TELENOT
Technik für Sicherheit

ALARMANLAGEN-APP

BuildSec 4.0

Hersteller/Inverkehrbringer

TELENOT ELECTRONIC GMBH
Wiesentalstraße 60
73434 Aalen
GERMANY

Telefon +49 7361 946-0
Telefax +49 7361 946-440
info@telenot.de
www.telenot.de

Original Technische Beschreibung deutsch

1 Inhaltsverzeichnis

2 Allgemein

Alarmanlagen-App BuildSec 4.0
Building Security

Die Alarmanlagen-App BuildSec 4.0 ist eine Anwendersoftware für Smartphones und Tablets, die ein Bedienteil der Einbruchmelderzentrale (EMZ) in vollem Funktionsumfang nachbildet.

Die Alarmanlagen-App BuildSec ist kompatibel zu folgenden Einbruchmelderzentralen:

- hiplex 8x00H
- complex 200H/400H in Verbindung mit einer Übertragungseinrichtung der Serie comXline
- compact easy 200H in Verbindung mit der eingebauten Übertragungseinrichtung comXline 2516 GSM easy

BuildSec 4.0 benötigt eine TCP/IP-Verbindung vom Smartphone / Tablet zur Einbruchmelderzentrale. Diese Verbindung kann auf 2 unterschiedliche Arten hergestellt werden:

- Direkte TCP/IP-Verbindung über Mobilfunk-IP oder WLAN
  (Ankommende Verbindung an der EMZ)
- TCP/IP-Verbindung über den hiXserver
  (stehende Verbindung zwischen EMZ und hiXserver)

Funktion

- Scharf-/Unscharfschaltung aller Sicherungsbereiche
- Ansicht offener Meldepunkte
- Alarmmeldungen im Klartext
- Abschalten/Sperren von Meldebereichen
- Steuern von Schaltfunktionen
- Ansicht des Ereignisspeichers
- Berechtigungen sperren

2.2 Systemvoraussetzungen

2.2.1 complex / compact easy

Smartphone / Tablet	ab iOS 9 (iPhone), Android 5.0
comXline 1516/2516/3516	ab Version 11.41
complex 200H/400H	ab Version 23.53
compasX	ab Version 20.0

2.2.2 hiplex

Smartphone / Tablet	iOS 9 (iPhone), Android 5.0
hiplex 8400H	Version F03

2.1 Sprachen

- **Angezeigte Meldungen** / Frei parametrierbare LEDs / Schaltfunktionen
  Frei parametrierbare Texte werden über die Parametriersoftware compasX oder hipas in der EMZ in der gewünschten Sprache eingegeben.
- **BuildSec-Menü**
  Die Sprache orientiert sich an der Spracheinstellung des Smartphones.
- **Display-Anzeige des virtuellen Bedienteils**
  Die Sprache für das Bedienteil muss in der Parametriersoftware compasX oder hipas eingestellt werden. (Details finden Sie in der Hilfe der jeweiligen Parametriersoftware).

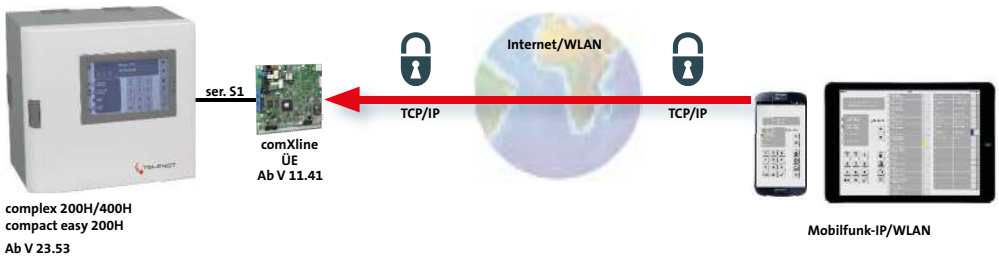
Mögliche Sprachen

- Deutsch
- Englisch
- Französisch
- Niederländisch

2.3 Direkte Verbindung

Ankommende Verbindung an der EMZ

complex / compact easy



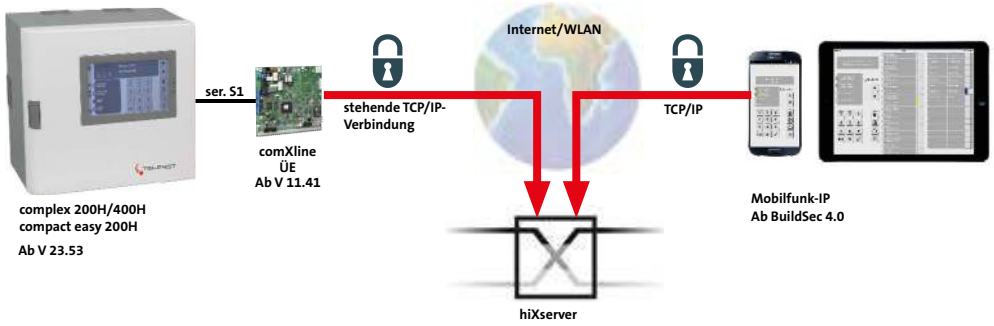
hiplex

Diese Verbindungsart von BuildSec 4.0 ist nicht zum Einsatz an einem IPv6-Anschluss mit DualStackLite (DSLite) geeignet.

2.4 Verbindung über hiXserver

Stehende Verbindung zwischen Übertragungseinrichtung und hiXserver.

complex / compact easy



Diese Verbindungsart von BuildSec 4.0 ist durch die stehende Verbindung (keine ankommende IPv4-Verbindung) zum Einsatz an einem IPv6-Anschluss mit DualStackLite (DSLite) geeignet.

2.5 Voraussetzungen für eine direkte Verbindung

Bei einer direkten Verbindung muss der IP-Fernzugang auf die Übertragungseinrichtung (complex / compact easy) oder auf die hiplex eingerichtet werden.

IP-Fernzugang zur ÜE

Die Erreichbarkeit wird zum Fernschalten, Fernabfragen und zur Fernparametrierung benötigt. Für die Erreichbarkeit ist die Parametrierung in compasX im Menü Fernzugang „freigegeben (für alle)“ und die Parametrierung/Beschaltung des Eingangs „AR-AUS“ in der ÜE entscheidend.

IP-Fernzugang zur hiplex

Die Erreichbarkeit wird zum Fernabfragen und zur Fernparametrierung benötigt. Für die Erreichbarkeit ist die Parametrierung der Ethernet-Schnittstelle der hiplex und des Routers in hipas entscheidend. Dazu muss in Topologie-Ansicht der hiplex-Platine an der Ethernet-Schnittstelle ein Router hinzugefügt werden und die interne IP-Verbindung zwischen Router und hiplex (lokale IP-Adresse / Hostname, lokaler Port, Standardgateway usw.) parametriert werden. Zudem muss der IP-Fernzugang auf den Router (Externe IP-Adresse / Domainname, externer Port) parametriert werden.

Beim Fernzugang wird der AES-Schlüssel überprüft und erst bei Übereinstimmung wird der Anruf entgegengenommen.

Für den Fernzugang ist die IP-Adresse der Übertragungseinrichtung oder der hiplex, die sowohl statisch als auch dynamisch sein kann, notwendig.

Voraussetzung für den Fernzugang mit dynamischer IP-Adresse:

Beantragen Sie einen Hostname bei einen DynDNS*-Anbieter. Es werden in der Regel folgende Angaben für die Anmeldung für den DynDNS-Dienst benötigt:

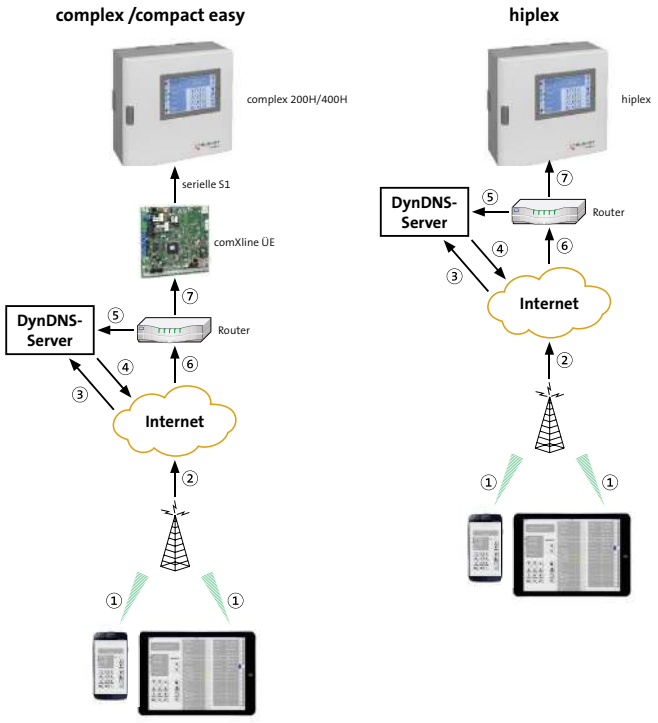
- USERNAME
- HOSTNAME
- PASSWORT
- E-MAIL-ADRESSE

Der „Username“ und die „E-Mail-Adresse“ werden benötigt, um sich auf der Webseite des DynDNS-Anbieters einloggen zu können.

Der „Hostname“ wird benötigt, um von außen über den DynDNS-Server auf die ÜE / hiplex zugreifen zu können. Hinter dem Hostname verbirgt sich die aktuelle IP-Adresse des Internetanschlusses der ÜE. Da sich die IP-Adresse im Normalfall bei einem Anschluss mit dynamischer IP-Adresse alle 24 Stunden ändert, wird der Hostname verwendet, um den Anschluss zu erreichen.

* DynDNS steht für Dynamic Domain Name System.

DynDNS stellt sicher, dass die ÜE mit dynamischen IP-Adressen immer über den selben Namen (Hostname) erreichbar ist.



① Mobilfunk-IP-Verbindung

② Netzübergang Mobiles Netz zum Internet

③ Übertragung des Hostnamens zum DynDNS-Server

④ Antwort des DynDNS-Servers mit der passenden IP-Adresse zum Hostnamen

⑤ Regelmäßiger Abgleich des Hostnamens mit der dynamischen IP-Adresse des Routers

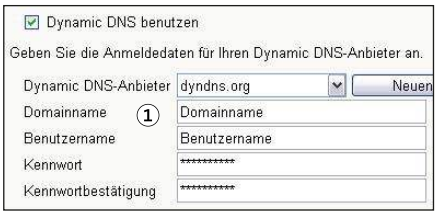
⑥ Ankommende Daten mit der korrekten IP-Adresse des Routers

⑦ Übertragung der Daten über Ethernet vom Router zum comXline ÜE oder zur hiplex

IP-Fernzugang zur ÜE / hiplex am Router einrichten

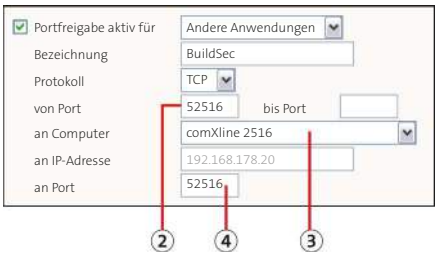
Freigabe DynDNS im Router (z. B. Fritz Box)

- Erweiterte Einstellungen
- Internet
- Freigaben
- DynDNS (z. B. Dyndns.org)



Portfreigabe im Router

- Erweiterte Einstellungen
- Internet
- Freigaben
- Portfreigabe



① Hostname (Domainname)

② Portfreigabe von IP-Port öffentlich

③ Hostname (im LAN)

④ Portfreigabe an Port (eingehende Verbindung)

2.6 Voraussetzungen für die Verbindung über hiXserver

Voraussetzungen von BuildSec 4.0

- Der Zugang zum hiXserver ist ab der BuildSec 4.0 möglich.
- Einmalige Registrierung des Nutzergeräts beim hiXserver. (Siehe „Neues Objekt: hiXsever (Betreibermodus)“).

Voraussetzungen der EMZ

- Internetverbindung (IPv4 oder IPv6)
- Einmalige Registrierung beim hiXserver
- Aktivierte Service-Lizenz hiXmobile

Hintergründe

Bei der Verbindung über den hiXserver muss, im Gegensatz zur direkten Verbindung, kein IP-Fernzugang auf die Übertragungseinrichtung (complex / compact easy) oder auf die hiplex eingerichtet werden.
Ein DynDNS-Dienst wird deshalb nicht benötigt.
In diesem Fall muss nur eine abgehende Verbindung von der Übertragungseinrichtung (complex / compact easy) oder von der hiplex zum hiXserver parametriert werden. Da es sich hierbei um eine stehende Verbindung handelt, kann per BuildSec 4.0-App auf den hiXserver zugegriffen werden, welcher dann die stehende Verbindung zur Übertragungseinrichtung oder hiplex „durchschaltet“.

Um den Zugang zum hiXserver nutzen zu können, müssen Sie sich als Errichter beim hiXserver-Portal registrieren und ein Lizenzpaket erwerben (Details zu den unterschiedlichen Lizenzpaketen finden Sie im Shop von TELENOT Smart Services).
Zum Betrieb von BuildSec 4.0 muss ein Objekt im hiXserver-Portal angelegt werden und eine Lizenz (hiXmobile) für dieses Objekt aktiviert werden. Zudem muss ein Nutzer von BuildSec 4.0 beim hiXserver registriert werden.

Details zu den unterschiedlichen Services finden Sie im Shop von TELENOT Smart Services.
Details zur Objektverwaltung und Servicefreigabe finden Sie in der Hilfe im hiXserver-Portal.

3 BuildSec 4.0-Download

3.1 BuildSec 4.0 (iPhone, iPad)

Der Download der BuildSec 4.0 Applikationen wird über das Smartphone/Tablet im App Store durch den Betreiber bzw. nach Absprache durch den Errichter durchgeführt.

- Suchen Sie im App Store nach „Alarmanlagen-App BuildSec 4.0“ oder „TELENOT“.
- Installieren Sie die BuildSec 4.0 Applikation.

3.2 BuildSec 4.0 (Android)

Der Download der BuildSec 4.0 wird über das Smartphone/Tablet im Google Play Store durch den Betreiber oder nach Absprache durch den Errichter durchgeführt.

- Suchen Sie im Google Play Store nach „Alarmanlagen-App BuildSec 4.0“ oder „TELENOT“.
- Installieren Sie die BuildSec 4.0 Applikation.

4 BuildSec 4.0-Betriebsmodus

4.1 Errichtermodus

Der Errichtermodus von BuildSec 4.0 bietet dem Errichter die Möglichkeit, die App kostenfrei dem Betreiber vorzustellen. Zudem kann der Errichter im Errichtermodus eine Wartung durchführen. Allerdings muss in diesem Fall der Betreiber zuvor im Bedienteil- menü der Einbruchmelderzentrale die App-Freigabe erteilen.
Die Objektliste im Errichtermodus unterscheidet sich von der Objektliste im Betreibermodus.

Für den Errichtermodus ist kein Freischaltcode erforderlich.

4.2 Betreibermodus

Der Betreibermodus ist kostenpflichtig und erfordert eine Freischaltung der App per Freischaltcode. Der Freischaltcode kann im Online-Shop von TELENOT erworben werden.

Für den Betreibermodus ist zwingend ein Freischaltcode erforderlich.

5 Betreibermodus

5.1 Freischaltcode erwerben (TELENOT-Shop)

Für den Betreibermodus ist zwingend ein Freischaltcode erforderlich.

1. Führen Sie im TELENOT-Shop eine App-Aktivierung durch. Dazu müssen Sie die Alarmanlagen-App BuildSec 4.0 in den Warenkorb legen (Einkaufswagen-Symbol / „Hinzufügen“ Schaltfläche).

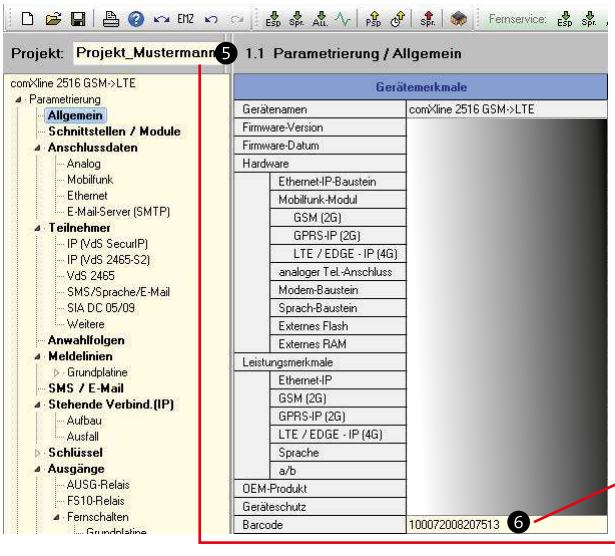
Aus technischen Gründen kann eine App-Aktivierung nur durchgeführt werden, wenn sich keine anderen Artikel im Warenkorb befinden. Zudem darf die BuildSec 4.0 nur 1-mal in den Warenkorb gelegt werden.

2. Öffnen Sie den Warenkorb.
3. Klicken Sie auf „Zur Bestellung“.

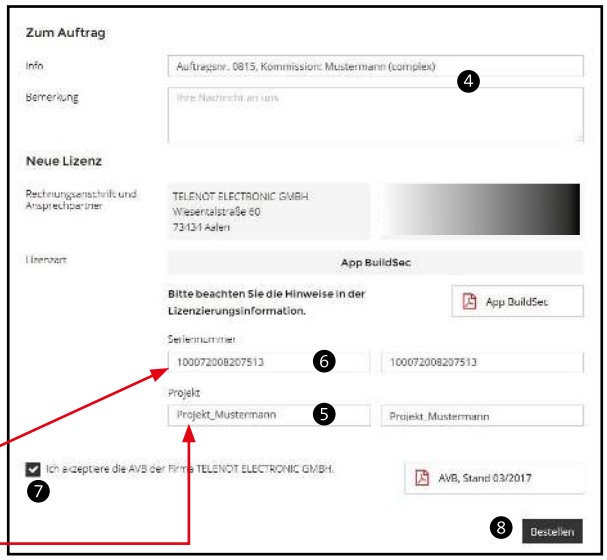
Anschließend wird das Formular zur Aktivierung der BuildSec 4.0 geöffnet.
Abhängig vom Typ der Einbruchmelderzentrale (complex / hiplex) müssen Sie unterschiedliche Daten eingeben:

5.1.1 Einbruchmelderzentralen complex-Serie

compasX: ÜE-Parametrierung



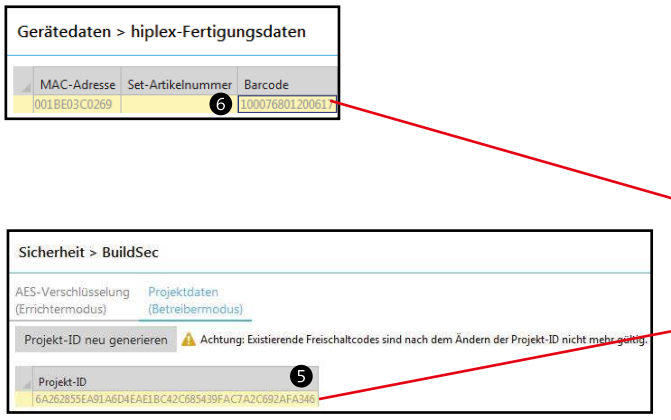
Formular: Warenkorb BuildSec



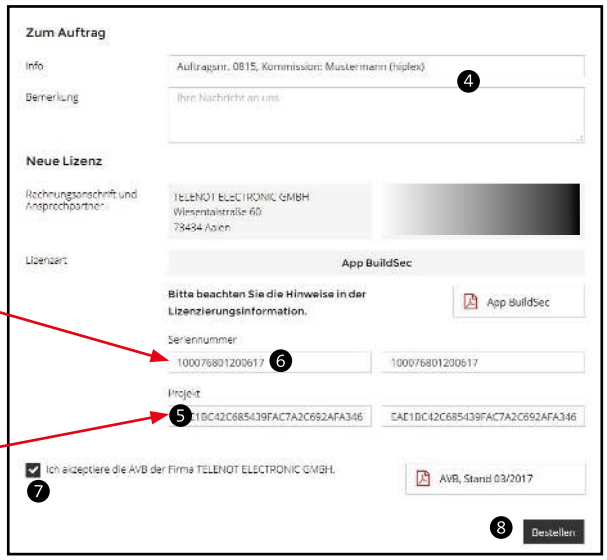
4. Tragen Sie die Informationen zur Identifizierung des Objekts (z. B. Auftragsnummer, Kommission) in das Formular ein.
5. Tragen Sie den Projektnamen aus der ÜE-Parametrierung (compasX) in das Formular ein.
Stellen Sie sicher, dass die Schreibweise des Projektnamens absolut identisch ist (Klein-, Großbuchstaben, Umlaute, Leerzeichen usw.), da der Projektname eine Variable bei der Erstellung des Freischaltcodes ist.
Wiederholen Sie die Eingabe im zweiten Feld („Bitte wiederholen“).
6. Tragen Sie den Barcode (Seriennummer) der Übertragungseinrichtung in das Formular unter Seriennummer ein.
Wiederholen Sie die Eingabe im zweiten Feld („Bitte wiederholen“).
7. Akzeptieren Sie die „AVB der Firma TELENOT ELECTRONIC GMBH“.
8. Klicken Sie auf „Bestellen“.

5.1.2 Einbruchmelderzentralen hiplex-Serie

hipas: hiplex-Parametrierung



Formular: Warenkorb BuildSec



❹ Tragen Sie die Informationen zur Identifizierung des Objekts (z. B. Auftragsnummer, Kommission) in das Formular ein.

❺ Tragen Sie die Projekt-ID aus der hiplex-Parametrierung (hipas) in das Formular ein.
Da es sich um eine sehr lange hexadezimale Zahl handelt, empfiehlt TELENOT die Projekt-ID direkt aus der Parametriersoftware hipas zu kopieren (Copy + Paste), da die Projekt-ID eine Variable bei der Erstellung des Freischaltcodes ist.
Wiederholen Sie die Eingabe im zweiten Feld („Bitte wiederholen“).

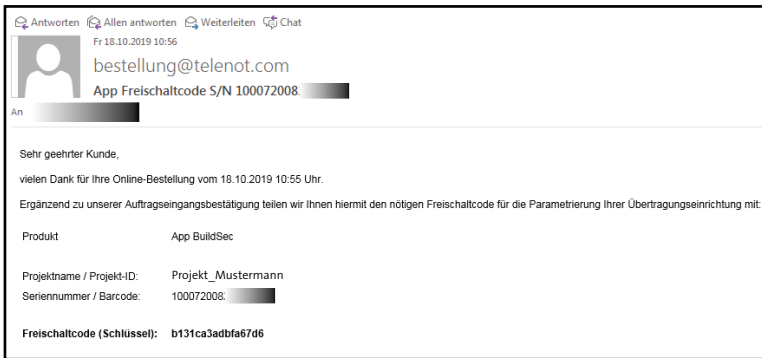
❻ Tragen Sie den **Barcode (Seriennummer) der hiplex-Platine** in das Formular unter Seriennummer ein.
Wiederholen Sie die Eingabe im zweiten Feld („Bitte wiederholen“).

❼ Akzeptieren Sie die „AVB der Firma TELENOT ELECTRONIC GMBH“.

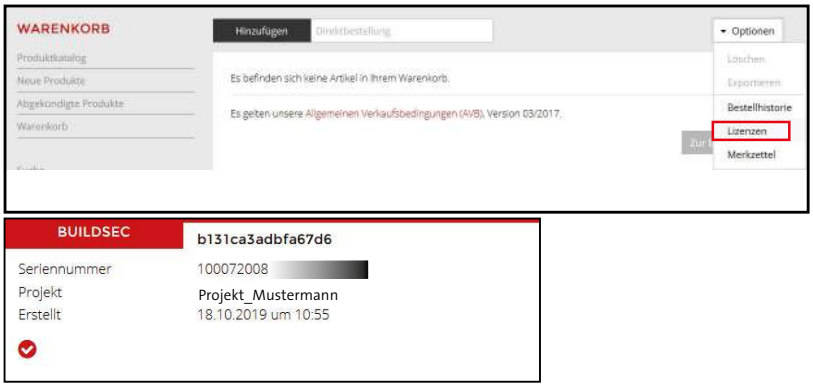
❽ Klicken Sie auf „Bestellen“.

5.2 Freischaltcode erhalten

Nach der Bestellung erhalten Sie eine E-Mail mit dem Freischaltcode.



Alternativ können Sie im TELENOT-Shop unter Warenkorb > Optionen > Lizenzen alle bisher erworbenen Lizenzen anschauen.

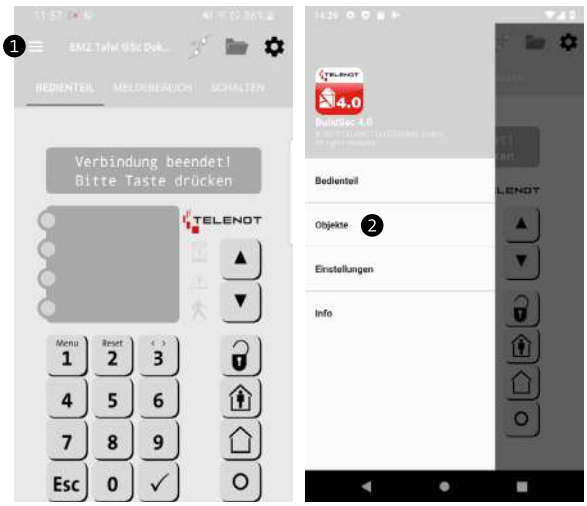


6 Objekte

Die Objekte werden im Errichtermodus und im Betreibermodus auf dieselbe Weise eingerichtet.

Die Anzahl der zu verwaltenden Objekte wird durch die Speicherkapazität des Smartphones/Tablets begrenzt. Objekte können jederzeit neu angelegt, bearbeitet und gelöscht werden.

6.1 Objektliste



① **Icon „hiXserver-Objekt“:** BuildSec verbindet sich über den hiXserver mit dem Objekt.
Grün hinterlegt: Aktive Verbindung zwischen Objekt und hiXserver

② **Icon „direkte Verbindung“:** BuildSec verbindet sich direkt mit dem Objekt.

③ Aktualisieren

④ Objektliste-Einstellungen

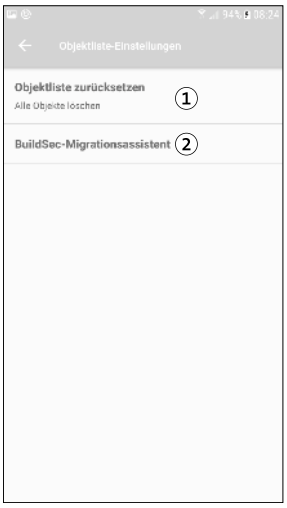
⑤ Neues Objekt anlegen

❶ Öffnen Sie mit dem Hamburger-Button das Hauptmenü.

❷ Klicken Sie auf „Objekte“, um die Objektliste zu öffnen.

Die Grafik zeigt die Objektliste auf einem Android-Smartphone. Auch alle anderen Menüpunkte werden in Android- und iOS-Smartphones identisch angezeigt. Bei der Bedienung unterscheiden sie sich minimal, da diese auf die jeweilige Standardbedienung des entsprechenden Betriebssystems angepasst ist.
Beispiel Unterschiede bei der Objektliste: Bei einem iOS-Phone (Apple) wird statt der 3-Punkt-Schaltfläche neben dem Objekt, im Menü der Text „Bearbeiten“ angezeigt. Zur Auswahl klicken Sie im iOS-Gerät zuerst auf „Bearbeiten“ und wählen anschließend das Objekt. Im Android-Gerät klicken Sie auf die 3-Punkt-Schaltfläche.

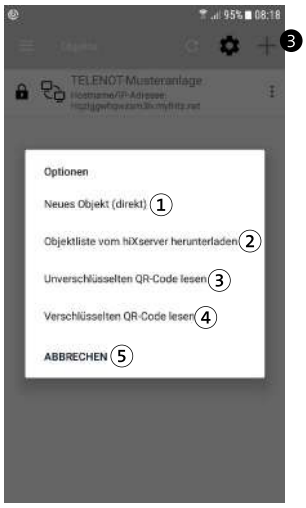
6.2 Objektliste-Einstellungen



① **Objektliste zurücksetzen:** Alle Objekte der Objektliste werden gelöscht.

② **BuildSec-Migrationsassistent:** Übernahme der Daten von BuildSec V 2.5 auf die aktuelle App-Version BuildSec 4.0.

6.3 Neues Objekt anlegen



① **Neues Objekt (direkt):** Neues Objekt mit direkter Verbindung anlegen.

② **Objektliste vom hiXserver herunterladen:** Ein neues Objekt mit Verbindung zum hiXserver muss auf dem hiXserver angelegt werden. Mit diesem Menüpunkt kann die Objektliste vom hiXserver heruntergeladen werden.

③ **Unverschlüsselten QR-Code lesen:** Neues Objekt mit Hilfe eines unverschlüsselten QR-Codes anlegen.
Anwendung: Übernahme von Objekten von einem Smartphone zu einem anderen Smartphone.

④ **Verschlüsselten QR-Code lesen:** Neues Objekt mit Hilfe eines verschlüsselten QR-Codes anlegen.
Anwendung: Übernahme von Objekten von einem Smartphone zu einem anderen Smartphone.
Zur Übernahme wird das Objektlisten-Passwort benötigt.

⑤ **Abbrechen:** „Neues Objekt anlegen“ abbrechen

❸ Über die Schaltfläche „+“ öffnen Sie das Menü, um ein neues Objekt hinzuzufügen.

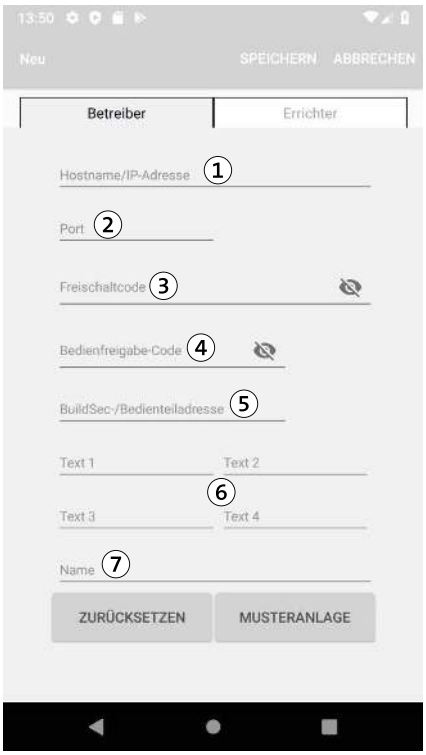
❹ Wählen Sie, welches Objekt Sie anlegen wollen (1) - (4), oder ob Sie abbrechen wollen (5).

Im Folgenden werden die unterschiedlichen Möglichkeiten detailliert beschrieben.

6.4 Neues Objekt: Direkte Verbindung (Betreibermodus)

6.4.1 complex / compact easy

- Tragen Sie folgende Daten in BuildSec ein:



① Statische IP-Adresse oder Hostname der ÜE (aus **compasX**: Parametrierung ÜE, Fernservice, Ethernet)

② IP-Port (öffentlich) der ÜE am Router (aus **compasX**: Parametrierung ÜE, Fernservice, Ethernet)

③ Freischaltcode: **Freischaltcode mit 16 Zeichen (aus E-Mail)**

④ Bedienfreigabe-Code mit „Freigegeben an BuildSec“ (aus **compasX**: Parametrierung complex 200H/400H, Bedien/Anzeigeteile, Touch-/LCD-BTs/Bedienfreigabe-Codes)
Falls dieses Feld leer ist, muss der Bedienfreigabe-Code vor jedem Verbindungsaufbau eingegeben werden.

⑤ Z. B. Bedienteiladresse 0 (oder jedes andere als Typ „BuildSec-App“ in **compasX** parametrierte Bedienteil der complex 200H/400H)

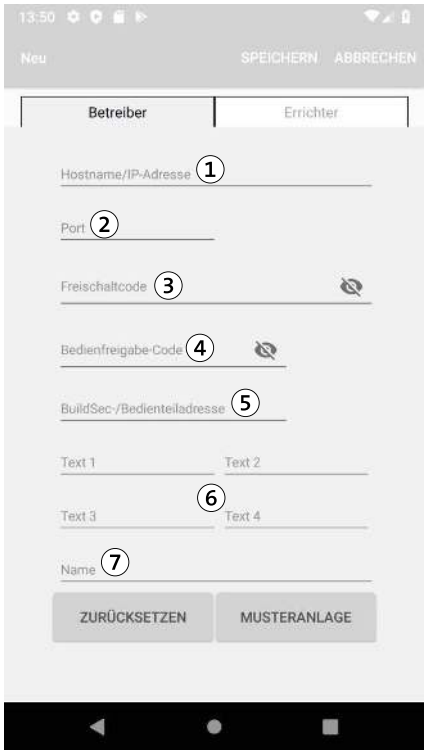
⑥ Text 1 bis 4 werden beim ersten Verbindungsaufbau einmalig, automatisch aus der EMZ (complex 200H/400H ab Firmware-version 23.53) von der oben angegebenen Bedienteiladresse empfangen.

⑦ Name: Name des Objekts (kundenspezifisch)

Detaillierte Informationen zu den einzelnen Parametern finden Sie in der **Hilfe der Parametriersoftware compasX**.

6.4.2 hiplex

- Tragen Sie folgende Daten in BuildSec ein:



① Externe IP-Adresse oder Hostname der hiplex (aus **hipas**: Topologie > Router > Router erreichbar über)

② Externer Port der hiplex am Router (aus **hipas**: Topologie > Router > Router erreichbar über)

③ Freischaltcode: **Freischaltcode mit 16 Zeichen (aus E-Mail)**

④ Codeberechtigung für BuildSec mit Reaktion „Freigegeben“ für unterschiedliche Berechtigungsvorgänge, wie z. B. „Anzeige und Menü“, Taste Unscharf, usw. (aus **hipas**: Personenverwaltung > Personenberechtigungen > Codeberechtigungen für BuildSec) **Falls dieses Feld leer ist, muss der Bedienfreigabe-Code vor jedem Verbindungsaufbau eingegeben werden.**

⑤ Z. B. Bedienteiladresse 0 (oder jedes andere als Typ „BuildSec“ in hipas parametrierte Bedienteil) (aus **hipas**: Topologie > Router > BuildSec (nur WLAN) > Komponentenadresse **oder** Topologie > Router > BuildSec (Internet und WLAN) > Komponentenadresse)

⑥ Text 1 bis 4 werden beim ersten Verbindungsaufbau einmalig, automatisch aus der EMZ von der oben angegebenen Bedienteiladresse empfangen.

⑦ Name: Name des Objekts (kundenspezifisch)

Detaillierte Informationen zu den einzelnen Parametern finden Sie in der **Hilfe der Parametriersoftware hipas**.

6.5 Neues Objekt: hiXserver (Betreibermodus)

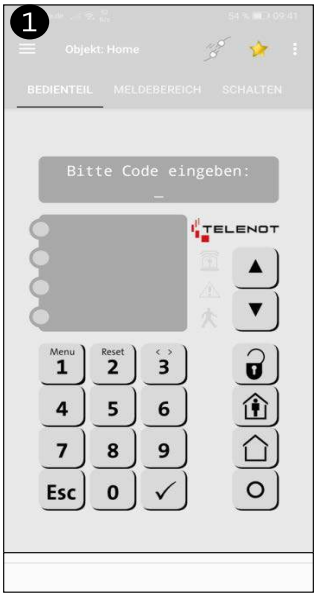
6.5.1 complex / compact easy

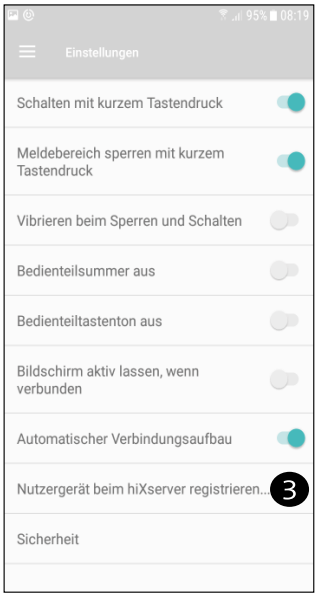
Voraussetzungen im hiXserver-Portal

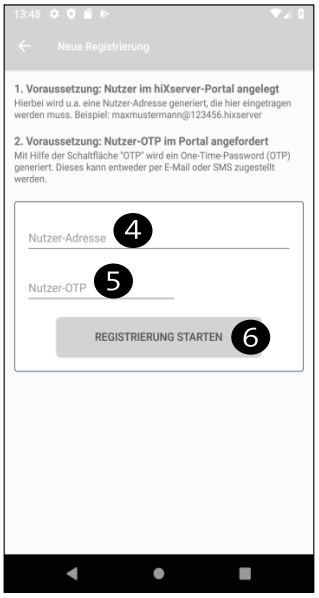
- Neuer Nutzer (Betreiber) ist angelegt.
- Dem Nutzer wurde die Fernzugangsberechtigung erteilt.
- Für den Nutzer wurde ein One-Time-Password (OTP) generiert (Gültigkeit 12 h).

Detaillierte Informationen zu den einzelnen Voraussetzungen aus dem hiXserver-Portal finden Sie in der Inbetriebnahme-Checkliste auf dem hiXserver-Portal.

Registrierung der BuildSec 4.0 beim hiXserver







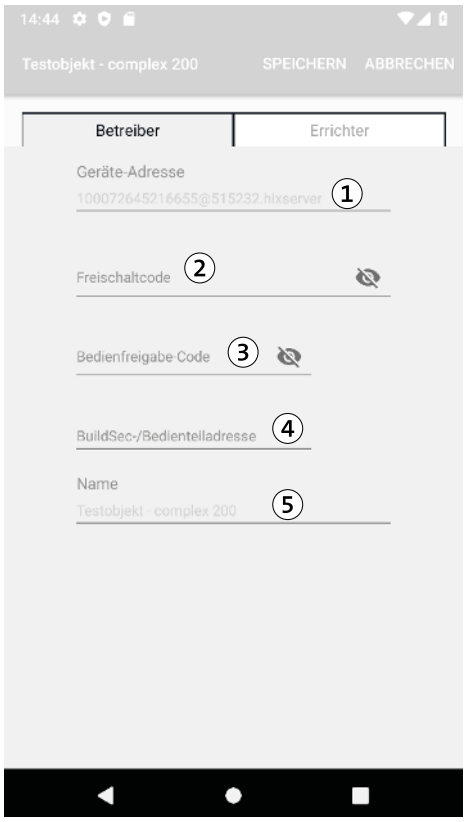
1. Öffnen Sie mit dem Hamburger-Button das Hauptmenü.
2. Klicken Sie auf „Einstellungen“.
3. Klicken Sie auf „Nutzergerät beim hiXserver registrieren“.
4. Tragen Sie die Nutzer-Adresse (aus hiXserver-Portal) ein: z. B. maxmustermann@123456.hixserver
5. Tragen Sie die Nutzer-OTP (aus hiXserver-Portal) ein.
6. Klicken Sie auf „Registrierung starten“. Anschließend wird die Objektliste vom hiXserver abgerufen.

Objekt grün hinterlegt: Aktive Verbindung zwischen Objekt und hiXserver. In der zweiten Zeile (Online seit...) wird angezeigt, seit wann diese Verbindung besteht.

Objekt rot hinterlegt: Die Verbindung zwischen Objekt und hiXserver wird aufgebaut.

7. Klicken Sie auf das gewünschte Objekt, um die Objektdaten einzutragen.

Objektdaten eintragen



Felder mit fehlenden Objektdaten sind rot hinterlegt.

① Geräte-Adresse der Übertragungseinrichtung (aus **hiXserver-Portal**: Objekte > Objektname > Einbruchmeldeanlagen)

② Freischaltcode: **Freischaltcode mit 16 Zeichen (aus E-Mail)**

③ Bedienfreigabe-Code mit „Freigegeben an BuildSec“ (aus **compasX**: Parametrierung complex 200H/400H, Bedien/Anzeigeteile, Touch-/LCD-BTs/Bedienfreigabe-Codes)
Falls dieses Feld leer ist, muss der Bedienfreigabe-Code vor jedem Verbindungsaufbau eingegeben werden.

④ Z. B. Bedienteiladresse 0 (oder jedes andere als Typ „BuildSec-App“ in **compasX** parametrierte Bedienteil der complex 200H/400H)

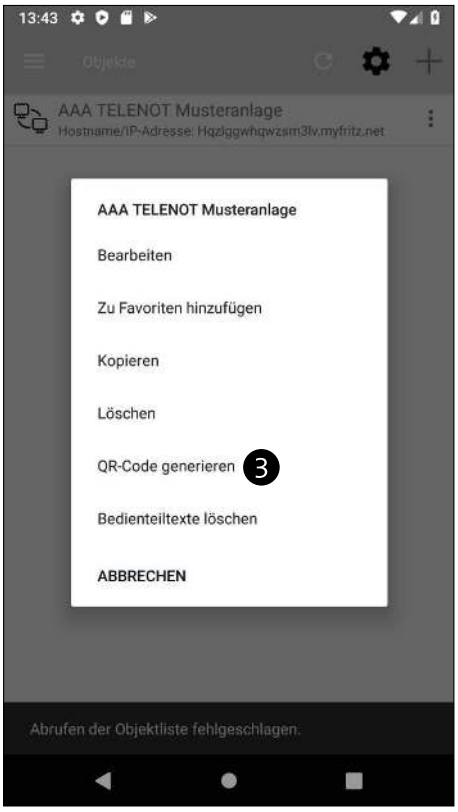
⑤ Name: Objektname (aus **hiXserver-Portal**: Objekte > Objektname)

Detaillierte Informationen zu den einzelnen Parametern finden Sie in der **Hilfe der Parametriersoftware compasX**.

6.6 Neues Objekt von anderem Smartphone / Tablet: Unverschlüsselten QR-Code lesen

Mit dieser Funktion können Sie auf einfache Art Objekte von einem Smartphone /Tablet auf ein anderes Smartphone / Tablet übertragen.

Um diese Funktion nutzen zu können, müssen Sie BuildSec 4.0 erlauben auf die Bilder und Videos zuzugreifen.



1. Öffnen Sie die Objektliste auf dem Smartphone / Tablet, von dem das Objekt übernommen werden soll (z. B. Hamburger Button > Objekte).
2. Öffnen Sie „Objekt bearbeiten“ (IOS: Bearbeiten, Android: 3-Punkte-Icon).
3. Klicken Sie auf „QR-Code generieren“.
4. Öffnen Sie die Objektliste auf dem Smartphone / Tablet, auf das das Objekt übertragen werden soll. Wählen Sie neues Objekt (+) und anschließend „Unverschlüsselten QR-Code lesen“.
   Anschließend wird der QR-Code automatisch gescannt und das neue Objekt angelegt.

6.7 Neues Objekt von anderem Smartphone / Tablet: Verschlüsselten QR-Code lesen

Mit dieser Funktion können Sie auf einfache Art verschlüsselte Objekte von einem Smartphone /Tablet auf ein anderes Smartphone / Tablet übertragen.

Um diese Funktion nutzen zu können, müssen Sie BuildSec 4.0 erlauben auf die Bilder und Videos zuzugreifen.

Der Ablauf enspricht dem zuvor geschilderten Ablauf „Neues Objekt von anderem Smartphone / Tablet: Unverschlüsselten QR-Code lesen“. Allerdings muss der Modus "Erweiterte Sicherheit" aktiviert sein und vor dem Lesen des QR-Codes das Passwort des anderen Gerätes eingegeben werden.

6.8 Objekt bearbeiten

① Objekt bearbeiten (siehe „Neues Objekt anlegen“)

② Objekt wird in der Objektliste als Favorit (gelber Stern) verwaltet.

③ Kopieren eines Objektes

④ Löschen eines Objektes

⑤ Generieren eines QR-Codes, um das Objekt mit allen Daten auf ein anderes Smartphone / Tablet zu kopieren.

⑥ Löschen der Bedienteiltexte (in BuildSec gespeicherte Bedienteiltexte werden gelöscht und beim nächsten Verbindungsaufbau wieder aus der EMZ geladen)

7 Errichtermodus

Der Errichtermodus dient zur:

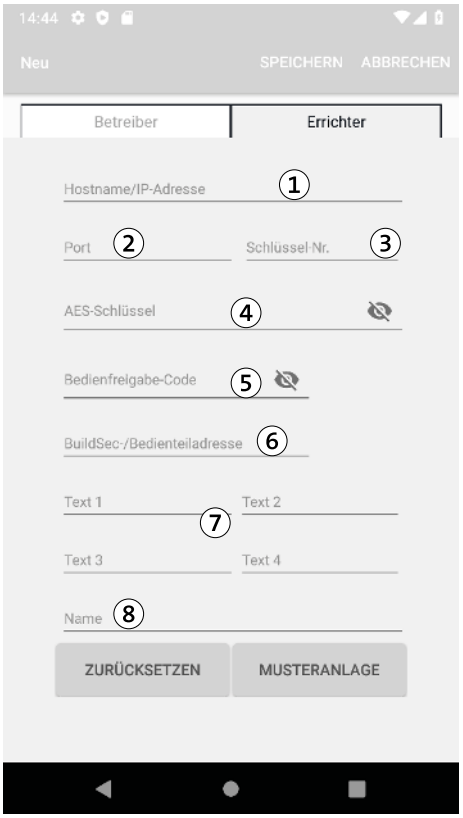
- Demonstration von BuildSec 4.0 beim Betreiber (Beratung/Verkauf)
- Durchführung der Bedienteil-Einmannrevision im Rahmen von Wartung und Service

Im Errichtermodus ist kein Freischaltcode notwendig. Der Betreiber muss allerdings den Zugang über das Bedienteil der EMZ freischalten. Der Zugang wird automatisch nach einer Stunde wieder gesperrt.

7.1 Neues Objekt: Direkte Verbindung (Errichtermodus)

7.1.1 complex / compact easy

- Tragen Sie folgende Daten in BuildSec ein:



① Statische IP-Adresse oder Hostname der ÜE (aus **compasX**: Parametrierung ÜE, Fernservice, Ethernet)

② IP-Port (öffentlich) der ÜE am Router (aus **compasX**: Parametrierung ÜE, Fernservice, Ethernet)

③ Schlüssel-Nr.: (aus **compasX**: Parametrierung ÜE, Fernservice, Ethernet, Schlüssel für sicheren Fernzugang)

④ AES-Schlüssel: (aus **compasX**: Parametrierung ÜE, Fernservice, Ethernet, Schlüssel für sicheren Fernzugang)

⑤ EMZ-Kennwort (Errichter): (aus **compasX**: Parametrierung EMZ Master, Schnittstellen)
Falls dieses Feld leer ist, muss der Bedienfreigabe-Code vor jedem Verbindungsaufbau eingegeben werden.

⑥ Z. B. Bedienteiladresse 0 (oder jedes andere als Typ „BuildSec-App“ in **compasX** parametrierte Bedienteil der complex 200H/400H)

⑦ Text 1 bis 4 werden beim ersten Verbindungsaufbau einmalig, automatisch aus der EMZ (complex 200H/400H ab Firmwareversion 23.53) von der oben angegebenen Bedienteiladresse empfangen.

⑧ Name: Name des Objekts (kundenspezifisch)

Detaillierte Informationen zu den einzelnen Parametern finden Sie in der **Hilfe der Parametriersoftware compasX**.

7.1.2 hiplex

- Tragen Sie folgende Daten in BuildSec ein:

① Externe IP-Adresse oder Hostname der hiplex (aus **hipas**: Topologie > Router > Router erreichbar über)

② Externer Port der hiplex am Router (aus **hipas**: Topologie > Router > Router erreichbar über)

③ Schlüssel-Nr.: (aus **hipas**: Sicherheit > BuildSec > AES-Verschlüsselung (Errichtermodus) > AES-Schlüsselnummer)

④ AES-Schlüssel: (aus **hipas**: Sicherheit > BuildSec > AES-Verschlüsselung (Errichtermodus) > AES-Schlüssel)

⑤ Codeberechtigung für BuildSec mit Reaktion „Freigegeben“ für unterschiedliche Berechtigungsvorgänge, wie z. B. „Anzeige und Menü“, Taste Unscharf, usw. (aus **hipas**: Personenverwaltung > Personenberechtigungen > Codeberechtigungen für BuildSec: Bedienprofil Errichter (Service))
Falls dieses Feld leer ist, muss der Bedienfreigabe-Code vor jedem Verbindungsaufbau eingegeben werden.

⑥ Z. B. Bedienteiladresse 0 (oder jedes andere als Typ „BuildSec“ in hipas parametrierte Bedienteil) (aus **hipas**: Topologie > Router > BuildSec (nur WLAN) > Komponentenadresse **oder** Topologie > Router > BuildSec (Internet und WLAN) > Komponentenadresse)

⑦ Text 1 bis 4 werden beim ersten Verbindungsaufbau einmalig, automatisch aus der EMZ von der oben angegebenen Bedienteil-adresse empfangen.

⑧ Name: Name des Objekts (kundenspezifisch)

Detaillierte Informationen zu den einzelnen Parametern finden Sie in der **Hilfe der Parametriersoftware hipas**.

7.2 Neues Objekt: hiXserver (Errichtermodus)

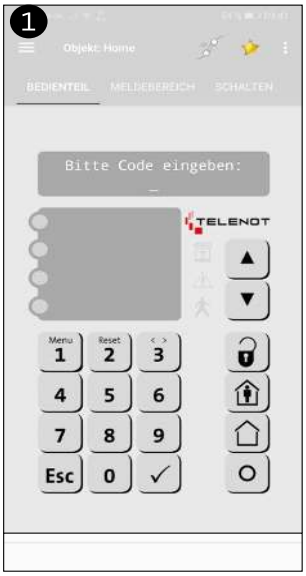
7.2.1 complex / compact easy

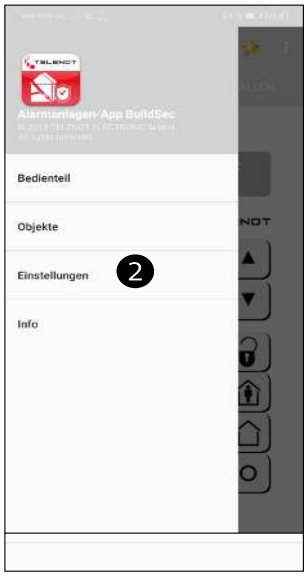
Voraussetzungen im hiXserver-Portal

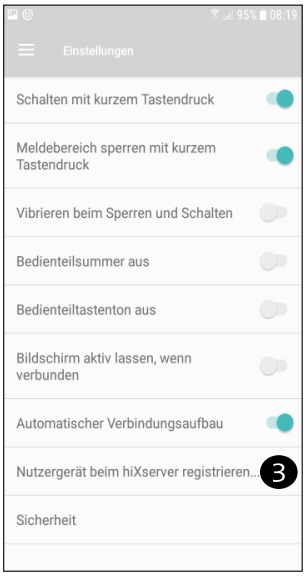
- Neuer Nutzer (Errichter) ist angelegt.
- Dem Nutzer wurde die Fernzugangsberechtigung erteilt.
- Für den Nutzer wurde ein One-Time-Password (OTP) generiert (Gültigkeit 15 min).

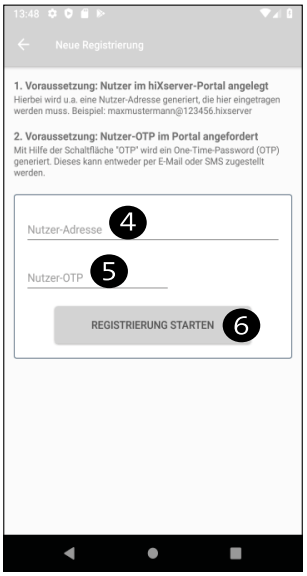
Detaillierte Informationen zu den einzelnen Voraussetzungen aus dem hiXserver-Portal finden Sie in der Inbetriebnahme-Checkliste auf dem hiXserver-Portal.

Registrierung der BuildSec 4.0 beim hiXserver









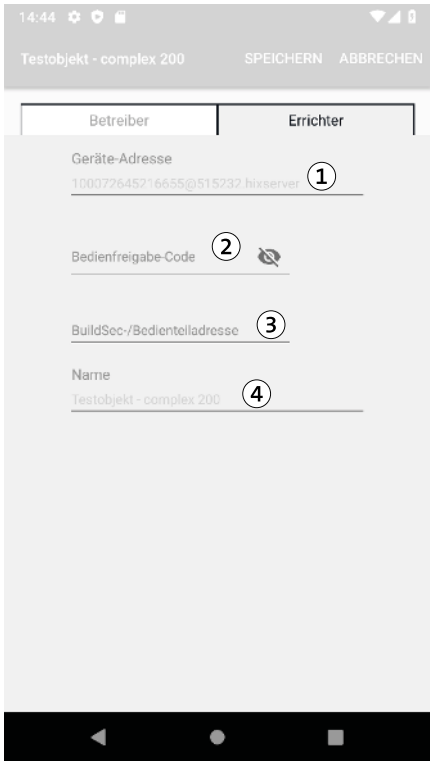
1. Öffnen Sie mit dem Hamburger-Button das Hauptmenü.
2. Klicken Sie auf „Einstellungen“.
3. Klicken Sie auf „Nutzergerät beim hiXserver registrieren“.
4. Tragen Sie die Nutzer-Adresse (aus hiXserver-Portal) ein: z. B. maxmustermann@123456.hixserver
5. Tragen Sie die Nutzer-OTP (aus hiXserver-Portal) ein.
6. Klicken Sie auf „Registrierung starten“. Anschließend wird die Objektliste vom hiXserver abgerufen.

Objekt grün hinterlegt: Aktive Verbindung zwischen Objekt und hiXserver. In der zweiten Zeile (Online seit...) wird angezeigt, seit wann diese Verbindung besteht.

Objekt rot hinterlegt: Die Verbindung zwischen Objekt und hiXserver wird aufgebaut.

7. Klicken Sie auf das gewünschte Objekt, um die Objektdaten einzutragen.

Objektdaten eintragen



Felder mit fehlenden Objektdaten sind rot hinterlegt.

① Geräte-Adresse der Übertragungseinrichtung (aus **hiXserver-Portal**: Objekte > Objektname > Einbruchmeldeanlagen)

② Bedienfreigabe-Code (Bedienfreigabe bis einschließlich Errichterebene) mit „Freigegeben an BuildSec“ (aus **compasX**: Parametrierung complex 200H/400H, Bedien/Anzeigeteile, Touch-/LCD-BTs/Bedienfreigabe-Codes)
Falls dieses Feld leer ist, muss der Bedienfreigabe-Code vor jedem Verbindungsaufbau eingegeben werden.

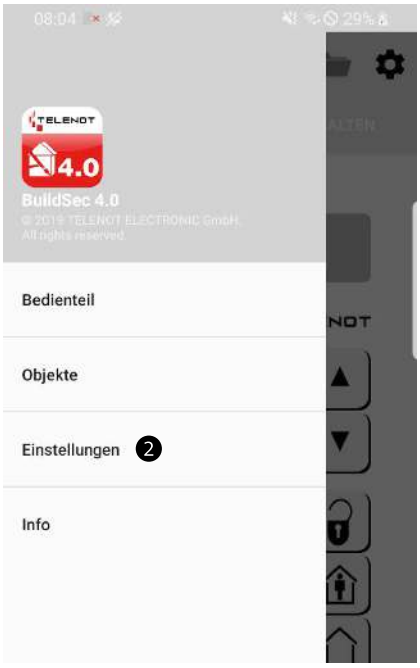
③ Z. B. Bedienteiladresse 0 (oder jedes andere als Typ „BuildSec-App“ in compasX parametrierte Bedienteil der complex 200H/400H)

④ Name: Objektname (aus hiXserver-Portal: Objekte > Objektname)

Detaillierte Informationen zu den einzelnen Parametern finden Sie in der Hilfe der Parametriersoftware compasX.

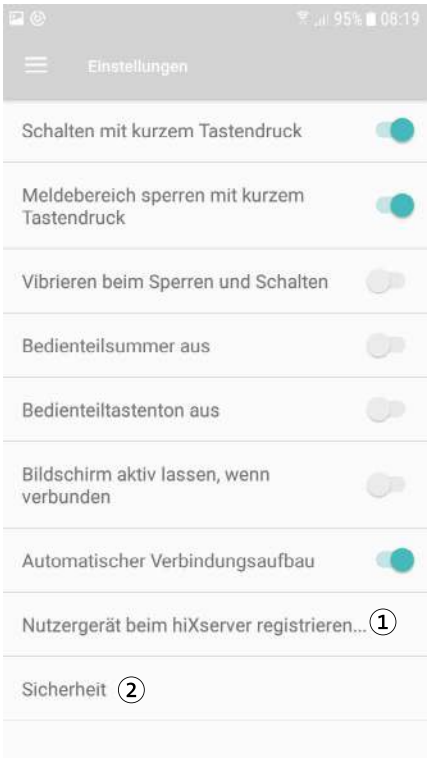
8 Einstellungen

❶ Öffnen Sie mit dem Hamburger-Button das Hauptmenü.



❷ Wählen Sie den Punkt „Einstellungen“ aus.

Menü Einstellungen



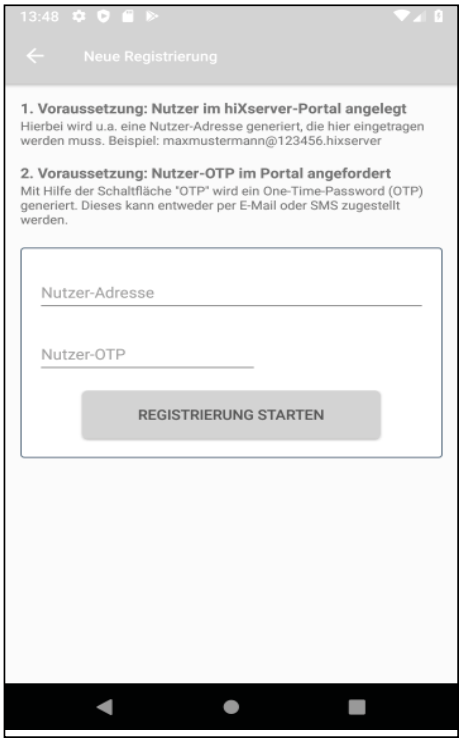
① hiXserver Nutzergeräte-Registrierung

② Menü zur Aktivierung der erweiterten Sicherheit

❸ Im Einstellungsmenü können Sie entsprechende Vorgaben für die Bedienung einstellen.

8.1 hiXserver Nutzergeräte-Registrierung

Anzeige vor der Nutzer-Registrierung

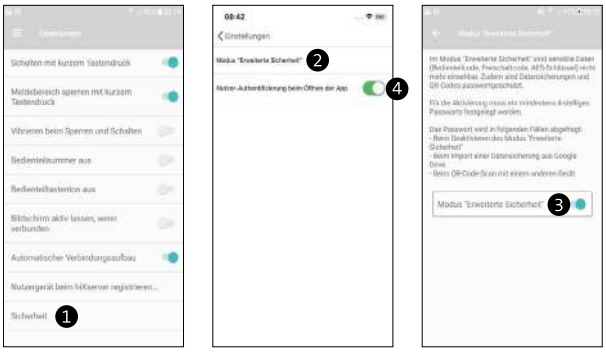


Anzeige nach erfolgreicher Nutzer-Registrierung

8.2 Erweiterte Sicherheit

In diesem Menü können Sie sensible Daten mit einem Passwort (mindestens 4 Stellen) verschlüsseln.
Diese Verschlüsselung bewirkt:

- Die sensiblen Daten (Bedienfreigabe-Codes, Freischaltschlüssel und AES-Schlüssel) sind nicht mehr einsehbar. Für das Einsehen der sensiblen Daten muss die Verschlüsselung deaktiviert werden (Passwort wird abgefragt).
- Beim Import einer verschlüsselten Datensicherung wird das Passwort abgefragt.
- Zum Anlegen eines neuen Objekts per QR-Code wird das Passwort abgefragt.



1. Klicken Sie im Menü „Einstellungen“ auf „Sicherheit“
2. Klicken Sie auf Modus „Erweiterte Sicherheit“, um in das Aktivierungsmenü zu gelangen.
3. Aktivieren Sie per Schieberegler den Modus „Erweiterte Sicherheit“.
4. Optional: Klicken Sie auf „Nutzer-Authentifizierung beim Öffnen der App“, um das Öffnen der App nur per Fingerprint oder Gesichtserkennung zuzulassen. (Nur bei IOS-Geräten möglich. Android in Vorbereitung)

9 Bedienung

9.1 Bedienung der App

① Der Hamburger-Button öffnet das Hauptmenü.

② Das Icon „Verbinden“ stellt eine Verbindung zum ausgewählten Objekt her.
Wenn die Verbindung hergestellt wurde, kann sie mit erneutem Tippen auf das Icon wieder getrennt werden.

③ Das Icon „Ordner“ öffnet die Objektauswahl.

④ Das Icon „Einstellungen“ öffnet das Einstellungsmenü (Das Einstellungsmenü kann auch über das Hauptmenü geöffnet werden.)

⑤ Über den Reiter „Bedienteil“ wird die Bildschirmseite LCD-Bedienteil (vgl. BT 800) angezeigt.

⑥ Über den Reiter „Meldebereich“ wird die Bildschirmseite Anzeigeteil (vgl. BT 800) angezeigt.

⑦ Über den Reiter „Schalten“ wird die Bildschirmseite Schaltfunktion/Schaltaktion (vgl. BT 800) angezeigt.

⑧ In der Display-Anzeige werden die Zustände der EMA (z. B. Scharfschaltzustände, ausgelöste Meldepunkte, Bedienteilmenüs usw.) angezeigt.

Möglichkeiten, um eine Verbindung zum Objekt herzustellen:

- Bei Anzeige des gewünschten Objektes: Doppelklicken Sie auf die Display-Anzeige des Bedienteils (8) oder tippen Sie auf das Icon „Verbinden“ (2).
- Tippen Sie auf das Objekt in der Objektverwaltung.
- Bei Neustart der App wird automatisch eine Verbindung zum zuletzt ausgewälten Objekt hergestellt.

Möglichkeiten, um eine Verbindung zu beenden:

- Doppelklicken Sie auf die Display-Anzeige des Bedienteils (8).
- Tippen Sie auf das Icon „Verbinden“ (2).

9.2 Bedienung der EMZ

Die Navigation zwischen den einzelnen Reitern funktioniert über Wischen oder Antippen des jeweiligen Reiters.

Bedienteil-Reiter

① Menü: Zugang zum Betreiber- bzw. Errichtermenü

② Reset: Alarme rücksetzen

③ Pfeiltasten (rechts / links): Auswahl im Menü

④ Esc: Menü verlassen

⑤ Enter-Taste

⑥ Auf-, Abwärtsblättern im Menü

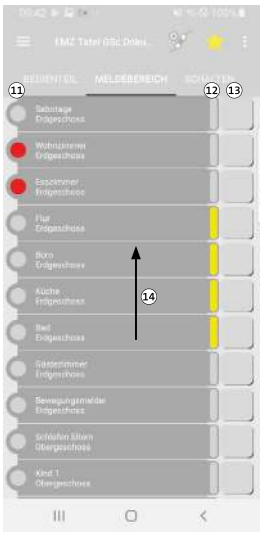
⑦ Unscharf schalten

⑧ Intern scharf schalten

⑨ Extern scharf schalten

⑩ Frei parametrierbar (z. B. Überfall)

Meldebereich-Reiter



⑪ Anzeige: Meldebereich ausgelöst (rot)

⑫ Anzeige: Meldebereich gesperrt (gelb)

⑬ Meldebereiche sperren / freigeben (langer Tastendruck)

⑭ Über Wischen werden weitere Meldebereiche angezeigt.

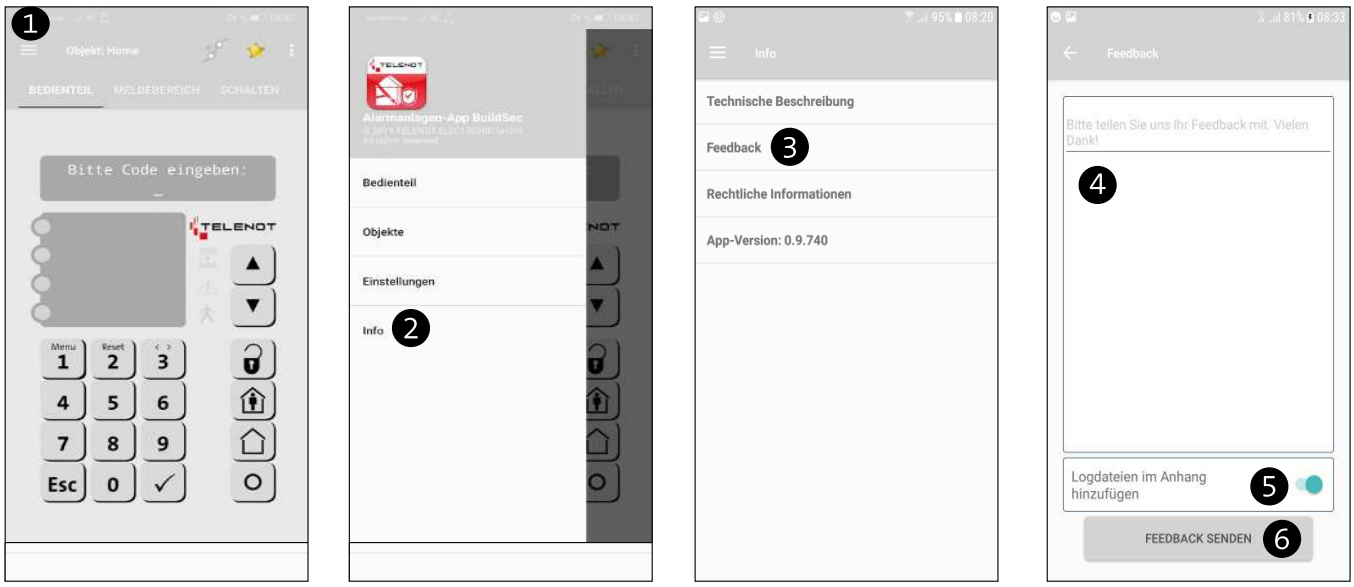
Schalten-Reiter

⑮ Schaltfunktion / Schaltaktion ein- bzw. ausschalten

Schaltfunktionen / Schaltaktionen können mit Codes ab Bedienebene 2 ausgelöst werden.

9.3 Feedback

Über das Menü „Feedback“ haben Sie die Möglichkeit eine E-Mail über BuildSec 4.0 direkt an TELENOT zu senden. An diese E-Mail können die Log-Dateien angehängt werden, um z. B. bei Problemen dem Service von TELENOT detaillierte Informationen zur Verfügung zu stellen. Voraussetzung für das Senden des Feedbacks ist ein aktiver E-Mail-Account auf dem Smartphone/Tablet.



1. Öffnen Sie mit dem Hamburger-Button das Hauptmenü.
2. Klicken Sie auf „Info“.
3. Klicken Sie auf „Feedback“.
4. Schreiben Sie Ihr Feedback in das Textfeld.
5. Bei Bedarf können Sie die Logdateien für den TELENOT-Service in den Anhang der E-Mail hinzufügen.
6. Klicken Sie auf „Feedback senden“. Anschließend wird die E-Mail-App geöffnet. Die E-Mail-Adresse „buildsecfeedback@telenot.de“ ist bereits eingetragen.