Deutsch

Nexello

Installationsanleitung

Wichtige Hinweise und FAQs zu diesem Produkt und weiteren Produkten finden Sie auf der Internetseite
www.abus.com

1.3.0

Deutsch

1. Einführung

Sehr geehrte Kundin, sehr geehrter Kunde,

Wir bedanken uns für den Kauf dieses Produkts.

Bitte beachten Sie, dass sich diese Anleitung an geschultes Fachpersonal richtet. Für eine sachgemäße Installation ist neben dieser Anleitung eine vorausgegangene Schulung notwendig. Wenn Sie eine solche Schulung nicht besucht haben, raten wir vor dem Verbau der Nexello ab.

Für einen einwandfreien und sicheren Betrieb muss dieses Gerät von einem von uns geschulten Fachmann installiert und regelmäßig gewartet werden. Vereinbaren Sie mit Ihrem Errichter regelmäßige Wartungstermine, um durch aktuelle Sicherheitsupdates und neue Funktionen einen dauerhaft reibungslosen Betrieb sicherzustellen.

2. Konformitätserklärung

Hiermit erklärt ABUS Security Center, dass das Nexello Sicherheitssystem der RED-Richtlinie 2014/53/EU entspricht. Das Gerät erfüllt zudem die Anforderungen der folgenden EU-Richtlinien: EMV Richtlinie 2014/30/EU, Nieder-Spannungsrichtlinie 2014/35/EU sowie RoHS Richtlinie 2011/65/EU. Der vollständige Text der EU-Konformitätserklärung ist unter den folgenden Internetadressen verfügbar:

www.abus.com/product/PLSP90000

Die Konformitätserklärung kann auch unter folgender Adresse bezogen werden:

ABUS Security Center GmbH & Co. KG
Linker Kreuthweg 5
86444 Affing
GERMANY

Um diesen Zustand zu erhalten und einen gefahrenlosen Betrieb sicherzustellen, müssen Sie als Anwender diese Bedienungsanleitung beachten!

Lesen Sie sich vor Inbetriebnahme des Produkts die komplette Bedienungsanleitung durch, beachten Sie alle Bedienungs- und Sicherheitshinweise!

Bei Fragen zum Produkt besuchen Sie unsere Supportseite support.abus-sc.com **oder wenden Sie sich an unseren Kundenservice:**

Post: ABUS Support, Linker Kreuthweg 5, 86444 Affing, Deutschland
E-Mail: support@abus-sc.com
Tel: +49 8207 959 90 300
Öffnungszeiten Hotline: Mo-Do: 08 - 17 Uhr; Fr: 08 – 14 Uhr

Symbolerklärung

	**Das Symbol mit dem Blitz im Dreieck wird verwendet, wenn Gefahr für die Gesundheit besteht, z.B. durch elektrischen Schlag.**
	**Ein im Dreieck befindliches Ausrufezeichen weist auf wichtige Hinweise in dieser Bedienungsanleitung hin, die unbedingt zu beachten sind.**
	**Dieses Symbol ist zu finden, wenn Ihnen besondere Tipps und Hinweise zur Bedienung gegeben werden sollen.**

Aufzählungen

1. ... 2. ...	**Aufzählungen mit festgelegter Reihenfolge im Text bzw. Warnhinweis.**
• ... • ...	**Aufzählungen ohne festgelegte Reihenfolge im Text bzw. Warnhinweis.**

Bestimmungsgemäße Verwendung

Verwenden Sie das Gerät ausschließlich für den Zweck für den es gebaut und konzipiert wurde! Jede andere Verwendung gilt als nicht bestimmungsgemäß! Bei Schäden, die durch Nichtbeachten dieser Sicherheitshinweise verursacht werden, erlischt der Garantieanspruch. Für Folgeschäden übernehmen wir keine Haftung!

3. Haftungsbeschränkung

Es wurde alles Erdenkliche unternommen, um sicherzustellen, dass der Inhalt dieser Anleitung korrekt ist. Jedoch kann weder der Verfasser noch ABUS Security Center GmbH & Co. KG die Haftung für einen Verlust oder Schaden übernehmen, der durch falsche Installation und Bedienung, bestimmungswidrigen Gebrauch oder durch Nichtbeachtung der Sicherheitshinweise und Warnungen verursacht wurde. Für Folgeschäden wird keine Haftung übernommen. Das gesamte Produkt darf nicht geändert oder umgebaut werden. Sollten Sie sich nicht an diese Hinweise halten, erlischt Ihr Garantieanspruch. Alle im Text enthaltenen externen Links begründen keine inhaltliche Verantwortung der ABUS Security Center GmbH & Co. KG, sondern sind allein von dem jeweiligen Dienstanbieter zu verantworten. ABUS Security Center GmbH & Co. KG hat die verlinkten externen Seiten zum Zeitpunkt der Veröffentlichung sorgfältig überprüft, mögliche Rechtsverstöße waren zum Zeitpunkt der Verlinkung nicht erkennbar. Auf spätere Veränderungen besteht keinerlei Einfluss. Eine Haftung der ABUS Security Center GmbH & Co. KG ist daher ausgeschlossen. Technische Änderungen vorbehalten.

Hinweis zum Datenschutz

Der Betreiber ist gemäß DSGVO als verantwortliche Stelle für den rechtskonformen Einsatz des Produkts verantwortlich.

4. 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 die Zentrale 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 entstanden sind.
	Bei Geltendmachung eines Gewährleistungsanspruches ist dem zu beanstandenden Produkt der originale Kaufbeleg mit Kaufdatum und eine kurze schriftliche Fehlerbeschreibung beizufügen.
	Sollten Sie an der Zentrale einen Mangel feststellen, der beim Verkauf bereits vorhanden war, wenden Sie sich innerhalb der ersten zwei Jahre bitte direkt an Ihren Verkäufer.

5. Open-Source Lizenzhinweise

Das Produkt enthält Softwarebestandteile, die von den Rechteinhabern als freie Software bzw. Open Source Software lizenziert werden (nachfolgend als „OSS“ bezeichnet). Die entsprechenden Lizenzen sind in gedruckter Ausgabe dem Produkt beiliegend und/oder über eine grafische Benutzeroberfläche abrufbar. Sie können Nutzungsrechte in dem dort geregelten Umfang unmittelbar von den Rechteinhabern erwerben.

Open Source Lizenzhinweise abrufbar unter: https://<YourDeviceIP>/OSS-License

Die Open Source-Lizenzen haben Vorrang vor allen anderen Lizenzbedingungen und vertraglichen Vereinbarungen mit ABUS in Bezug auf die entsprechenden im Produkt enthaltenen OSS-Softwarekomponenten.

Generell können Lizenzinformationen zu ABUS Produkten auf www.abus.com im Downloadbereich der Produktbeschreibung abgerufen werden.

Deutsch

Inhalt

6. Sicherheitshinweise

Vor der ersten Verwendung des Gerätes lesen Sie bitte die folgenden Anweisungen genau durch und beachten Sie alle Warnhinweise, selbst wenn Ihnen der Umgang mit elektronischen Geräten vertraut ist. Die vollständigen Sicherheitshinweise für die Nexello finden Sie zum Download unter www.abus.com/product/PLSP90000

6.1. Auspacken

Während Sie das Gerät auspacken, handhaben sie dieses mit äußerster Sorgfalt. Verpackungen und Packhilfsmittel sind recyclingfähig und sollen grundsätzlich der Wiederverwertung zugeführt werden. **Bei einer eventuellen Beschädigung der Originalverpackung, prüfen Sie zunächst das Gerät. Falls das Gerät Beschädigungen aufweist, senden Sie dieses mit Verpackung zurück und informieren Sie den Lieferdienst.**

6.2. Grundsätze

- Benutzernamen und Passwörter für die Anmeldung an Sicherheits-Systemen dürfen nur den rechtmäßigen Besitzern bekannt sein und niemals an Unberechtigte weitergegeben werden.
- Sollten Benutzername und Passwort schriftlich weitergegeben werden müssen, dürfen diese nicht in einer einzigen Mail übermittelt werden.
- Benutzernamen und Passwort sollten regelmäßig geändert werden.
- Benutzernamen sollten insbesondere nicht den eigenen Namen, den Namen von Familienmitgliedern, des Haustieres, des besten Freundes, des Lieblingsstars, des Hobbies oder Geburtsdaten enthalten.
- Vermeiden Sie Benutzernamen und Passwörter, die Sie auf anderen Websites verwenden oder die leicht von anderen erraten werden können.
- Der Benutzername sowie das Passwort sollte nicht in Wörterbüchern vorkommen und auch keine Produktbezeichnung sein.
- Er sollte nicht aus gängigen Varianten und Wiederholungs- oder Tastaturmustern bestehen, wie z.B. asdfgh oder 1234abcd usw.
- Benutzernamen und Passwörter sollten spätestens nach 180 Tagen geändert werden.
- Neue Benutzernamen und Passwörter sollten nicht identisch sein mit einem der drei Letzten.
- Neue Benutzernamen und Passwörter sollten sich in mindestens zwei Zeichen vom bisherigen Benutzernamen und Passwort unterscheiden.
- Makros und Scripte sollten nicht zur Eingabe von Benutzernamen und Passwörtern benutzt werden.

6.3. Stromversorgung

- Um Feuergefahr und die Gefahr eines elektrischen Schlages zu vermeiden, setzen Sie die Zentrale sowie die Komponenten weder Regen noch sonstiger Feuchtigkeit aus.
- Nehmen Sie das Gerät nicht in der Nähe von Badewannen, Swimmingpools oder spritzendem Wasser in Betrieb.
- Es ist verboten Umbauten am Gerät vorzunehmen.
- Beschädigte Geräte bzw. beschädigte Zubehörteile dürfen nicht mehr verwendet werden
- Eine andere Verwendung als die zuvor beschriebene kann zur Beschädigung dieses Produkts führen. Darüber hinaus ist dies mit Gefahren, wie z.B. Kurzschluss, Brand, elektrischer Schlag, etc. verbunden.
- Wenn Sie das Gerät von einer kalten in eine warme Umgebung bringen, kann sich im Inneren des Geräts Feuchtigkeit niederschlagen. Warten Sie in diesem Fall etwa eine Stunde, bevor Sie es Betrieb nehmen.
- Trennen Sie das Gerät von der Netzstromversorgung, bevor Sie Wartungs- oder Installationsarbeiten durchführen.

Gefahr
Einbauten oder Modifikationen des Gerätes führen zum Garantieverlust.

7. Montage

Hinweise zur Montage finden Sie in dem unter www.abus.com/product/PLSP90000 zum Download bereitgestellten Quickguide des Nexello Sicherheitssystems.

8. Vorbereitungen im ABUS Nexello Pilot

Um die Einrichtung Ihrer **Nexello** zu starten, ist es notwendig, einen Account auf dem zugehörigen **Fernwartungsportal** zu erstellen. Hierüber können Sie später diese und weitere Anlagen verwalten.

Besuchen Sie hierzu die Website https://nexello-pilot.abus.com

Sie sehen nun die Anmeldemaske des Nexello Pilots. Klicken Sie auf **jetzt registrieren** und führen den Registrierungsprozess durch. Nach der Prüfung und Freigabe Ihrer Daten durch den Abus-Vertrieb erhalten Sie eine Bestätigung mit dem Link für den Login. **Beachten Sie, dass zur Freischaltung des Pilot-Accounts eine erfolgreich abgeschlossene Abschlussprüfung der Grundlagenschulung notwendig ist.**

Laden Sie die App **Nexello Sicherheitssystem** aus dem **Apple-Store** (iOS) oder den **Google Playstore** (Android) herunter und öffnen Sie die App.

Nachdem Sie die AGB's und Datenschutzbestimmung gelesen und akzeptiert haben, müssen Sie Ihr Endgerät mit Ihrem Portal-Account verknüpfen. Klicken Sie in der App auf **App verifizieren**, wählen Sie im Portal den Punkt **App verifizieren** unter **Accountinfo** und scannen den angezeigten QR-Code. **(Achten Sie darauf, dass sowohl die App, als auch das Portal die Verifizierung bestätigen)**

9. Smart Pairing (WLAN)

Unter der **Smart Pairing** Funktion versteht man die initiale Verbindung der Nexello über Bluetooth und der folgenden Einrichtung einer WLAN-Verbindung mit Ihrem Netzwerk.

Hinweis
Wir empfehlen, die Nexello physisch per LAN zu betreiben

Sollten Sie keine Möglichkeit haben, Ihre Nexello per LAN-Kabel mit Ihren Netzwerk zu verbinden, können Sie dies auch per WLAN tun. Starten Sie hierfür Ihre Zentrale ohne angestecktes Ethernet-Kabel. Starten Sie die Ersteinrichtung in Ihrer Nexello-App und achten darauf, dass das Bluetooth an Ihrem Gerät aktiviert ist.

In der Serversuche sollte Ihnen nun die Nexello angezeigt werden – wählen Sie diese aus und hinterlegen in den folgenden **WLAN-Einstellungen** die **SSID** und das **Passwort** Ihres Netzwerks. Die Nexello versucht, nach dem Speichern dieser Einstellungen, sich mit Ihrem WLAN-Netz zu verbinden. Sie bekommen bei erfolgreicher Verbindung einen Hinweis. Warten Sie mit dem ersten Einloggversuch, bis die Nexello alle Updates und Lizenzsynchronisationen abgeschlossen hat. Die LED Ihrer Anlage leuchtet grün, wenn alle Vorgänge abgeschlossen sind.

Hinweis: *Sollte Ihre Zentrale bereits in Betrieb genommen sein, können Sie durch* ***2-sekündiges Drücken des Reset-Tasters*** *den Smart Pairing Modus aktivieren. Die Anlage signalisiert das das aktivierte Bluetooth mit einer blinkenden blauen LED.*

10. Ersteinrichtung

Anschließend können Sie die **Ersteinrichtung** starten. Die App sollte nach einem kurzen Suchvorgang Ihre Zentrale im Netzwerk ausfindig machen. Wählen Sie die Anlage aus und verifizieren sich mit ihrem persönlichen Installateur-QR-Code auf Ihrer **Mitarbeiterkarte**. Diesen finden Sie in Ihrem Portalzugang unter **Accountinfo – Profil – Mitarbeiterkarte**.

Alternativ können Sie die Anlage am Webbrowsers Ihres Computers konfigurieren. Rufen Sie hierzu die IP-Adresse der Nexello auf. Diese finden Sie in Ihrem Heimrouter oder in der Nexello App.

Hinweis: *Wir empfehlen derzeit ausschließlich den Webbrowser ‚****Edge****‘ beim Zugriff auf das Nexello Portal, sowie auf die Nexello selbst zu nutzen.*

Sie haben die Möglichkeit über den Punkt **Karte sichern** die Mitarbeiterkarte in der App fest zu hinterlegen und mit einem Passwort, bzw. Ihrer biometrischen Anmeldung (Fingerprint/ Gesichtserkennung) abzusichern.

10.1. Backup

Zu aller Erst haben Sie die Möglichkeit, ein zuvor erstelltes **Backup** in die Zentrale einzuspielen. Stecken Sie hierfür den mit dem **Backup** bespielten USB-Stick und klicken auf **Backup wiederherstellen**. Wenn die Wiederherstellungsdatei auf dem Stick gefunden werden kann, wird Ihnen diese aufgelistet. Nach der Passworteingabe für diese Datei wird das Backup eingespielt. Warten Sie bis die Anlage neu gebootet ist. Danach ist ein Zugriff mit den bestehenden Nutzern möglich.

10.2. Art des Zuhauses

Sie können nun wählen, wie viele **Bereiche** Sie in Ihrem Objekt benötigen. Sie können mit einem Teilbereich arbeiten, mit zwei Teilbereichen, oder, wenn Sie beispielsweise zwei Wohnungen mit einem gemeinsamen Eingangsbereich haben, die dritte Auswahlmöglichkeit „2 Teilbereiche + gemeinsamer Bereich“ wählen.

Legen Sie die/den Namen für die/den Bereich/e fest und bestätigen diese.

***Hinweis**: Die Sortierung der Bereiche im Dashboard erfolgt anschließend alphabetisch*

10.3. Raumauswahl

In der **Raumauswahl** können Sie die Räume für Ihr Objekt den jeweiligen Bereichen hinzuzufügen

Es werden, je nach vorheriger Auswahl des Systems, die Räume

1. für den gemeinsamen Bereich
2. für den Bereich 1
3. für den Bereich 2

gewählt.

Im Folgenden Schritt werden Komponenten in diese Räume eingelernt.

10.4. Komponenten hinzufügen

Sie haben nun die Möglichkeit, **Komponenten** (Z-Wave, Kameras, Zylinder) durch Klicken auf das Plus-Symbol **hinzuzufügen**. Wie genau dies funktioniert, entnehmen Sie bitte dem Absatz *Komponenten hinzufügen (Inklusion)*.

Durch Klicken auf die Fläche rechts vom **Plus-Symbol** können Sie die **Geräteliste** öffnen, in welcher Sie die hinzugefügten Komponenten auf den Raum beschränkt angezeigt bekommen. Hier haben Sie auch die Möglichkeit, eingelernte Komponenten wieder zu entfernen.

Hinweis

Nach dem Versetzen einer netzgebundenen Komponente muss die Funktion „Mesh-Netzwerk neu routen“ in der Z-Wave Erweiterung gestartet werden um das Routing des Z-Wave Netzwerks neu zu starten.

10.5. Alarmkonfiguration

Im nächsten Schritt finden Sie Einstellungen zu den **Beteiligten Meldern**, dem **Ein/Ausgangsweg** und den **Benachrichtigungen**.

10.5.1. Beteiligte Melder

Unter dem Punkt **Beteiligte Melder** finden Sie als erste Auswahlmöglichkeit die **Alarmmelder**.
Genauer beschrieben wird dieser Punkt unter 4.2.1 Beteiligte Melder.

Alarmmelder

Hier können Sie Melder in bzw. aus der Überwachung nehmen, sowie die Zuordnung „**Innenbereich / Gebäudehülle / Außenbereich**“ vornehmen.

Signalgeber

Unter dem Punkt **Signalgeber** werden Ihnen eingelernte Innen- und Außensirenen aufgelistet. Sie haben hier die Möglichkeit, diese in die Alarmkette zu integrieren.

Kamera-Überwachung

Der Punkt **Kamera-Überwachung** listet Ihnen alle hinzugefügten Kameras auf. Sie können diese zur Überwachung hinzufügen (Default) oder die Überwachung deaktivieren, um die Kameras unabhängig von der Alarmkette zu nutzen.

10.5.2. Ein/Ausgangsweg

Die Konfiguration des **Ein-/Ausgangswegs** setzt sich auch den **Ein/Ausgangsgeräten** und der **Ein/Ausgangsverzögerung** zusammen.

Bei den **Ein/Ausgangsgeräten** wählen Sie alle Melder aus, welche sie beim Betreten des Hauses auslösen würden. Diese Melder lösen dann keinen sofortigen Einbruchalarm, sondern eine eingestellte **Ausgangsverzögerung** aus.

Diese **Ausgangsverzögerung** können Sie, genau wie die **Eingangsverzögerung** im nächsten Punkt einstellen. Hier findet sich zusätzlich noch die Funktion **Letzte Tür**. Komponenten, welche hier angehakt werden, beenden die **Ausgangszeit** in dem Moment, wenn Sie geschlossen werden.

Eine genaue Erklärung der Funktion finden Sie unter **13.2.2. Ein-/Ausgangsweg**

10.5.3. Benachrichtigungen

Hier können für die einzelnen Ereignisse die externen Reaktionen eingestellt werden. Bitte beachten Sie, dass diese Einstellung in der Ersteinrichtung nur für den Installateur gilt. Die **Benachrichtigungen** können später pro Benutzer vom **Besitzer** definiert werden. Siehe ***4.2.3. Benachrichtigungen***

11. Offline-Case

Sie haben die Möglichkeit, die Anlage auch ohne eine vorhandene Verbindung zum Internet zu betreiben. Die Erstinbetriebnahme muss jedoch immer mit einer bestehenden Internetverbindung durchgeführt werden, sodass sich die Zentrale mit dem **Nexello-Portal** verbinden kann, um sich die nötigen Lizenzen und Updates herunterladen zu können.

Bitte beachten Sie auch, dass für den Offline-Case zwingend ein Besitzer angelegt sein muss.

Bei der Erstinstallation setzen Sie als Installateur ein Passwort, welches Sie, wenn der in der Anlage hinterlegte QR-Code nicht bekannt ist, im **Offline-Case** benötigen, um sich bei der Anlage anzumelden. Sie können dies unter **Einstellungen – Benutzer** tun.

Da ohne vorhandene Verbindung zum Internet keine **Push-Benachrichtigungen** verschickt werden können, muss für eine Anmeldung des Installers ein Administrator angemeldet sein, um den Zugriff frei zu geben.

Hinweis

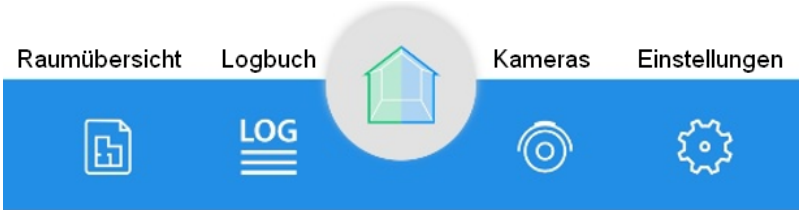
Die Einloggdaten für den Installateur-Login sind Ihre 4-stellige Installer-Kennung (Nexello-Portal) und ihr selbst vergebenes Passwort.

12. Dashboard

Das **Dashboard** dient Ihnen als Übersichtsseite und zeigt Ihnen die wichtigsten Informationen auf einen Blick.

Sie sehen hier, ob Störungen anliegen, welchen Zustand die Zentrale hat (aktiv / deaktiv / intern aktiv) und können sich Hotkeys und Shortcuts anzeigen lassen. Außerdem haben Sie natürlich die Möglichkeit, die Zentrale zu aktivieren, intern scharf zu schalten und auch wieder zu deaktivieren.

In der Navigationsleiste, welche sich im unteren Bildrand des Dashboards befindet, können Sie folgende Punkte aufrufen:



13. Alarmkonfiguration

In der Alarmkonfiguration finden Sie, wie es der Name schon verrät, die wichtigsten Programmierpunkte zur Alarmkette der Zentrale.

Unter dieser findet sich einmal die Konfiguration des **Systems** und die Einstellungen pro **Bereich**.

13.1. System

Neben dem **Wartungsmodus**, dem **Gehtest** und den **reversiblen Zuständen** finden sich noch einige Einzeleinstellungen unter dem System.

Mit der **Signalisierung** können Sie einstellen, welche Bauteile der Zentrale Sie zur akustischen und visuellen Anzeige nutzen möchten.

LED: Aktivieren/Deaktivieren der LED auf der Platine

Sound: Aktivieren/Deaktivieren des Lautsprechers auf der Platine

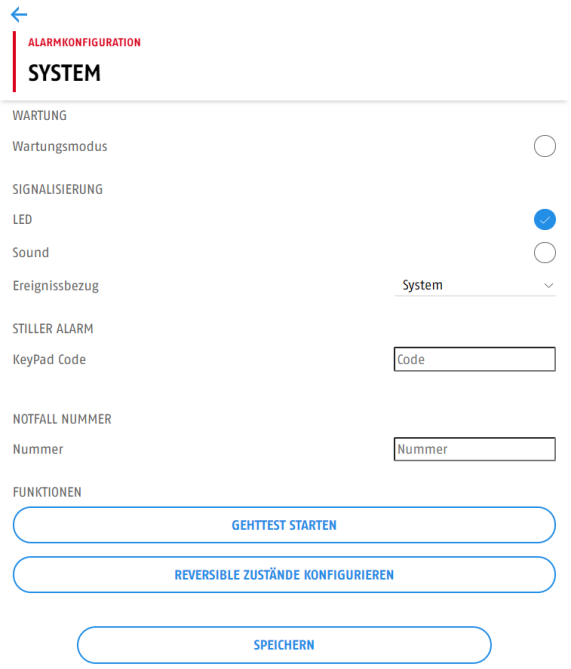
Ereignisbezug: Definieren Sie, wo Ihre Zentrale verbaut ist. Je nach Wahl reagieren die LED sowie der Sounder der Anlage.

System = Gemeinsamer Bereichn

Alarmbereich 1 = Bereich 1

Alarmbereich 2 = Bereich 2

Hardware = Keine LED/Sounder



Unter dem **KeyPad Code** im Reiter **Stiller Alarm** können Sie Ihren **Bedrohungscode** festlegen. Dieser Code hat normale Benutzerrechte – die Anlage kann hiermit also aktiviert und deaktiviert werden. Bei Nutzung dieses Codes wird ein stiller Alarm ausgelöst. Benutzen Sie diesen Code, wenn Sie bedroht werden.

Unter der **Notfallnummer** können Sie eine Rufnummer hinterlegen, welche im Alarmfenster angezeigt wird und durch einfaches Drücken direkt angerufen werden kann.

13.1.1. Wartungsmodus

Ein wichtiger Punkt in der Nexello ist der **Wartungsmodus**. Aktivieren Sie diesen, um die Sabotage und sonstige Alarmauslösungen der Zentrale vorübergehen zu ignorieren. Wir empfehlen dies bei der kompletten Installation, sowie bei jeder Wartung und jedem Batteriewechsel zu machen.

Vergessen Sie nicht, den **Wartungsmodus** wieder zu deaktivieren, wenn dieser nicht mehr gebraucht wird. Es ist sonst nicht möglich die Zentrale scharf zu schalten.

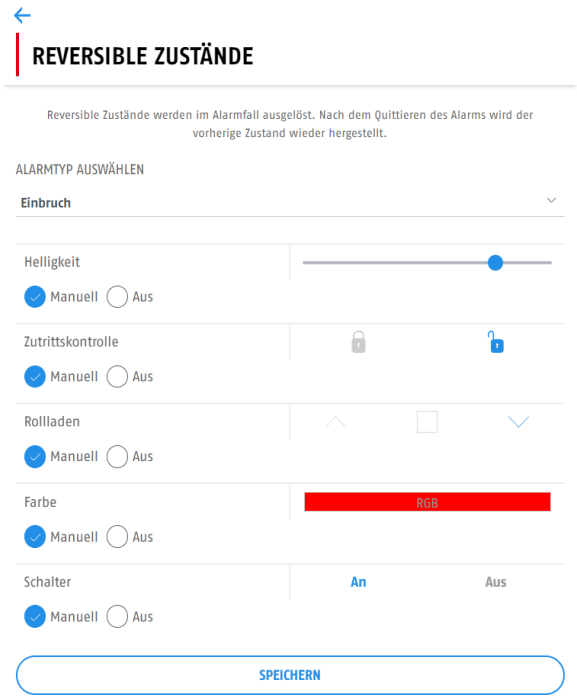
13.1.2. Gehtest

Der **Gehtest** dient zum Testen der Grundfunktionen Ihrer Z-Wave Komponenten. Wenn Sie diesen starten, können Sie den Alarmkontakt sowie den Sabotagekontakt des Melders überprüfen. Auch kann er zur Identifizierung einer Komponente genutzt werden.

Achtung! Zum Starten des **Gehtests** muss zwingend der **Wartungsmodus** aktiviert sein!

13.1.3. Reversible Zustände

Reversible Zustände werden im Alarmfall ausgelöst. Sie können hier definieren, was in der verschiedenen Alarmfällen (Einbruch, Feuer, etc.) geschehen soll. (Erklärung 20.3. FAQ Punkt 5)



Sie können unter den reversiblen Zuständen als erstes den Alarmtyp wählen, welchen Sie definieren möchten. Hier haben Sie die Auswahl zwischen **Einbruch, Überflutung, Gas, Panik, Sabotage, Rauch, Medizin und Bedrohung**.

Pro Alarmtyp können Sie die gewünschten Reaktionen auswählen. Befindet sich eine passende Komponente in Ihrem System und wurde unter **Alarmkonfiguration – Reversible Geräte** ausgewählt, führt diese die ausgewählte Einstellung aus.

Helligkeit: *verändert den DPI-Wert bei eingebundenen Lampen*
Zutrittskontrolle: *Einkoppeln/ Entkoppeln der Funkzylinder*
Rollladen: *Herauf-/Herunterfahren von Rollläden*
Farbe: *verändert RGB-Wert bei eingebundenen Lampen*
Schalter: *Ein/Ausschalten von eingebundenen Schaltern*

13.2. Bereich

Die folgenden Einstellungen werden pro **Bereich** vorgenommen. Beachten Sie, dass sich diese nur auf die Komponenten beziehen, welche sich in dem jeweiligen **Bereich** befinden.

13.2.1. Beteiligte Melder

Der Punkt **Beteiligte Melder** untergliedert sich in die **Alarmmelder**, die **Signalgeber** und **die Kamera-Überwachung**.

Unter den **Alarmmeldern** können Sie für die sich in dem Bereich befindenden Melder verschiedene Einstellungen treffen. Vor allem haben Sie die Möglichkeit, die Melder in die bzw. aus der Alarmkette zu nehmen. Sie können außerdem den Sabotagemelder der Komponenten einzeln deaktivieren.

Hinweis
Wir empfehlen keine dauerhafte Deaktivierung des Sabotagekontakts.

Als weitere Einstellung können Sie die Zuordnung ***Innenbereich / Gebäudehülle / Außenbereich*** vornehmen.

*Melder, welche sich im **Innenbereich** befinden, werden bei einer internen Scharfschaltung nicht mit überwacht. Zum **Innenbereich** gehören alle Melder, welche sich im Gebäude, jedoch nicht an der Außenwand befinden (meist Bewegungsmelder).*

*Melder, welche sich in der **Gebäudehülle** befinden, werden immer überwacht. Sowohl bei der internen, als auch bei der externen Scharfschaltung. Diese Melder sind in der Regel an der Außenwand montiert.*

*Melder, welche sich im **Außenbereich** befinden, lösen keinen Einbruchalarm aus. Es wird sowohl bei der internen, als auch bei der externen Aktivierung eine **Perimeterwarnung** ausgelöst (Störung, Benachrichtigung, Logbucheintrag). Der **Außenbereich** deklariert alle Melder, welche außerhalb des Gebäudes z.B. den Garten überwachen*

Wenn Sie die **Bypass-Einstellung** eines Alarmmelders bei der Aktivierung auf immer gestellt haben, haben Sie außerdem ein zusätzliches Feld unter dem jeweiligen Melder, welches Ihnen erlaubt, dieses wieder aus dem Bypass zu entfernen und damit wieder in die Überwachung aufzunehmen.

Unter dem Punkt **Signalgeber** werden Ihnen eingelernte Innen- und Außensirenen aufgelistet. Sie haben hier die Möglichkeit, diese in die Alarmkette zu integrieren und zu konfigurieren, bei welchen Ereignissen die jeweilige Sirene alarmieren soll.

Der Punkt **Kamera-Überwachung** listet Ihnen alle hinzugefügten Kameras auf. Sie können diese zur Überwachung hinzufügen (Default) oder die Überwachung deaktivieren, um die Kameras unabhängig von der Alarmkette zu nutzen.

13.2.2. Ein-/Ausgangsweg

Unter dem **Ein-/Ausgangsweg** können Sie einmal die **Ein-/Ausgangsgeräte** definieren, sowie die **Ein-/Ausgangsverzögerung** nach ihrem Belieben einstellen.

Wählen Sie als erstes unter den **Ein-/Ausgangsgeräten** die Melder aus, welche sich auf Ihrem Eingangsweg liegen. Ausgewählte Melder lösen beim Eintreten keinen sofortigen Einbruchalarm aus, sondern die eingestellte **Eingangsverzögerung**.

Diese **Eingangsverzögerung** stellen Sie, genau wie die **Ausgangsverzögerung** im schon angesprochenen Punkt **Ein-/Ausgangsverzögerung** ein. Sie haben hier einen Spielraum von 10 – 180 Sekunden.

Außerdem können Sie einzelnen Meldern die Eigenschaft **Letzte Tür** geben, wodurch die Melder bei einer laufenden Ausgangsverzögerung diese beim Schließen des Melders sofort unterbrechen und die Anlage scharf schalten.

Verhalten der Verzögerungszeiten in den verschiedenen Systemen (1TB/2TB/2+gem.TB):

Eingangsverzögerung:

Wenn Sie einen gemeinsamen Bereich haben, nutzt die Nexello, wenn die Eingangsverzögerung durch einen Melder aus diesem gemeinsamen Bereich ausgelöst wurde, immer die längste eingestellte Eingangszeit.

Beispiel:

Eingangsverzögerung TB1: 10 Sek

Eingangsverzögerung TB2: 20 Sek

-> Eingangsverzögerung, bei betreten gem. Bereich: 20 Sek

Ausgangsverzögerung:

Wenn Sie einen gemeinsamen Bereich haben, nutzt die Nexello **bei gleichzeitiger Aktivierung** beider Bereiche die längst eingestellte Ausgangsverzögerung.

Beispiel:

Ausgangsverzögerung TB1: 30 Sek

Ausgangsverzögerung TB2: 20 Sek

-> Aktivierung der Bereiche nach 30 Sek

13.2.3. Benachrichtigungen

In den Benachrichtigungen können Sie Einstellungen zur Kommunikation vornehmen.

Für jeden Benutzer können differenziert pro **Alarm** folgende Reaktionen gewählt werden:

E-Mail, Push-Nachricht

Für jeden Benutzer können differenziert pro **Status-Änderung** folgende Reaktionen gewählt werden:

E-Mail, Push-Nachricht

Für jeden Benutzer können differenziert pro **Warnung** folgende Reaktionen gewählt werden:

E-Mail, Push-Nachricht

13.2.4. Reversible Geräte

Wie bereits unter 13.1.3 Reversible Zustände beschrieben, haben Sie hier die Möglichkeit, alle Komponenten (Aktoren) auszuwählen, die als **reversible Geräte** genutzt werden sollen.

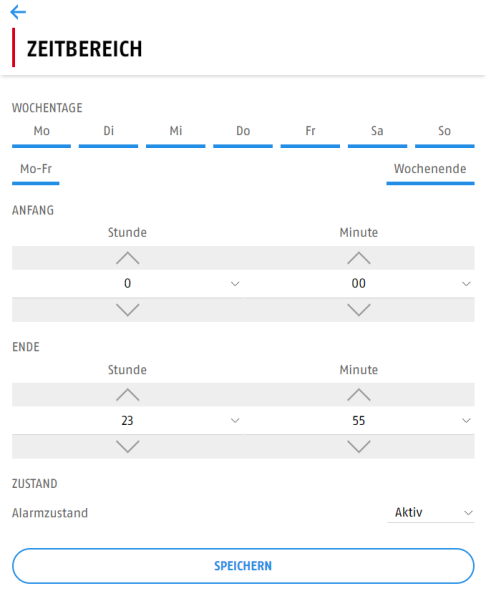
Alle angehakten Aktoren werden, wie in den **reversiblen Zuständen** definiert, bei den jeweiligen Alarmen reagieren.

13.2.5. Zeitplan

Im **Zeitplan** können Sie eine zeitliche automatische Aktivierung, interne Aktivierung und Deaktivierung konfigurieren.

Über das Bearbeitungs-Symbol rechts oben und anschließendem Drücken des Plus-Symbols können Sie einen **Zeitplan** hinzufügen.

Indem sich öffnenden Dialog kann dieser nun definiert werden. Sie können die Tage, den Anfang des Zustands und Ende des Zustands einstellen. Außerdem muss im untersten Punkt den gewünschten Alarmzustand gewählt werden.



13.2.6. Bypass-Einstellungen

Unter den **Bypass-Einstellungen** können Sie definieren, wie die Anlage bei einer versuchten Aktivierung reagieren soll, wenn ein Melder in diesem Moment geöffnet (ausgelöst) ist.

Sie haben folgende Einstellungsmöglichkeiten:

Nie: Die Möglichkeit, Melder auszublenden, ist nicht gegeben.

Nachfragen: Bei einem offenen Melder wird das Störungsmenü aufpoppen, worüber man den Melder manuell ausblenden kann.

Automatisch: Offene Melder werden automatisch ausgeblendet, sollten diese bei einem Aktivierungsversuch offen sein.

14. Benutzerverwaltung

In der **Benutzerverwaltung** können Sie neue Nutzer anlegen, bestehende bearbeiten oder dieser löschen.

*Bitte beachten Sie, dass die **Benutzerverwaltung** eine Funktion des Anlagenbesitzers ist. Nur dieser hat den vollständigen Zugriff auf diesen Konfigurationspunkt. Wir empfehlen, die folgenden Einstellungen nach der Übergabe, das heißt mit angelegtem **Besitzer-Account** durchzuführen.*

Die Benutzerverwaltung wird untergliedert in die Reiter **Benutzer** und **Gruppen**.

Im Reiter **Benutzer** können Sie als Administrator der Nexello neue **Benutzer** hinzufügen (5.2), sowie bestehende verwalten und bearbeiten (5.3).

Im Reiter **Gruppen** können Sie bestehende **Benutzer** den verschiedenen **Gruppen** hinzufügen und die Berechtigungen dieser **Gruppen** bearbeiten. Wählen Sie hierzu eine bestehende **Gruppe** aus.

Von Besitzer (Admin) zu bearbeitende Gruppen:

- **Administrator**
- **Bereich 1**
- **Bereich 2**

Vom Installateur zu bearbeitende Gruppe:

- **Installer**

Zusätzliche Benutzereinschränkungen:

- **Wachmann:**
  Wird einem Benutzer die Rolle des Wachmanns zugeteilt, so hat dieser die Möglichkeit, im Alarmfall den Alarmbereich zu betreten, den Alarm zu quittieren und anschließend wieder zu aktivieren. Er darf die Anlage ausschließlich im Alarmfall bedienen.

14.1. Übergabe an Besitzer

Um den schon beschriebenen **Besitzer-Account** anzulegen, muss der der Anlage beiliegende QR-Code im Anmeldefenster gescannt werden. Es öffnet sich ein Dialog zum Anlegen des Nutzers.

Nach der Übergabe an den Besitzer muss dieser jeden Zugriff des Errichters auf die Zentrale freigeben. Diese Freigabe kann auch zeitlich für 1,2,3 oder 8 Stunden erteilt werden.

Wir empfehlen, die Übergabe an den Besitzer erst durchzuführen, wenn alle Installer-Funktionen konfiguriert wurden.

14.2. Benutzer hinzufügen/entfernen

Um einen **Benutzer** hinzuzufügen, betreten Sie als Nutzer mit Administrationsrechten die **Benutzerverwaltung**.

*Als Installateur haben Sie **keine** Rechte zum Hinzufügen, Löschen sowie Bearbeiten der Benutzer.*

Wenn Sie den Button **Neuen Nutzer erstellen** drücken, öffnet sich der Dialog zum Erstellen eines neuen **Benutzers**. Achten Sie darauf, dass Sie über das Zahnradsymbol rechts oben in die **Zutrittskontrolle** wechseln können, um Tags einzulernen, bzw. auf **Erweitert**, um Einstellungen wie E-Mail, Key-Pad-Code etc. vorzunehmen

14.3. Benutzer bearbeiten

Sie können einen bestehenden **Benutzer** natürlich auch **bearbeiten.** Klicken Sie hierfür als Nutzer mit Administrationsrechten auf den zu bearbeitenden Nutzer.

*Als Installateur haben Sie **keine** Rechte zum Hinzufügen, Löschen sowie Bearbeiten der Benutzer.*

Bei einem Installateur haben Sie lediglich die Möglichkeit diesen zu deaktivieren/aktivieren oder zu löschen.

Wenn Sie einen normalen **Benutzer** oder **Administrator** aufrufen, können Sie in der ersten Übersicht den Vor- und Nachnamen des Nutzers abändern, ein neues Passwort vergeben, sowie die **Benutzergruppen** festlegen.

Über das Einstellungssymbol rechts-oben können die Punkte **Zutrittskontrolle** und **Erweitert** aufgerufen werden.

Unter **Zutrittskontrolle** können Sie **Schließmedien** (Mifare-Proximity-Schlüssel) hinzuzufügen.

Wenn Sie den Punkt **Erweitert** aufrufen, können Sie unter dem Punkt **Keypad** den Benutzercode festlegen, mit welchem Sie über das Funk-Bedienteil die Anlage scharf und unscharf schalten können. Des Weiteren können Sie neben dem **Geschlecht** und Ihrem **Geburtsdatum** die **E-Mail-Adresse** und die **Rufnummer** des Nutzers festlegen, um Benachrichtigungen von der Anlage empfangen zu können.

Unter dem Reiter **Zugriffsbeschränkung** kann eine zeitliche Beschränkung des lokalen unter remote-Zugriffs konfiguriert werden. Wenn hier im **Systemzugriff** die Auswahl **Zeitprofil** getroffen wird, können Sie einen neuen Zeitplan anlegen, in welchem die erlaubten und nicht erlaubten Zeiten markiert werden können.

15. Raumübersicht

Die Raumübersicht zeigt Ihnen alle angelegten Räume in den jeweiligen Bereichen. Sie können hier weitere Bereiche, Komponenten und Automationen sowohl hinzufügen als auch löschen. Des Weiteren lassen sich diese natürlich auch bearbeiten.

15.1. Räume hinzufügen / löschen

Wenn Sie sich in der Raumübersicht befinden können Sie mit dem Symbol in der oberen rechten Ecke den Bearbeitungsmodus starten.

Sie haben nun die Möglichkeit über das Plus-Symbol einen Raum hinzuzufügen. Sie haben die Wahl, in welchen Bereich Sie diesen setzen.

Über das X-Symbol, welches Ihnen an jedem bestehenden Raum angezeigt wird, können Sie den jeweiligen Raum entfernen. Es dürfen sich hierfür keine eingelernten Komponenten in dem Raum befinden.

15.2. Räume bearbeiten

Um einen Raum zu bearbeiten, rufen Sie über die Raumübersicht diesen auf, klicken zuerst auf das Bearbeitungs-Symbol rechts oben und anschließend auf das Zahnrad-Symbol. Sie können hier nun den Namen und das Icon bearbeiten, sowie die Bereiche wählen, in welchen sich der Raum befinden soll.

15.3. Komponenten hinzufügen (Inklusion)

Um eine Komponente hinzuzufügen, müssen Sie als erstes einen gewünschten Raum wählen. Wenn Sie sich in diesem befinden, können Sie mit dem Symbol in der oberen rechten Ecke den Bearbeitungsmodus starten.

Sie sehen nun den Button **Weiteres Gerät hinzufügen**. Wenn Sie dieses wählen, bekommen Sie eine Seite, welche Ihnen im ersten Schritt die Auswahlmöglichkeiten **ABUS** und **Andere** gibt. Wählen Sie hier also als erstes, ob Sie eine ABUS-Komponente, oder eine Fremdhersteller-Komponente haben.

Hinweis

Nach dem Versetzen einer netzgebundenen Komponente muss die Funktion „Mesh-Netzwerk neu routen“ in der Z-Wave Erweiterung gestartet werden, um das Routing des Z-Wave Netzwerks neu zu starten.

15.3.1. ABUS – Komponente einlernen

Unter dem Punkt **ABUS** finden sich die Kategorien **ABUS-Kamera**, **ABUS-Z-Wave**, und **ABUS-wAppLoxx**.

ABUS - Kamera:

Nachdem Sie den gewünschten **Kameratyp** gewählt, sowie den Namen der Kamera vergeben haben, sucht die Nexello nach ABUS-Cams in Ihrem Netzwerk. Wählen Sie, wenn nicht schon von der Anlage geschehen, die einzulernende Kamera aus und tragen den richtigen **Gerätesicherheitscode** sowie den **Administratorcode** ein. Nach einem kurzen Ladevorgang sollte die Kamera hinzugefügt sein.

*Beachten Sie bitte, dass die Kamera vor dem Hinzufügen in die **Nexello-App** in der **App2CamPlus** eingerichtet worden sein muss. Der **Gerätesicherheitscode** sowie der **Administratorcode** müssen zwingend verändert werden.*

ABUS - Z-Wave:

Hier können Sie alle für die Nexello freigegebenen ABUS-Z-Wave-Komponenten einlernen. Andere Z-Wave-Produkte werden unter **Andere** eingelernt.

Wählen Sie den einzulernenden Gerätetyp aus, vergeben den Gerätenamen und klicken auf **Anlernvorgang starten**. Beachten Sie anschließend die gerätespezifischen Informationen zum Einlernvorgang, welche Ihnen in der App angezeigt werden.

ABUS – wAppLoxx (optional):

Um einen **WLX Schließzylinder** einzulernen, wählen Sie diesen unter dem Menüpunkt aus und klicken auf Anlernvorgang **starten.** Sie werden nun von der App geleitet. Nach dem Vorhalten der Systemkarte (und ggfls. der Reset-Karte beim ersten Zylinder) ist der Zylinder hinzugefügt.

Ihre Tags zum Bedienen der Zylinder werden vom Administrator in der Benutzerverwaltung den jeweiligen Nutzern hinzugefügt.

Wenn Ihnen eine Auswahlmöglichkeit fehlt, wird das zuständige Modul nicht erkannt. Überprüfen Sie, ob dieses richtig gesteckt ist. Trennen Sie ggfls. de Spannungsversorgung der Zentrale und stecken das Modul neu.

15.3.2. Andere Komponente einlernen (Fremdprodukt)

Unter dem Punkt **Andere** finden sich die Kategorien **Türstation**, **Z-Wave**, und **smartCONTROL Funktion**.

Türstation:

Hier können Sie aus bestehenden, schon eingelernten Einzelkomponenten eine virtuelle Türstation erzeugen. Bitte stellen Sie sicher, dass alle gewünschten Komponenten bereits eingelernt sind.

Z-Wave:

Um ein von einem Fremdhersteller bezogenes Z-Wave-Gerät hinzuzufügen, starten Sie den Einlernvorgang in diesem Menüpunkt. Halten Sie sich hierbei an die dem Gerät beiliegende Inklusionsanleitung.

smartCONTROL Funktion:

In diesem Menü können Sie der Anlage virtuelle Geräte hinzufügen, um diese später in Automationen und per Hotkeys nutzen zu können.

Folgende virtuelle Geräte können Sie hinzufügen:

- **Timer** – hierbei handelt es sich um eine virtuelle Zeitschaltuhr
- **Virtueller Blink-Aktor** – wenn dieser virtuelle Eingang aktiviert ist, schaltet dieser automatisch im Wechsel An- und Aus. Maximale Blink-Impulse können eingestellt werden.
- **Virtueller Rollladenschalter** – kann für eine Rollladenschaltung genutzt werden
- **Virtueller Schalter** – Einfacher Schalter, Ein- und Ausschaltverzögerung möglich
- **Virtueller Taster** – Einfacher Taster (Impulsschalter), Ein- und Ausschaltverzögerung möglich

15.4. Komponente entfernen (exkludieren)

Zum Entfernen einer Komponente gibt es zwei Möglichkeiten.

Die Standardmethode zum exkludieren einer Komponente starten Sie über die **Raumübersicht**. Betreten Sie den Raum, in welchem sich die zu entfernende Komponente befindet und starten den **Bearbeitungsmodus.** Neben der Komponente erscheint ein X-Symbol. Durch Klick hierauf wird der Exklusionsvorgang gestartet. Beachten Sie hier bitte die gerätespezifischen Informationen in der App.

Sie können eine Exklusion außerdem über den Erweiterungspunkt **Z-Wave** starten. Hier können Sie auch ein defektes, oder nicht vorhandenes Gerät löschen. Die hierfür benötigte **Geräte-ID** finden Sie in den Erweiterten Einstellungen der Komponente.

15.5. Komponenten bearbeiten

Die aufgeführten Unterpunkte beziehen sich auf ABUS-Z-Wave-Komponenten. Andere Z-Wave-Komponenten können sich hiervon unterscheiden. Die Unterpunkte bei Kameras finden sie hier.

15.5.1. Bedienung

In der **Bedienung** können Sie keine Einstellungen ändern, jedoch haben Sie eine Statusübersicht über die jeweilige Komponente. Es werden Ihnen die produktspezifischen Sensoren, sowie der **Batteriestatus** etc. angezeigt.

15.5.2. Geräteeinstellungen

In den **Geräteeinstellungen** kann die Grundkonfiguration für die Komponente vorgenommen werden. Neben dem **Icon** und dem **Namen** können Sie den Sprachassistent für diese Komponente aktivieren oder einstellen, ob der Melder automatisierbar sein soll.

Unter **Erweiterte Konfiguration** kann die **Größe** und der **Wert** von speziellen **Parametern** abgefragt und geändert werden. Informationen zu den Parametern können Sie der dem Produkt beiliegenden Anleitung entnehmen.

15.5.3. Verwendung

Den Punkt **Verwendung** finden Sie nur unter bestimmten Komponenten. Hier können Zusatzfunktionen wie die Tastenbelegung bei einem Taster definiert werden.

15.5.4. Erweiterte Einstellungen

In diesem Menü können für jede Komponente unterschiedliche Zusatzeinstellungen getroffen werden. Außerdem finden Sie hier unter **Weitere Informationen** die **Netzwerk-ID** sowie die **Geräte-ID**, welche zum Exkludieren eines defekten Geräts benötigt wird.

Unter **Aufwachzeit** können Sie definieren, wie oft die Komponente von sich aus ein Wake-Up-Signal aussendet, d.h. sich bei der Anlage meldet.

In der **Konfiguration** haben je nach Produkt, spezielle Einstellungsmöglichkeiten. Jeder dieser Möglichkeiten wird unter dem Info-Symbol in der App genau beschrieben.

15.5.5. Geräteinformationen

In den Geräteinformationen finden Sie folgende Angaben:

- Hersteller
- System
- Bezeichnung
- Typ

15.5.6. Verknüpfungen

In den Verknüpfungen sind alle angelegten Automationen aufgelistet, in welche die Komponente eingebunden ist.

15.6. wAppLoxx (WLX)

Wie unter **15.3.1** beschrieben können Sie bis zu vier WLX-Schließzylinder in die Nexello einlernen.

Durch Auswahl Ihres WLX-Zylinders in der Raumübersicht können Sie über das Einstellungssymbol in der rechten oberen Ecke folgendes auswählen:

- **Bedienung:** Öffnen/Schließen des Zylinders + Permanenter Zugriff (**Achtung:** Funktion nur als User nutzbar)
- **Geräteeinstellungen:** Vergabe des Gerätenamens, Raumauswahl, Auswahl Automatisierbar Ja/Nein
- **Fallback Tags:** Vergeben Sie hier Ihren eingelernten Benutzertags die Fallback-Rechte. Fallback-Tags können die Zylinder auch bei einer fehlenden Verbindung zur Anlage öffnen.
- **Erweiterte Einstellungen:** Auswahl Anlernzylinder An/Aus, Öffnungszeit 6 Sek/ 12 Sek
- **Geräteinformationen:** Angabe Hersteller, System, Bezeichnung & Typ

Hinweis

Der erste eingelernte Tag wird automatisch mit Fallback-Rechten ausgestattet

16. Automationen

In den Automationen können Sie verschiedene Wenn-Dann-Verknüpfungen erstellen. Im ‚Wenn'-Teil werden Bedingungen erfasst. Sind diese erfüllt, schalten die Komponenten auf den im ‚Dann'-Teil konfigurierten Zustand.

Achtung

Automationen dürfen sich nicht zirkulär gegenseitig aufrufen!

Bedingungen in einem ‚Oder'-Block gelten bei Zutreffen einer einzelnen Teilbedingung als erfüllt. Bedingungen in einem ‚Und'-Block hingegen gelten erst als erfüllt, wenn alle Teilbedingungen zutreffen.

Es gibt hier zur Auswahl:

- Automation: Die Standard-Automation ermöglicht die automatische Schaltung von Geräten anhand definierter Bedingungen.
- An/Aus – Automation: Bietet die Möglichkeit, zusammenhängende Schaltaktionen für An/Aus-Aktoren in einer Hülle zusammen zu fassen. In den Dann-Teil können nur An/Aus-Aktoren oder Dimm-Geräte eingefügt werden.
- Rollladen – Automation: Bietet die Möglichkeit, zusammenhängende Schaltaktionen für Rollläden in einer Hülle zusammen zu fassen. In den Dann-Teil können nur Rollladen-Aktoren eingefügt werden.
- Toggle – Automation: Mit einer Toggle-Automation können Sie bei Zutreffen einer Bedingung der Reihe nach zwischen verschiedenen Unter-Automationen wechseln. Die Bedingung der Unter-Automationen ist immer gleich, nur der Dann-Teil weicht voneinander ab.
- Toggle – Automation An/Aus: Diese Automation unterscheidet sich nur insofern von der normalen Toggle-Automation, dass diese jeweils fest An und Aus im Dann-Teil stehen haben.

Hinweis

Automationen tauchen in nur in den Hotkeys auf, wenn diese einem Raum zugewiesen sind

17. Kameraübersicht

Hier finden Sie alle der Anlage hinzugefügten Kameras. Durch Klick auf eine dieser Kameras gelangen Sie in die **Bedienung.** Nachdem Sie in die Bedienung gewechselt haben, können Sie durch Klick auf das Einstellungssymbol rechts oben, weitere Kamera-Einstellungen öffnen.

17.1. Bedienung

In der **Bedienung** können Sie diverse Funktionen der Kamera nutzen. Außerdem haben Sie hier Zugriff auf den **Livemodus**, in welchem Sie alle 5 Sekunden einen aktuellen Snapshot der Kamera angezeigt bekommen. Im **Bildarchiv** können die bisher getätigten Aufzeichnungen betrachten.

Unterhalb des angezeigten „Livebildes“ finden sich zwei Buttons – ein Foto-Symbol, mit welchem Sie ein Einzelbild aufnehmen können, sowie ein Blatt-Symbol, mit welchem sich eine Bilderreihe (Einstellbar unter Erw. Einst.) aufnehmen lässt.

Position anfahren: Anfahren einer der davor abgespeicherten Positionen
Position speichern: Drei Positionen speicherbar, um diese anzufahren
Letztes Bild: Zeitstempel des zuletzt aufgenommenen Bilds
Bewegungsmelder: Anzeige ob Auslösung der Bewegungserkennung
Neigen/Schwenken: PIZ-Funktion der Kamera – Kamerasteuerung
Scharfschaltung: scharf/unscharf-schalten der Bewegungserkennung
Aufzeichnung: Starten einer Videoaufzeichnung (1 Min; auf SD-Karte in der Kamera)
Störung: Anzeige ob Störung in der Kamera vorhanden

17.2. Geräteeinstellungen

Hier können Sie über das Zahnradsymbol im rechten oberen Bildschirmrand die Grundeinstellungen für die Kamera festlegen:

- Name und Icon
- Raumzuweisung
- Automatisierbar – Ja/Nein
- Sprachassistent aktivieren – Ja/Nein
- PT-Kalibrierung auslösen

17.3. Reversible Zustände

Hier können Sie die Gerätespezifische Einstellungen zu den **reversiblen Zuständen** für jeden Alarmtyp einzeln festlegen.

Manuell: Einstellung Scharfschaltung manuell für dieses Gerät festlegen
Auto: Der Reversible Zustand wird aus den übergreifenden Einstellungen übernommen (System)
Aus: Dieses Gerät reagiert auf keine reversiblen Zustände

17.4. Erweiterte Einstellungen

Hier finden Sie die **Erweiterten Einstellungen** zu Ihrer Kamera.

Unter **Kamerabild** können Sie den **Gerätesicherheitscode**, sowie den **Admincode** der Kamera hinterlegen, sowie das Intervall der Bildabfrage einstellen. Legen Sie fest, wie oft die Anlage einen Snapshot von der Kamera abfragt (Default 5 Sek). Des Weiteren wird Ihnen die **Gerätekennung (DID)** der Kamera angezeigt.

Unter **Aufnahme** stellen Sie die Anzahl der Bilder ein, welche bei Auslösung der Aufzeichnung aufgenommen werden, sowie das Intervall, in welchem dies geschehen soll.

17.5. Geräteinformationen

In den **Geräteinformationen** werden Ihnen die Grunddaten der Kamera angezeigt – sie sehen hier **Hersteller**, **System, Bezeichnung** und **Typ** der Kamera.

17.6. Verknüpfungen

Unter Verknüpfungen werden Ihnen alle Automationen angezeigt, in welchen die Kameras genutzt werden.

18. Erweiterungen

In den Erweiterungen werden Ihnen alle auf der Anlage installierten Module angezeigt. Sie haben hier die Möglichkeit, diese Erweiterungen im jeweiligen Punkt zu konfigurieren. Des Weiteren können Sie Erweiterungen über den Shop erwerben.

18.1. E-Mail-Benachrichtigungen

Unter dem Reiter **E-Mail-Benachrichtigungen** können Sie den Postausgangsserver für den E-Mail-Versand einstellen. Hier wird also Ihr E-Mail-Konto hinterlegt, von welchem die Mails von Ihrer Zentrale verschickt werden.

Nachdem Sie den Button „konfigurieren“ gedrückt haben, müssen Sie als erstes Ihre E-Mail-Adresse und das zugehörige Passwort hinterlegen.

Je nach Provider wird im nächsten Punkt der Postausgangsserver (SMTP) abgefragt. In Einzelfällen müssen Sie hiernach noch den SMTP-Port eingeben. Meist wird dieser jedoch von der Anlage ergänzt.

18.2. Push-Benachrichtigungen

In den **Push-Benachrichtigungen** können für Push eingerichteten Endgeräte verwaltet werden, bzw. noch nicht eingerichtete registriert werden.

Ist Ihr Endgerät noch nicht in der Push-Liste zu finden, können Sie den Button **Dieses Gerät registrieren** betätigen.

Durch Auswahl eines angezeigten Gerätes können Sie dieses bearbeiten. Hier können Sie den **Gerätename**, den **zugeordneten Benutzer** sowie den **Status** abändern, sowie das Gerät aus dem Push-Service **löschen**.

*Beachten Sie, dass dem **Endgerät** ein **Benutzer** zugeordnet sein muss. Andernfalls wird dieses Gerät keine Push-Mitteilungen empfangen.*

18.3. Z-Wave

Unter Konfiguration können Sie ein **Gerät inkludieren**, ein **Gerät exkludieren**, das **Mesh-Netzwerk neu routen**, den **Z-Wave Modul Werksreset** durchführen oder ein **fehlerhaftes Gerät entfernen**.

Gerät inkludieren: Über diese Funktion können Sie eine Z-Wave Komponente in die Nexello einlernen. Wir empfehlen, den Weg über die Raumübersicht zu nutzen.

Gerät exkludieren: Mithilfe dieser Funktion können Sie eine beliebige Komponente aus der Anlage entfernen und somit auch zurücksetzen. Sie können auch eine nicht in Ihre Anlage inkludierte Komponente hierüber resetten.

Mesh-Netzwerk neu routen: Über diese Funktion können Sie Ihr Z-Wave Netzwerk manuell neu routen lassen. Die Gateway wird automatisch die besten Wege berechnen und diese in den Routing-Tabellen hinterlegen. Nutzen Sie diese Funktion immer, wenn Sie eine Netz-Komponente in Ihrem Objekt versetzt haben.

Beachten Sie, dass es je nach Größe des Netzwerks mehrere Stunden dauern kann, bis das Routing abgeschlossen ist. In dieser Zeit kann es zu Verzögerungen im der Funkauswertung kommen.

Z-Wave Modul Werksreset: Diese Funktion dient zum Zurücksetzen Ihres Z-Wave Moduls. Alle Z-Wave Komponenten müssen hiernach manuell zurückgesetzt und neu inkludiert werden.

Fehlerhaftes Gerät entfernen: Mit dieser Funktion können Sie ein fehlerhaftes Gerät zwangslöschen. Die einzugebende Geräte-ID finden Sie in den erweiterten Einstellungen der jeweiligen Komponente.

***Vorsicht:** Durch das Resetten des Netzwerks werden alle Z-Wave-Komponenten aus Ihrer Zentrale gelöscht, sowie alle Z-Wave-Einstellungen zurückgesetzt.*

Bitte warten Sie nach dem Reset des Z-Wave Moduls mindestens 10 Minuten bis Sie mit der Inklusion neuer Komponenten beginnen.

18.4. Sprachassistent Alexa

Mit Hilfe der Sprachsteuerung können Geräte und Automationen komfortabel ohne Tastendruck bedient werden.

1. Installieren Sie den Nexello-Skill in Ihrer Alexa-App
2. Kopieren Sie den in der Nexello-App angezeigten Aktivierungscode
3. Fügen Sie den kopierten Aktivierungscode in den Nexello-Skill Ihrer Alexa-App ein

Nachdem Sie dies eingerichtet haben, können Sie den Sprachassistent für jedes Gerät einzeln unter **12.5.2 Geräteeinstellungen** aktivieren.

18.5. UMTS (Mobilfunk-Modul)

Unter der Erweiterung **UMTS** können Sie die Konfiguration Ihres Mobilfunkmoduls (PLAC90220) vornehmen, sowie alle Informationen hierzu auslesen.

Info:

Über den Punkt **Info** können Sie sich alle relevanten Daten zum Mobilfunkmodul und der eingelegten SIM-Karte anzeigen lassen. Hier sehen Sie auch den **Verbindungsstatus**, die **Signalstärke** und den **Datenverbrauch**.

Webinterface:

Mit den Klick auf den Button **Öffnen** werden Sie auf die Weboberfläche des UMTS-Sticks weitergeleitet.

Zur Nutzung der Funktionen sind folgende Schritte notwendig:

1. Aktivieren Sie hier unter dem Reiter **Mobile Network** das **Data Roaming**
2. Fügen Sie durch einen Klick auf das Plus-Symbol unter **Profiles** ein neues Profil hinzu
3. Vergeben Sie einen beliebigen Profilnamen, lassen Sie die Felder **Username** & **Password** frei
4. Geben Sie im Feld **APN** folgendes ein: **iot.1nce.net**
5. Klicken Sie auf **Save**

Unter dem Reiter **Home** sollten nun alle Verbindungen in grün angezeigt werden.

Das Webinterface des Mobilfunk-Moduls ist nur bei lokalem Zugriff auf die Anlage erreichbar. Bei einem Fernzugriff ist das Webinterface nicht aufrufbar.

19. System

19.1. Informationen

In den **System-Informationen** sehen Sie alle wichtigen Daten der Anlage:

- **App** -> Uhrzeit, Name, Version & Domain
- **Benutzer** -> Angemeldeter Nutzer, Berechtigungen & Sprache
- **Nexello** -> Zeit d. Nexello, Server IP, Client IP, MAC, Server-Version, Updatemanager-Version, Z/IP Gateway Version, Angeforderte API, Übersetzungs-Version, Gerätelisten-Version
- **Module** -> Anzeige aller installierten Module
- **Systeme** -> Anzeige aller installierten Systeme
- **Sprachen** -> Auf der Anlage installierte Sprachen
- **Push-Benachrichtigungen** -> Anzeige aller registrierten Push-Geräte
- **Sprachassistent** -> OAuth-URL

19.2. System Einstellungen

Sie haben hier die Funktionen

- **Neustart**, zum manuellen neu starten der Zentrale
- **Nach Updates suchen**, um den Server nach neu verfügbaren Updates zu durchsuchen
- und **Lizenzen synchronisieren**, um Ihre gekauften Module zu aktualisieren

19.3. System zurücksetzen

Über den Punkt **System zurücksetzen** können Sie App- und Anlagenbezogene Resets durchführen.

APP:

- **Cache löschen**: Löscht alle im Zwischenspeicher der App enthaltenen Daten
- **App-Daten zurücksetzen**: Löscht alle Einstellungen und Daten der App (Zustand wie nach Erstinstallation)

Gerätespeicher:

- **Werkseinstellungen Server**: Setzt die Anlage komplett auf Werkseinstellungen. Alle Daten werden gelöscht.

Sie haben alternativ die Möglichkeit, die Anlage mithilfe des Reset-Tasters zurückzusetzen.

19.4. Systemsicherung

In der **Systemsicherung** haben Sie die Möglichkeit ein Backup zu starten sowie ein solches wiederherzustellen.

Für diese Funktionen muss ein USB-Speichergerät in der Zentrale eingesteckt sein.

Durch den Druck auf **Backup starten** öffnet sich ein Dialogfenster, in welchem Sie ein Passwort für das Backup vergeben müssen. Nachdem Sie dies getan haben wird die Backup-Datei auf dem USB-Stick abgelegt.

Wenn Sie auf **Backup wiederherstellen** klicken, durchsucht die Anlage den gesteckten USB-Stick nach gespeicherten Backup-Dateien und listet diese auf. Nach Eingabe des vergebenen Passworts wird das Backup auf die Zentrale aufgespielt

Deutsch

20. Ereignisspeicher (Log Status)

Ereignis	Erklärung	Aktion
Warnungen		
Alarmzentrale: Warnung **Kein Netzwerk**	Netzwerkverbindung getrennt	Physische Verbindung zum Router prüfen; DSL Verbindung prüfen
Alarmzentale: Warnung **Stromversorgung**	5V Spannungsversorgung liegt nicht an	Netzteil prüfen; Spannungsversorgung wiederherstellen
Alarmzentale: Warnung **Stromversorgung verbunden**	5V Spannungsversorgung liegt wieder an	keine Aktion erforderlich
Kamera: Störung **Keine Verbindung**	Netzwerkverbindung zur Kamera wurde verloren	Netzwerkverbindung der Kamera prüfen
Kamera: Störung **Keine Störung**	Kamera Störungsfrei	Keine Aktion erforderlich
Komponente: Status **Kein Signal**	Funk--Verbindung zur Komponente XY verloren	Funktion der Komponente, Signalstärke und Batteriespannung überprüfen
Komponente: **Z %**	Batteriestand der Komponente XY = Z %	Aktion nicht zwingend erforderlich. Wenn Batteriestand unter 20% -> Empfehlung Batterie wechseln
Komponente: Status **Ok**	Funk-Verbindung zur Komponente XY wiederhergestellt	keine Aktion erforderlich
Alarmbereich: Warnung **Aktivierungsstörung**	Anlage konnte wegen anstehender Störung nicht aktiviert werden	Störung beseitigen
Jamming	Eine Funk-Überlagerung wurde erkannt	Eventuelle Störsignale ausfindig machen; Errichter kontaktieren; Bei häufigem Auftreten Funkmessung durchführen
Perimeterwarnung	Eine Auslösung im Außenbereich hat stattgefunden	Außenbereich überprüfen
Alarme		
Einbruch	Ein Einbruchalarm wurde ausgelöst	Echtheit des Alarms überprüfen; ggfls. Notdienste benachrichtigen; Alarm quittieren
Überflutung	Ein Überflutungsalarm wurde ausgelöst	Objekt nach Überflutung überprüfen; Alarm quittieren
Gas	Ein Gasalarm wurde ausgelöst	Objekt umgehend verlassen; Notdienste benachrichtigen; Alarm quittieren
Medizinisch	Ein medizinischer Alarm wurde ausgelöst	Zustand der medizinisch überwachten Person prüfen; Alarm quittieren

Panik	Ein Panikalarm wurde ausgelöst	Notdienste benachrichtigen; Alarm quittieren
Sabotage	Ein Sabotagealarm wurde ausgelöst	Komponente überprüfen (Sabotagekontakt); Alarm quittieren
Bedrohung	Ein Bedrohungsalarm wurde ausgelöst	Notdienste benachrichtigen; Alarm quittieren
Rauch	Ein Feueralarm wurde ausgelöst	Objekt umgehend verlassen; Notdienste benachrichtigen; Alarm quittieren
Statusänderungen		
Aktiv	Der Alarmbereich wurde extern aktiviert	keine Aktion erforderlich
Deaktiv	Der Alarmbereich wurde deaktiviert	keine Aktion erforderlich
Intern aktiv	Der Alarmbereich wurde intern aktiviert	keine Aktion erforderlich
Sonstiges		
Quittiert	Der Alarm wurde quittiert	keine Aktion erforderlich
Name - **Automation 1**	Automation wurde ausgeführt	keine Aktion erforderlich
Zutritts-Status: **Zutritt gewährt**	wAppLoxx-Zylinder - Zutritt durch legitimes Medium gewährt	keine Aktion erforderlich
Zutritts-Status: **Tag unbekannt**	wAppLoxx-Zylinder - unbekanntes Medium wurde vorgehalten	ggfls. Medium einlernen
Nexello neu gestartet	Anlage startet neu	keine Aktion erforderlich
Nexello wird neu gestartet	Anlage wurde manuell neu gestartet	keine Aktion erforderlich
Server-Update wurde durchgeführt	Update durchgeführt von Version X auf Version Y	keine Aktion erforderlich

21. App-Fehlermeldungen

Folgende Fehlermeldungen können bei der Benutzung der App auftreten:

„Verschlüsselung bei Rückmeldung vom Portal nicht dekodierbar (4001).“

➔ Ihre App wurde nicht richtig verifiziert. Führen Sie die Verifizierung mithilfe des QR-Codes im Portal durch.

22. Zusätzliche Informationen / Anhang

22.1. Browser-Zugriff

Über die IP-Adresse der Nexello können Sie auch über den Webbrowser Ihres PC's/Mac auf die Anlage zugreifen und diese hierüber konfigurieren und bedienen.

https://<YourDeviceIP>

Für den Zugriff ist auch hier einmalig eine Verifizierung des Browsers notwendig. Fügen Sie hierfür den im Nexello-Pilot unter **Accountinfo - App verifizieren** hinterlegten QR-Code, durch Kopieren des Textes unter dem QR-Code, in die Verifizierungsmaske ein.

Hinweis: *Wir empfehlen derzeit ausschließlich den Webbrowser ‚**Edge**' sowie den ‚**Chrome**' beim Zugriff auf das Nexello Portal, sowie auf die Nexello selbst zu nutzen.*

22.2. Technische Daten

Abmessungen	(B x L x H) 300 x 180 x 50
Alarmierung	Push-Benachrichtigung / E-Mail / Akustisches Warnsignal / Anruf & SMS (optional)
Anzahl Benutzer	50
Anzahl Ereignisse	2000
Anzahl Z-Wave Komponenten	100
Anzahl Bluetooth Komponenten	3
Anzahl WLX Pro Komponenten	3
Anzahl IP-Kameras	4
Anzahl Automationen	100
Anzeige	LED
Batterie - Batterie im Lieferumfang enthalten	Ja
Batterie - Typ	3,7 V 5.000 mAh 18,5 Wh
Batterie - wiederaufladbar	Ja
Benutzerstufen	3 (Installer; Owner; User)
Bruttogewicht (kg)	0,9
Nettogewicht (kg)	0,72
Farbe	weiß
Funkfrequenz	868,42 (Z-Wave Plus) 2.4/5GHz (WLAN/Bluetooth)
Funk-Modulation	Z-Wave Plus (S2) / FSK (BFSK / GFSK)
Funkreichweite (m)	max. 20 - 40 (im Gebäude)
Gehäusematerial	Kunststoff
Gleichzeitiger Netzwerkzugriff	3
Kompatibel zu	Z-Wave Komponenten (EU-Frequenz: 868,42MHz), Bluetooth Komponenten (2.4 GHz), WLX Pro Zylinder (868MHz)
Kompatibel zu wAppLoxx Pro	Ja

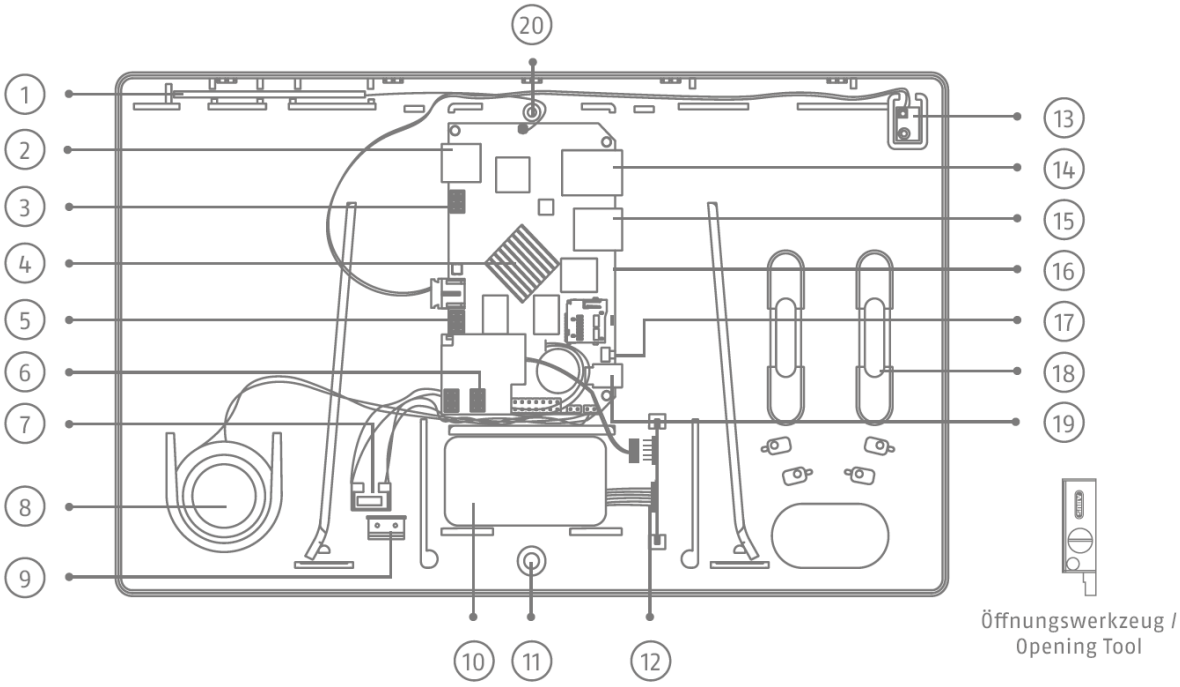
Lautsprecher	Ja
Leuchtfarbe	Blau / Gelb / Rot / Grün / Weiß
Max. Betriebstemperatur (°C)	40
Max. Luftfeuchtigkeit (%)	70
Min. Betriebstemperatur (°C)	0
Min. Luftfeuchtigkeit (%)	5
Netzwerkanschluss	RJ-45 Buchse (10/100 Mbit/s)
Notstromversorgung	Ja
Sabotageschutz	Ja
Schalldruck (dB @1m)	70
Sendeleistung (dBm)	16
Software	App: ABUS Nexello (Android / iOS), HTTPS Webserver
Spannungsversorgung DC	5V
Steckertyp	DC-Stecker 4 / 1.7 mm
Stromaufnahme (mA)	43,5
Stromaufnahme Standby (mA)	30,5
Unterstütze IP-Kameras	PPIC32020 / PPIC32520 / PPIC34520 / PPIC35520 / PPIC36520 / PPIC90000
Verschlüsselung	AES128, HTTPS, SSL
Teilbereiche/Überwachungsbereich	2 + Gemeinsamer Bereich
Verpackungsmaße LxBxH	34 x 22 x 13
Fernwartung	Ja (Portal & App)
Max. Notstrom Laufzeit (h)	5
Netzteil	extern
Netzwerk-Protokolle	HTTPS

22.3. LED-Anzeigen

Generell:
Blinkend = Vorgang in Aktion
Leuchtend = Stabiler Zustand

LED	LED-Anzeige	System	Alarmzentrale	USB-Stick
	Weiß leuchtend	Bootvorgang abgeschlossen (weitere Systemschritte ausstehend)	//	//
	Weiß blinkend	Bootvorgang in Aktion	//	//
	Blau leuchtend	LAN/WLAN Suche (keine Netzwerkkonfiguration gefunden)	Anlage scharf / intern scharf	//
	Blau blinkend	WLAN-Konfiguration	Verzögerung Ein-/Ausgangsweg	//
	Rot leuchtend	//	Alarm stummgeschalten	//
	Rot blinkend	Fehler/Problem liegt vor	Alarm anstehend	Fehler bei Ausführung vom Stick
	Gelb leuchtend	Suche nach Updates, Lizenzen, Daten auf dem Stick	Störung anstehend	//
	Gelb blinkend	Installation von Updates, Lizenzen	Störung beim Aktivieren (scharf / intern scharf)	//
	Grün leuchtend	Alles i.O / normaler Betriebszustand	Anlage unscharf	//
	Grün blinkend	//	//	Erfolgreiche Verarbeitung
	Violett blinkend	Datei von USB-Stick wird ausgeführt	//	Stick erkannt

22.4. Gerätedetails



1. WLAN / Bluetooth Antenne
2. USB-Steckplatz 1
3. Steckplatz für WLX Pro Modul
4. Hauptplatine
5. Steckplatz für Z-Wave Modul
6. Audiomodul
7. Sabotageschalter Deckel
8. Lautsprecher
9. Sabotageschalter Wand
10. Akku
11. Schraubendurchführung zur Fixierung am Wandanker
12. Ladeelektronik für Notstromversorgung
13. LED für Statusanzeige
14. Netzwerkanschluss
15. USB-Steckplatz 2 + 3
16. Micro SD Card Slot
17. Reset-Taster
18. Zugentlastungen
19. Stromversorgung DC Buchse
20. Schraubdome zur Fixierung der Abdeckung

Die Anzeige & Ausgabe der Status LED u. des Lautsprechers kann von Ihrem Nexello Fachpartner einem einzelnen, oder beiden Teilbereichen gemeinsam zugeordnet, bzw. ausgeschalten werden.

Sabotageschutz:

Unterhalb des **Netzteilanschlusses** befinden sich die Anschlüsse für die beiden **Sabotagekontakte** der Nexello. Es handelt sich hierbei um **NO** (normally open) Kontakte. Um die **Sabotagekontakte** zu „überbrücken“, ziehen Sie die Kabel einfach von den Anschlüssen ab.

Akkuverhalten:

Bei **optimaler Stromversorgung** liegt das reguläre Spannungslevel deutlich **über 4V**. Das **maximale** Spannungslevel liegt systembedingt bei **5V**. Bei einer Unterbrechung der regulären Stromversorgung sinkt das Spannungslevel mit der Entladung der Batterien bis zu einem Level von **3,7V**. Dann schaltet sich das Hauptsystem der Nexello ab (wird runtergefahren). Das Powerboard **bleibt aktiv**, um bereit zu sein, wenn die Batterien wieder geladen werden können.

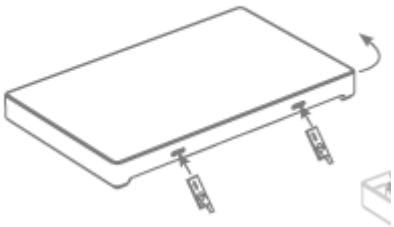
Der **kritische Bereich** des Spannungslevels liegt bei **3.3V**. Wird dieser unterschritten kann das Powerboard nicht mehr anschließend die Batterie laden und es kann ab da zu den Tiefenentladungsbeeinträchtigungen bei den Batterien kommen. **Daraus folgt:** Dauert ein Ausfall der Hauptstromversorgung über den Überbrückungszeitraum der Batterien hinaus an, so sollten bald Maßnahmen getroffen werden, um die Batterien von der Lösung zu trennen.

22.5. Hinweise zur Zentrale

Gehäusedeckel öffnen & Sabotageschutz

Die Nexello Zentrale ist durch einen Deckelkontakt sowie durch einen Kontakt zur Wandhalterung vor Sabotage geschützt. Setzen Sie das System vor dem Öffnen in den Wartungs-Modus um eine Alarmauslösung zu verhindern.

Schieben Sie die Öffnungstools in die Auslässe um den Deckel zu lösen.



Reset-Taster

Die Reset-Taste verfügt über 3 Funktionen:

Kurz drücken	=	System Neustart
3 Sekunden drücken	=	System startet den Wifi Konfigurations-Modus
10 Sekunden drücken	=	System setzt sich in den Werkszustand zurück.

Die Verknüpfung der Zentrale mit Ihrem Nexello-Fachpartner Account bleibt nach Reset weiterhin bestehen. Um alle Module und Verknüpfungen der zentrale zurückzusetzen, muss ein RMA-Vorgang über den Abus-Support angestoßen werden.

22.6. Firewall

Wenn Sie die Nexello in einem Netzwerk installieren, welches durch eine Firewall geschützt wird, müssen zur Nutzung der jeweiligen Dienste folgende Ports geöffnet werden:

- Zeitabfrage: 123
- Module / Lizenzen: 443
- Updates: 1443
- RemoteHome Zentrale: 4444 + 4447
- RemoteHome Browser: 4452
- Browserzugriff: 8081
- RemoteHome App: 4450 + 4451

22.7. Wartung und Instandhaltung durch Errichter

Die Zentrale sollte einmal pro Jahr überprüft werden. Bei jeder Inspektion:

- Überprüfen Sie die Nexello auf offensichtliche Anzeichen von Schäden an dem Gehäuse oder der Frontabdeckung.
- Überprüfen Sie die Wirkung des Gehäuse-Sabotage-Schalters und des Wand-Sabotage-Schalter (Wandabrisskontakt)
- Überprüfen Sie den Zustand der Notstrom-Akkus
- Überprüfen Sie die Verkabelung auf Anzeichen von Schäden oder Verschleiß
- 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 alle Melder durch.
- Testen Sie alle externen Signalgeber
- Testen Sie die Kommunikation.

22.8. FAQ

- Was ist der gemeinsame Bereich?

Im gemeinsamen Bereich befinden sich alle Melder, welche dem Bereich 1, sowie dem Bereich 2 zugewiesen sind – also beiden Bereichen. Diese Melder sind nur aktiv, wenn auch beide Bereiche scharf geschalten sind. Der gemeinsame Bereich kann z.B. bei einem Mehrfamilienhaus für den Eingangsbereich (Treppenhaus) genutzt werden.

- Was mache ich, wenn ich eine Z-Wave Komponente nicht einlernen kann?

Wenn sich eine Z-Wave Komponente nicht einlernen lässt, ist im ersten Schritt zu vermuten, dass sich diese noch im Inkludierten Zustand befindet. In diesem Fall muss die Komponente, bevor sie sich einlernen lässt, auf Werkseinstellungen zurückgesetzt werden. Wie Sie die Werkseinstellungen der jeweiligen Komponente herstellen, können Sie, nachdem Sie die Inklusion gestartet haben, unter dem angezeigten Info-Symbol nachlesen. Alternativ finden Sie eine Anleitung hierzu in den Unterlagen des jeweiligen Produkts.

- Wie teste ich die Melder in meiner Nexello?

Grundsätzlich empfehlen wir eine jährliche Wartung samt Batteriewechsel der Komponenten durch eine Fachfirma. Wenn Sie ihre Melder selbst testen möchten, müssen Sie hierzu in der **Alarmkonfiguration** in den Menüpunkt **System** wechseln. Hier finden Sie den **Gehtest**. Um diesen starten zu können, müssen Sie davor den **Wartungsmodus** aktivieren, welcher sich im gleichen Menü finden lässt. Nach dem anschließendem Starten des **Gehtests** können Sie durch Auslösen der Melder feststellen, ob diese in Funktion sind.

- Wie gehe ich bei einem Batteriewechsel vor?

Grundsätzlich empfehlen wir eine jährliche Wartung samt Batteriewechsel der Komponenten durch eine Fachfirma. Wenn Sie die Batterien in den Funkkomponenten selbst wechseln möchten, müssen Sie die Anlage zuerst in den **Wartungsmodus** schalten, dass Sie beim Öffnen der Komponente keine Sabotage auslösen. Betreten Sie hierzu in der **Alarmkonfiguration** den Punkt **System** und setzen den Haken beim Punkt **Wartungsmodus**. Anschließend können Sie die Batterien Ihrer Komponenten wechseln. Beachten Sie hierzu die jeweiligen Anleitungen der Produkte.

- Was sind reversible Zustände?

Ein reversibler Zustand beschreibt eine im Alarmfall ausgeführte Aktion, welche nach Rückstellen des Alarms wieder in den Ursprungszustand zurück geht. So können Sie beispielsweise bei einem Feueralarm alle Lichter anschalten, sowie alle Rollläden hochfahren lassen. Nachdem der Alarm quittiert wurde, gehen die Geräte wieder in den zuvorigen Zustand.

- Was ist der Unterschied zwischen S0, S2 (ohne DSK) und S2 (mit SDK)?

Der Unterschied in den verschiedenen Inklusionsarten liegt in der Verschlüsslung beim Einlernprozess und damit in der Sicherheit der Funk-Kommunikation zwischen Anlage und Komponente. Z-Wave-Geräte haben unterschiedliche verfügbare Sicherheitsklassen, welche bei der Inklusion frei auswählbar sind. Wir empfehlen, immer die höchst-verfügbare Sicherheitsklasse zu wählen. Bei einer „unsicheren“ Inklusion ist die Verbindung unverschlüsselt. Wir raten dringendst davon ab, das Gerät so zu nutzen.

- Warum muss ich meinen Browser immer wieder neu verifizieren?

Als erstes sollten Sie darauf achten, nur die Empfohlenen Browser zu nutzen. Aktuell sind diese der Edge oder Chrome. Wenn bei einem dieser Browser das Verhalten auftritt, prüfen Sie die Browsereinstellungen. Wenn hier beim Schließen des Browsers die Cookies und/oder der Cache gelöscht wird, ändert sich die Browser ID beim nächsten Start, wodurch eine neue Verifizierung notwendig wird.

- Kann ich die Nexello ohne Akku betreiben?

Grundsätzlich können wir von einem dauerhaften Betrieb der Nexello ohne Akku nur abraten. Zur kurzzeitigen Überbrückung gibt es die Möglichkeit, zwei PINs an den Audioboard mithilfe eines Jumpers zu brücken, wodurch die Anlage auch ohne angeschlossenen Akku funktioniert. Eine Anleitung hierzu finden Sie auf der Produktseite der Nexello unter www.abus.com.

22.9. E-Mail Provider – Liste

Gmail (ehem. Google Mail)

Postausgangsserver:

smtp.gmail.com (SSL; Port 465 oder 587)

Benutzername:

Benutzername@gmail.com

Besonderheiten:

Sie müssen in Ihrem Account den POP3- und SMTP-Zugriff zunächst aktivieren. („weniger sichere Apps zulassen) -> separate Anleitung vorhanden

GMX

Postausgangsserver:

mail.gmx.net (bei SSL Port 465)

Benutzername:

GMX-Kundennummer oder GMX-E-Mail-Adresse

Besonderheiten:

SMTP steht auch über den alternativen Port 587 zur Verfügung.

Sollte es beim Anmelden Probleme geben, sollten Sie in jedem Fall beide Möglichkeiten für den Benutzernamen ausprobieren

POP3- und IMAP-Zugriff müssen erst in den Postfach-Einstellungen freigeschaltet werden. -> separate Anleitung vorhanden

mail.de

Postausgangsserver:

smtp.mail.de (SSL; Port 587)

Benutzername:

Benutzername@mail.de

Besonderheiten:

Verwendet SMTP-Authentifizierung.

POP3, IMAP und SMTP laufen über TLS- bzw. SSL-Verschlüsselung.

Outlook.com (ehemals Windows Live Hotmail)

Postausgangsserver:

smtp.office365.com (STARTTLS; Port 587)

Benutzername:

Vollständige Outlook.com-E-Mail-Adresse

Besonderheiten:

Verwendet SMTP-Authentifizierung.

POP3, IMAP und SMTP laufen über TLS- bzw. SSL-Verschlüsselung.

WEB.DE FreeMail

Postausgangsserver:

smtp.web.de (bei STARTTLS Port 587)

Benutzername:

Benutzername

Besonderheiten:

Verwendet SMTP-Authentifizierung.

POP3- und IMAP-Zugriff müssen erst in den Postfach-Einstellungen freigeschaltet werden. -> Anleitung vorhanden

Yahoo! Mail (gilt für Yahoo! Deutschland)

Postausgangsserver:

smtp.mail.yahoo.com (SSL; Port 465)

Benutzername:

Benutzername

Besonderheiten:

Verwendet SMTP-Authentifizierung.

Sie müssen in Ihrem Account den POP3- und SMTP-Zugriff zunächst aktivieren.

Diese Daten gelten für die deutsche Version von Yahoo! Mail. In anderen Ländern ist es unter Umständen nicht möglich, POP3 und SMTP kostenlos zu nutzen.

T-Online

Postausgangsserver:

securesmtp.t-online.de (SSL; Port 465)

Benutzername:

E-Mail-Adresse

Besonderheiten:

Verwendet SMTP-Authentifizierung.

POP3, IMAP und SMTP laufen über SSL-Verschlüsselung.

Das E-Mail-Passwort ist nicht identisch mit dem Passwort, das Sie bspw. für den Zugriff auf das Kundencenter und andere Web-Dienste verwenden.

Grundsätzlich ist jeder Provider mit SMTP-Versand mit der Nexello „kompatibel“ – bei nicht getesteten Providern können Probleme auftreten. Eine öffentliche E-Mail-Liste finden Sie unter https://www.patrick-canterino.de/pop3-smtp/. Die hier angegebenen Daten wurden von uns nicht auf ihre Richtigkeit überprüft. ABUS übernimmt für falsche Angaben keine Gewähr.