deurbel	Schakelt het gonggeluid in (onder  het aantal herhalingen (max. 30) en het interval van de piëzo (max. 30 s) instellen
Comfion-rookmelder	Alarm stoppen	Schakelt het alarmgeluid van de Comfion-rookmelder uit. (de melder gaat opnieuw af bij detectie)
WLX-uitgang (Comfion Hybrid-module)	Uitgang 1, 2, 3 aan	Schakelt uitgang 1, 2 of 3 van de Comfion-hybridemodule in
	Uitgang 1, 2, 3, uit	Schakelt uitgang 1, 2 of 3 van de Comfion-hybridemodule uit
	Uitgang 1, 2, 3 omschakelen	Voer de omschakeling uit voor uitgang 1, 2 of 3 van de hybride Comfion-module
Comfion PIR-camera / PIR-buitencamera	Snapshot	Maak een handmatige beeldopname
WLX Pro-cilinder (toegang/indringers)	Kantoormodus (permanente toegang)	Een aanvulling op de kantoormodus (maakt toegang mogelijk zonder NRC-tag) Door te klikken op het pictogram:  wordt gekozen of de kantoormodus moet worden "ingeschakeld" of "uitgeschakeld".
	Vrijgave op afstand (Op afstand openen)	Koppelt de sluitcilinder via de app en verleent zo toegang. Door te klikken op het pictogram:  stelt u de koppelingstijd in (max. 180 sec.)
WLX Pro Wandlezer (toegang/indringers)	Vrijgave op afstand (Op afstand openen)	Stuurt de deuropener (uitgang op de Bridge-Box) aan via de app en verleent zo toegang. Door te klikken op het pictogram:  Stelt u de impulsduur in (6 of 12 s)
IP-camera (IPxxxxxxx)	Ga naar Preset	Lijnt de PTZ-camera op een vooraf gedefinieerde positie uit. Door te klikken op het pictogram:  Selecteert u positie 1, 2, 3 of 4.

- Klik op reeds geconfigureerde scènes om deze opnieuw te bewerken of te verwijderen.

Automatisering = bestaat altijd uit een 'als'- en een 'dan'-deel. Vrij configureerbaar.
Voorbeeld: Wanneer het systeem ingeschakeld is, dan het licht uit

Voorbeeldconfiguratie van een automatisering:



Stap 1:

- Vul de naam van de automatisering in (verplicht veld)
- Leg vast of de automatisering ingeschakeld of uitgeschakeld is
- Wijzig het symbool door op het pictogram te klikken

Stap 2: (Wanneer gebeurtenis vastleggen)

- Kies tussen een En-voorwaarde of een Of-voorwaarde.
 - Met de EN-koppeling moet aan ALLE voorwaarden worden voldaan om de actie uit te voeren. Er moet aan minstens EEN voorwaarde zijn voldaan om de actie uit te voeren bij de OF-koppeling.
- Selecteer de gebeurtenis "Als".
 - Er kunnen meerdere gebeurtenissen worden ingesteld, waarbij aan ALLE (en-voorwaarden) ofwel aan ten minste ÉÉN (of-voorwaarde) moet worden voldaan.
- De volgende gebeurtenissen kunnen worden geselecteerd:
 - Systeem -> Hier vindt u systeemgebeurtenissen zoals een stroomstoring, maar ook het tijdschema
 - Regel -> Bestaande automatiseringen kunnen in een automatisering worden geïntegreerd ...
 - Partitie -> Partitiegebeurtenissen zoals ingeschakeld/uitgeschakeld, inbraak, klaar om in te schakelen en nog veel meer zijn hier te vinden
 - Zone -> Alle zone-gerelateerde gebeurtenissen kunnen hier worden gevonden (bijv. zone-inbraak)
 - Ruimte -> Alle componenten en de bijbehorende gebeurtenissen kunnen hier worden gevonden (bijv. openingsmeldercontact geopend of knop van wandschakelaar ingedrukt)
- Selecteer daarnaast onder "Geavanceerd" ...
 - ... hoe lang de ingestelde voorwaarden moeten gelden voordat de actie wordt uitgevoerd. De actie wordt alleen uitgevoerd als aan de voorwaarden voor de ingestelde tijdsperiode is voldaan en deze niet meer veranderen.
 - Voorbeeld: Als de deur 30 seconden openstaat, dan... een pushmelding verzenden.

Stap 3: (Vervolgens de gebeurtenis vastleggen)

- De "Als, dan" -> actie wordt uitgevoerd als aan de voorwaarden in het "Als"-gedeelte is voldaan
 - De acties die hier configureerbaar zijn, komen overeen met die in de scène-configurator (stap 3)
- "Als voorbij, dan" -> actie wordt uitgevoerd als de voorwaarden in het "Als"-gedeelte NIET langer van toepassing zijn

Een scène/automatisering bewerken

Om te bewerken houdt u het pictogram van de scène/automatisering ongeveer 2 seconden ingedrukt en laat u het vervolgens los

Een scène/automatisering verwijderen

U kunt een scène/automatisering verwijderen door naar de bewerkingsmodus te gaan (zie "Een scène/automatisering bewerken") en vervolgens op de knop "Scène/automatisering verwijderen" onderaan het scherm te klikken.

7.5. Resets



7.5.1. Fabrieksreset

Om de centrale terug te zetten naar de fabrieksinstellingen, houdt u de reset-toets (toets 12, zie *2.3 Beschrijving van het apparaat*) langer dan 10 seconden ingedrukt en laat u deze vervolgens los. De leds van de centrale gaan na enkele seconden uit en de centrale start opnieuw op. Na het opnieuw opstarten bevindt zich het centrale systeem in de fabrieksinstellingen en kan zij opnieuw worden geconfigureerd.

7.5.2. Opnieuw opstarten (reboot)

Houd de herstarttoets (toets 13) 2 seconden ingedrukt. De leds van de centrale gaan even uit. De centrale voert een herstart uit.

 Opmerking	Bij de hier beschreven herstart wordt de stroomtoevoer niet onderbroken. Als de centrale bijvoorbeeld in het kader van een herstartproces handmatig van de stroomtoevoer wordt losgekoppeld, voert de centrale na afloop van het herstartproces een controle uit van alle aangesloten apparaten, en deze controle leidt tot veel logboekvermeldingen.
---	--

7.5.3. User-reset

Om de gebruikers van de installatie te resetten of alle gebruikers uit de installatie te verwijderen, drukt u binnen 5 seconden 5 keer op de netwerk-reset-toets (nr. 14). Na enkele seconden gaat het internetlampje korte tijd rood branden. U zou op de gekoppelde apparaten een pushmelding moeten ontvangen dat de betreffende centrale is verwijderd.

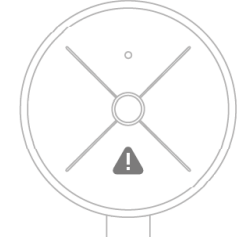
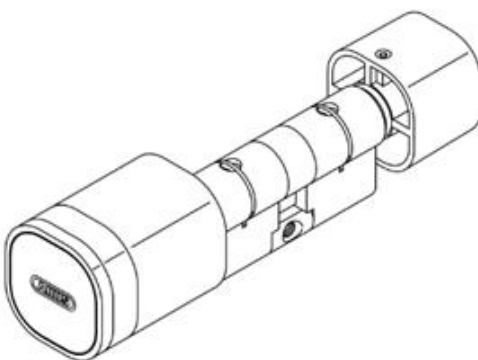
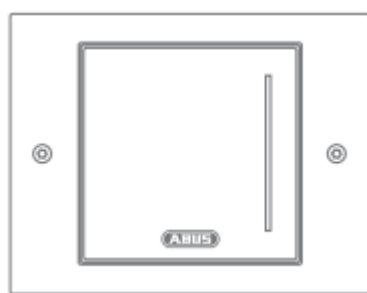
Als alle LED-lampjes weer groen branden (de internet-LED kan groen knipperen), kunt u de installatie via het +-symbool in uw app opnieuw toevoegen.

7.5.4. Netwerketreset

Als u uw installatie niet meer via het netwerk kunt bereiken vanwege onjuiste IP-instellingen, kunt u de centrale resetten naar DHCP. Houd hiervoor de toets voor het resetten van het netwerk aan de achterkant van de centrale (nr. 14) 6 seconden ingedrukt. Na enkele minuten zou de installatie weer bereikbaar moeten zijn.

7.6. Bediening

7.6.1. Inschakelen / uitschakelen

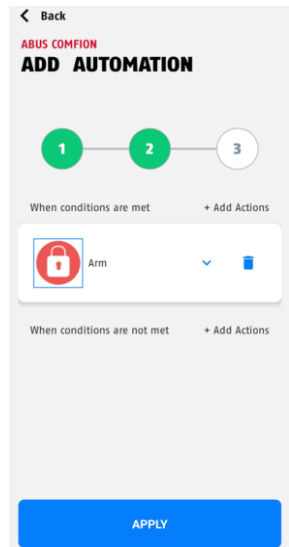
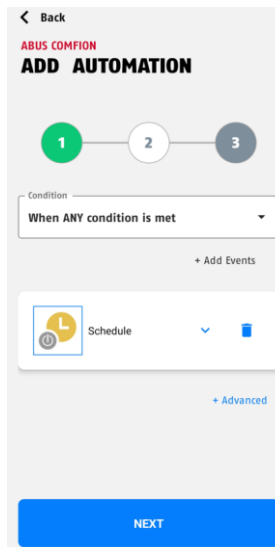
APP: Het in- en uitschakelen van het alarm kan in de app worden uitgevoerd via de alarmmodi. Klik hiervoor in het dashboard op de knop in het midden onderaan het scherm (het slot-symbool) en selecteer vervolgens de gewenste actie (bijv. alles inschakelen).	
BEDIENINGSPANEEL: U kunt het systeem via een draadloos bedieningspaneel in- en uitschakelen. Voer hiervoor uw gebruikerscode in of houd de NFC-tag voor het bedieningspaneel en klik vervolgens op de actieknop (slottoetsen) die u wilt uitvoeren. Meer informatie vindt u in de gebruikershandleiding of in de handleiding van het bedieningspaneel	
AFSTANDBEDIENING: U kunt de toetsen van uw draadloze afstandsbediening toewijzen aan de alarmmodi en met een druk op de toets de betreffende actie uitvoeren. U vindt deze instelling onder de afstandsbediening.	
WLX-Pro-cilinder / WLX Pro-wandlezer: gebeurt direct op de lezer Inschakelen: • RFID-tag bij de lezer houden • Vergrendel het apparaat evt. binnen de openingstijd en houd de RFID-tag opnieuw voor de lezer • Inschakelen gelaagd: Rode LED 1 x lang • Niet geslaagd: Rode LED 6 x Uitschakelen: • RFID-tag bij de lezer houden • Nadat het uitschakelen is gelukt, schakelt de cilinder in en knippert de groene LED 1 x lang • Niet geslaagd: De rode LED knippert 6x  Aanwijzing Als de radioverbinding wordt onderbroken, wordt de fallback-functie uitgevoerd na de derde mislukte lees poging. Zie hoofdstuk 6.1.8 voor meer informatie	 

AUTOMATISERING: Via een automatisering kunt u het in- of uitschakelen van de installatie aan bepaalde voorwaarden koppelen. Hiermee kan bijvoorbeeld volgens een tijdschema worden geschakeld, of bij het aansturen van een draadingang.



Aanwijzing

Volgens EN 50131 mag de uitschakeling alleen door bevoegde personen worden uitgevoerd. Een tijdgestuurde inschakeling mag alleen plaatsvinden als aan de noodzaak-voorwaarde wordt voldaan (bijvoorbeeld: de gebruiker moet het gebouw verlaten en de deur vergrendelen voordat het systeem kan worden ingeschakeld) en als het systeem in een storingsvrije toestand is. Het inschakelen moet in dit geval door middel van een akoestisch signaal en/of een optisch signaal worden aangekondigd.



7.6.2.Alarmen resetten

Het Comfion Pro-systeem kan, afhankelijk van de instellingen, op de volgende manieren worden gereset:

- Als de optie "Automatische reset activeren" is geactiveerd (onder Centrale config. – Veiligheidsinstellingen) reset de centrale het alarm automatisch, wanneer de betreffende melders gesloten zijn en het systeem wordt uitgeschakeld.
- Als de optie "Automatisch resetten" gedeactiveerd is (onder Centrale config. – Veiligheidsinstellingen) wordt na een alarm een melding weergegeven aan de bovenkant van het scherm van de app, die handmatig door de gebruiker moet worden gereset.

Veiligheidsinstellingen	Dashboard	Alarm resetten

7.6.3. Gedwongen ingeschakeld

Met de functie "Dwanginschakeling" kan de centrale worden ingeschakeld ondanks een geactiveerde/open partitie. De betreffende zone wordt dan automatisch verborgen. Het is niet nodig om de melder nogmaals handmatig uit te schakelen.

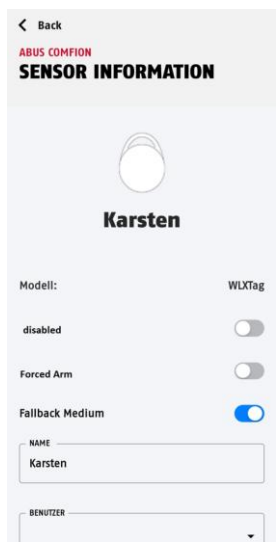
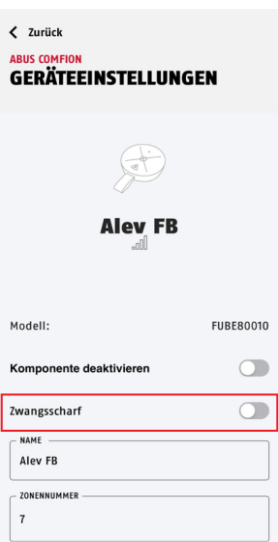
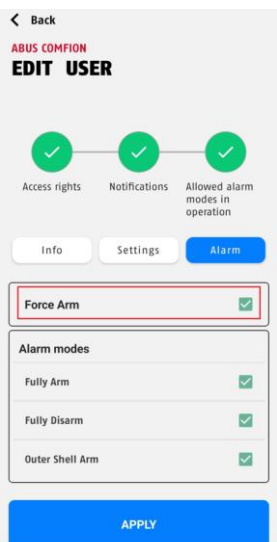
 Opmerking	Houd er rekening mee dat de functie 'Dwanginschakeling' alleen kan worden uitgevoerd als de geactiveerde/open partitie de partitie-instelling ' Overbrugbaar ' heeft.
--	--

Voor het geforceerde inschakelen **via het bedieningspaneel** kan onder de centrale-configuratie onder "pincodes" (zie **hoofdstuk 6.1.4**) de code voor gedwongen inschakeling worden vastgelegd. Deze 3-cijferige code moet achter de 4-cijferige gebruikerscode worden ingevoerd om het systeem via het bedieningspaneel in de gedwongen ingeschakelde toestand te schakelen.

Bovendien kan aan een **transponder** de eigenschap 'gedwongen inschakeling' worden toegewezen om hiermee te schakelen.

Om de beveiliging **via de draadloze afstandsbediening** handmatig in te schakelen, kunt u in de instellingen van de afstandsbediening het vinkje bij "gedwongen inschakelen" aanvinken.

Om het systeem **via de app** handmatig in te schakelen, kunt u bij elke gebruiker op het tabblad "Alarm" het vakje "gedwongen inschakelen" aanvinken.

			
Bedieningspaneel & code voor geforceerde inschakeling	Transponderinstellingen	Afstandsbediening	Gebruikersinstellingen Alarm

7.7. Verklaring van symbolen

Stroomvoorziening	
	Laadstatus van de batterij (of accu) 100% / 75% / 50% / 25% / Batterij leeg
	Links: externe voeding (DC of wisselstroom) aangesloten Rechts: Noodstroomvoorziening (accu) in stand-by
Radiosignaal	
	4 balken = Uitstekend 3 streepjes = zeer goed 2 balken = matig 1 balk = slecht
	Draadloze verbinding verbroken. Dit gebeurt na het uitval van het supervisiesignaal van de betreffende component, d.w.z. na > 1 uur (dit kan per component verschillen)
Gedrag van het apparaat	
	Component geactiveerd (bijv. magneetcontact geopend, trillingsmelder geactiveerd, rookmelder geactiveerd, watermelder geactiveerd)
	Beweging gedetecteerd (PIR-bewegingsmelder / microgolf-bewegingsmelder)
	Apparaat geactiveerd (bijv. sirene aangestuurd, druk op de toets)
	Partitie gesloten (bijv. magneetcontact gesloten)
	Partitie geopend (bijv. magneetcontact geopend) → Wordt weergegeven naast het pictogram 'Component geactiveerd'

Storingen	
	Sabotage gedetecteerd (bijv. behuizing geopend of apparaat van montage-oppervlak verwijderd) Alternatief symbool: 
	Kabelbreuk gedetecteerd (bijv. 3-in-1-melder)
Actiepictogrammen (als u op het pictogram drukt, wordt de beschreven actie uitgevoerd)	
	Apparaatstatus UIT (bijv. draadloos stopcontact uitgeschakeld) → Als u op het pictogram drukt, wordt het apparaat ingeschakeld
	Apparaatstatus AAN (bijv. draadloos stopcontact ingeschakeld) → Als u op het pictogram drukt, wordt het apparaat UITgeschakeld
	PIR-camera 1. Opname maken (door op het pictogram te drukken wordt de handmatige opname gestart) 2. Er wordt een opname gemaakt 3. De opname wordt naar het centrale geheugen verzonden.
WLX-pictogrammen (toegangscontrole)	
	Toegang verleend De weergave geldt voor de tijd waarin de cilinder ingekoppeld is (6/12 sec)
	Permanente toegang is geactiveerd (kantoormodus geactiveerd)  Aanwijzing De permanente toegang is een configuratie in de centrale. Om deze handeling uit te voeren, moet de cilinder eerst worden gewekt (d.w.z. gedraaid) en een draadloze verbinding met de centrale tot stand brengen. Vervolgens wordt toegang verleend.
	Deelgebied ingeschakeld De deelgebieden waaraan de cilinder/wall-reader zijn toegewezen, zijn geactiveerd

7.8. ABUS-cloud

Het draadloze Comfion Pro-beveiligingssysteem maakt bij de eerste inbedrijfstelling verbinding met de ABUS Cloud. De installatie wordt bovendien opgeslagen in het ABUS Cloud-account voor de gespecialiseerde vakmensen van de installateur. Als dit niet gewenst is, kan bij de betreffende gebruiker in de installatie het vinkje bij "Hoofdinstallateur" worden verwijderd of bij een andere installateur worden aangevinkt.

7.9. Opmerkingen over de harde schijf / SSD-geheugenopslag

- De schroeven voor de bevestiging van de harde schijf mogen alleen met de hand worden aangedraaid
- De batterijduur van de centrale wordt beïnvloed door de ingebouwde harde schijf en het stroomverbruik daarvan, alsmede door het aantal aangesloten BUS-deelnemers.
 - De volgens EN 50131 vereiste noodstroomduur voor inbraakalarmcentrales van EN-klasse 2 wordt gegarandeerd door het gebruik van een SSD-gegevensopslag en de aansluiting van maximaal 2 BUM080000 WLX Pro-modules op de Comfion Pro BUS!
- De harde schijf die in de Comfion Pro is ingebouwd, moet zijn geformatteerd in het exFAT- of NTFS-bestandssysteem
- Vervang de harde schijf/SSD-opslag alleen in de toestand waarin de centrale niet onder spanning staat

7.10. Onderhoud en service door installateurs

Test tijdens het routine-onderhoud of het systeem goed werkt:

- Controleer de Comfion Pro op zichtbare tekenen van schade aan de behuizing, de muurbeugel of de frontplaat.
- Controleer of de sabotageschakelaar werkt
- Controleer de toestand van de noodstroomaccu
- Maak de behuizing schoon
 - Gelieve de oppervlakken met een droge, zachte doek schoon te vegen.
 - Gebruik geen water of oplos- of reinigingsmiddelen.
- Controleer de signaalsterkte en de status van de batterij/oplaadbare batterij van alle componenten
- Vervang de batterijen of accu's zoals aanbevolen in de instructies van de fabrikant
- Test elke component.
- Reinig voorzichtig de objectieven van alle PIR-melders en camera's met een schone, droge, zachte doek.
 - Gebruik geen water of oplos- of reinigingsmiddelen.
- Voer een looptest uit van alle melders.
- Test alle signaalgevers
- Test de communicatie.

 Opmerking	ABUS adviseert om de centrale accu na maximaal 3 jaar te vervangen. Bij langdurig gebruik kan een plotselinge vermogensdaling niet worden uitgesloten.
--	--

Hoe vervang ik de accu van de centrale:

- Zet de centrale in de onderhoudsmodus (beveiligingsinstellingen)
- Verwijder de centrale uit de wandbevestiging
- Zet de accuschakelaar op "UIT"
- Open de voorkant door de schroeven aan de achterkant los te draaien en de afdekking los te wrikken (zie **hoofdstuk 3.1** Wandmontage van de centrale voor meer informatie)
- Koppel de voeding en de oude accu los van de centrale
- Wacht 30 seconden
- Sluit de nieuwe accu en de spanningsvoorziening weer aan
- Sluit de klep van het systeem en verlaat de onderhoudsmodus weer

7.11. Tabel met signaalsterktes van het draadloze netwerk

In de onderstaande tabel wordt de betekenis beschreven van de signaalwaarden van de Comfion-draadloze componenten, weergegeven in dBm.

RSSI-waarde (dBm)	Betekenis	Weergave op component
<= -100	Slecht	0 balk
<= -96	OK	1 balk
<= -91	Goed	2 balken
<= -86	Zeer goed	3 balken
> -86	Uitstekend	4 balken

8. Garantie

- ABUS-producten zijn met de grootst mogelijk zorgvuldigheid ontworpen, geproduceerd en op basis van de geldende voorschriften getest.
- De garantie heeft uitsluitend betrekking op gebreken die op materiaal- of fabrieksfouten duiden op het moment van verkoop. Indien er sprake is van een aantoonbare materiaal- of fabricagefout, wordt de module naar goeddunken van de garantieverstrekker gerepareerd of vervangen.
- De garantie eindigt in dit geval met het aflopen van de oorspronkelijke garantieperiode van 2 jaar. Verdergaande aanspraken zijn uitdrukkelijk uitgesloten.
- ABUS is niet aansprakelijk voor gebreken en schade die zijn ontstaan door externe invloeden (bijvoorbeeld door transport, geweld, onjuist gebruik), oneigenlijk gebruik, normale slijtage of het niet opvolgen van deze handleiding en de onderhoudsinstructies.
- Bij het indienen van een garantieclaim dient u bij het product waarover u een klacht indient het originele aankoopbewijs met aankoopdatum en een korte schriftelijke beschrijving van het defect te voegen.
- Als u gebreken aan het product vaststelt, die bij de aankoop reeds aanwezig waren, wendt u zich binnen de eerste twee jaar direct aan uw verkoper.

9. Recyclen



Voer het apparaat af in overeenstemming met de EU-richtlijn 2012/19/EU voor afgedankte elektrische en elektronische apparatuur - WEEE (Waste Electrical and Electronic Equipment). Neem bij vragen contact op met de gemeentelijke instantie die verantwoordelijk is voor de afvalverwerking. Informatie over verzamelpunten voor afgedankte apparatuur krijgt u bij de gemeente, regionale afvalbedrijven of bij uw verkoper.

10. Conformiteit

10.1. EU-conformiteitsverklaring

ABUS Security-Center GmbH & Co. KG verklaart hiermee dat het radiocommunicatiesysteem type FUAA85000 voldoet aan Richtlijn 2014/53/EU en 2011/65/EU. De volledige tekst van de EU-conformiteitsverklaring is beschikbaar op het volgende internetadres: abus.com > Productzoeker > FUAA85000 > Downloads

10.2. Conformiteit aan EN 50131

Het beveiligingssysteem FUAA85000 is bij correcte installatie gecertificeerd volgens veiligheidsgraad 2 en voldoet aan EN 50131-1+A3:2020, EN 50131-3:2009, EN 50131-10:2014, EN 50136-1+A1:2018, EN 50136-2:2013 en EN 50131-5-3:2017.

11. Bijlage

11.1. Contact-ID-codetabel

Code	Codeklasse	Aanvullende gegevens	Type	Beschrijving
111	Brandalarm	Zone	Rook	Een rookmelder heeft een 24-uurs brandalarm geactiveerd
120	Paniekalarm	Zone	Paniek	Op het bedieningspaneel is het paniekalarm geactiveerd
121	Paniekalarm	Gebruiker	Dreigingsalarm	Een gebruiker heeft de bedreigingscode ingevoerd
130	Inbraak-alarm	Zone	Inbraak	Er is een inbraakzone geactiveerd terwijl de installatie ingeschakeld was
131	Inbraak-alarm	Zone	Perimeter	Een perimeterzone activeert een vooralarm
133	Inbraak-alarm	Zone	24-uurszone	Er is een 24-uurs inbraakalarm getriggert

134	Inbraak-alarm	Zone	In-/uitgang	Er is een in-/uitgangszone getriggered terwijl het systeem ingeschakeld was
135	Inbraak-alarm	Zone	Direct bewaakte zone	Er is een direct bewaakte zone geactiveerd terwijl het systeem ingeschakeld was
137	Inbraak-alarm	Zone	Sabotage	Er is een sabotage van de centrale gemeld
139	Inbraak-alarm	Zone	Glasbreuk	Inbraak bevestigd via een zone
154	24 uur technisch alarm	Zone	waterniveau alarm	Watermelder meldt een storing
301	Systeemstoring	Zone	Uitval van de wisselstroomvoeding	Uitval van de netspanning van de centrale of uitbreidingsmodule bij uitgeschakeld systeem
302	Systeemstoring	Zone	Accu-storing	De bufferaccu van de centrale is leeg in uitgeschakelde toestand
305	Systeemstoring	Zone	Reset	Het systeem is gereset en opnieuw opgestart
306	Systeemstoring	Zone	Herstarten	Het systeem is opnieuw opgestart
308	Systeemstoring	Zone	Uitschakelen	Het systeem is uitgeschakeld en werkt niet meer
311	Systeemstoring	Zone	Geen accu / buiten gebruik	De back-up-batterij van de centrale ontbreekt of is volledig leeg
338	Storing in de randapparatuur	Zone	Bedieningspaneel geblokkeerd	Het bedieningspaneel is geblokkeerd omdat er meerdere keren een verkeerde code is ingevoerd
344	Storing in de randapparatuur	Zone	Jamming-herkenning	De draadloze ontvanger heeft een storingssignaal (jamming) gedetecteerd.
350	Communicatiestoring	Zone	Communicatiefout	Het systeem heeft een communicatiefout vastgesteld.
381	Storingsmelding	Zone	supervisie	De aangegeven zone heeft zich tijdens het supervisie-interval niet gemeld.
383	Storingsmelding	Zone	Sabotage	Er is een sabotagemelding afgegeven in de betreffende zone
384	Storingsmelding	Zone	Batterij bijna leeg	Er is een melding van een lage batterij in de betreffende zone
393	Storingsmelding	Zone	Storing Onderhoud	De betreffende zone heeft een storing gemeld
400	Inschakelen/ uitschakelen/ Toegang op afstand	Gebruiker	Ingeschakeld/ Uitgeschakeld	De betreffende gebruiker heeft het systeem via de afstandsbediening in- of uitgeschakeld
401	Inschakelen/ uitschakelen/ Toegang op afstand	Gebruiker	In-/uitschakelen via gebruiker	De betreffende gebruiker heeft het systeem via de smartphone-app in- of uitgeschakeld
406	Inschakelen/ uitschakelen/ Toegang op afstand	Gebruiker	Resetten	De betreffende gebruiker heeft het eerder getriggerde alarm gereset
407	Inschakelen/ uitschakelen/ Toegang op afstand	Gebruiker	In-/uitschakelen via het bedieningspaneel	de betreffende gebruiker heeft het systeem via een draadloos bedieningspaneel in- of uitgeschakeld
443	Inschakelen/ uitschakelen/ Toegang op afstand	Gebruiker	Inschakelen met overbruggen	De betreffende gebruiker heeft het systeem ingeschakeld door storingen te overbruggen
454	Inschakelen/ uitschakelen/ Toegang op afstand	Gebruiker	Het inschakelen is mislukt	Het systeem kon na de uitgangsvertraging niet worden ingeschakeld
461	Inschakelen/ uitschakelen/ Toegang op afstand	Zone	Verkeerde code ingevoerd	Er is een verkeerde code ingevoerd op het bedieningspaneel.
570	Overbruggen	Zone	Zone overbruggen	De betreffende partitie is overbrugd
572	Overbruggen	Zone	24 uur-zone overbruggen	De betreffende 24-uurszone is overbrugd
602	Test	-	Periodieke testmelding	Er is een periodieke testmelding naar de meldkamer verzonden.

ABUS | Security Center GmbH & Co. KG
abus.com

Linker Kreuthweg 5
86444 Affing
Germany

Tel: +49 82 07 959 90-0