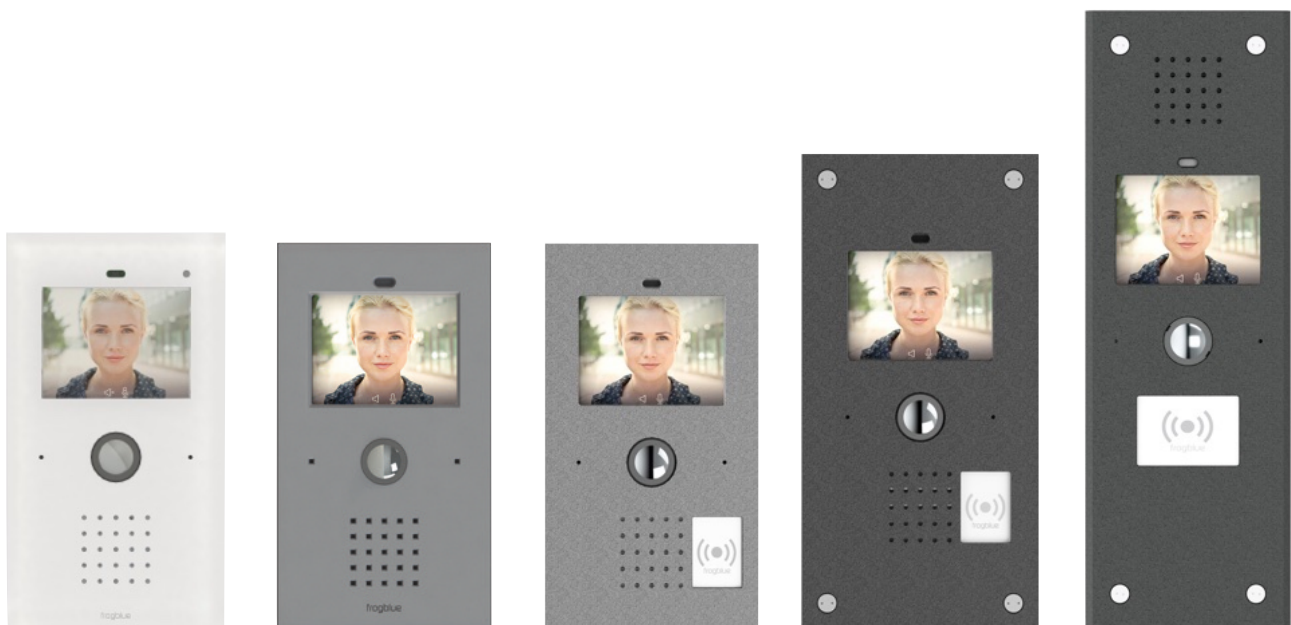


## frogTerminal Installationshandbuch

### Funktionsübersicht und technische Beschreibung

Das frogTerminal ist eine SIP-Video-Gegensprechanlage mit Multi-Faktor-Authentifizierung, dezentraler RFID-Zutrittskontrolle und Bluetooth/IP-Automatisierung. Es unterstützt direkte SIP-Anrufe, Multi-Server-Registrierung, Echtzeit-Sicherheitswarnungen und VMS/SIP-Integration von Drittanbietern.



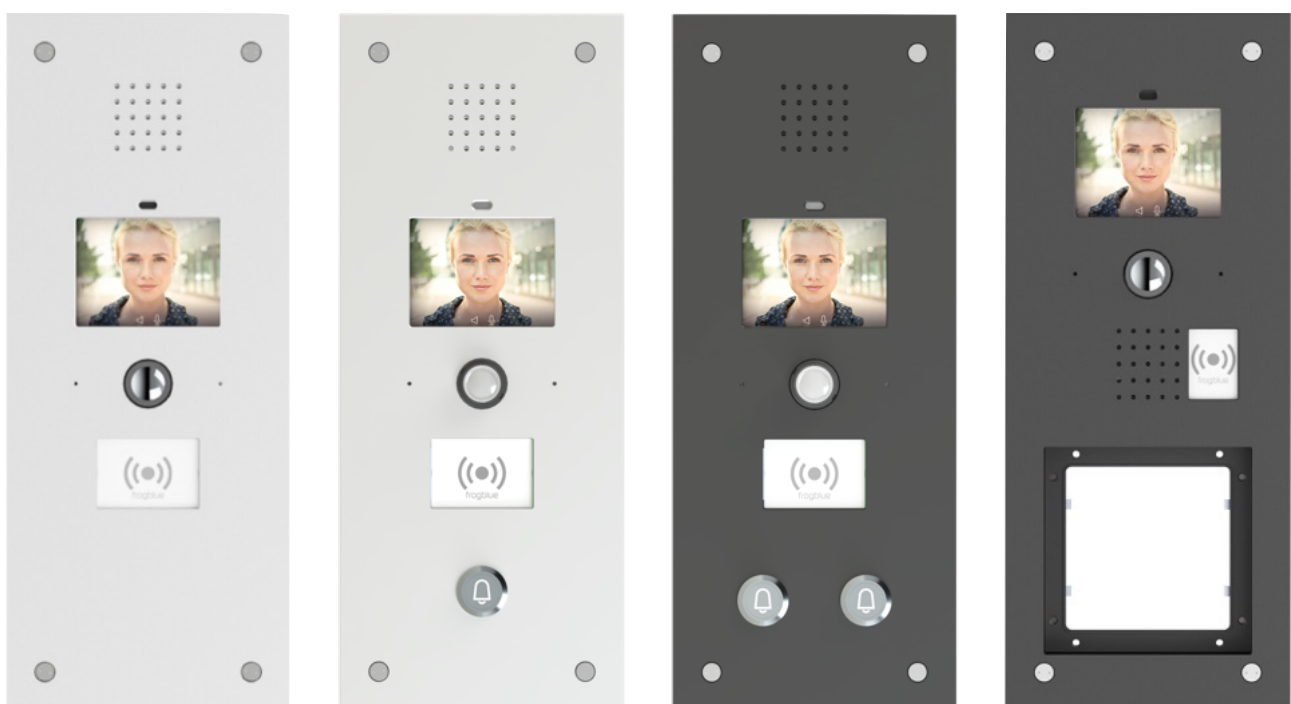
Glas - Line

K - Line

ALU - Line

S2 ALU

S3 X



S3 Plus

S3 Plus B1

S3 Plus B2

S3 Vario

---

# frogTerminal Installationshandbuch

## Funktionsübersicht und technische Beschreibung

---

<b>A. Einführung, Systemübersicht und Hauptmerkmale</b>	<b>8</b>
1. Übersicht	8
2. Hauptvorteile des frogTerminals	9
3. Telefonie-Übersicht	9
3.1. Weltweiter Telefonie-Standard	9
3.2. Direkte Integration von Endgeräten	10
3.3. Das frogDisplay	10
3.4. Die frogStation	10
3.5. Integration mit Telefoniesystemen	11
3.6. frogSIP-App und das Anrufen eines Smartphones	11
3.7. Mischbetrieb	11
3.8. Video-Gegensprechanlage	11
4. Überblick über die Zutrittskontrolle	12
4.1. Einführung	12
4.2. Dezentrale Zutrittskontrolle	12
4.3. NFC/RFID-Karteninformationen	12
4.4. Zutritts-Funktionen	13
4.5. Besondere Zutrittsfunktionen	13
4.6. Übersicht der frogTerminal Zutrittskontrolleinstellungen	14
4.7. Hinzufügen und Sperren von RFID-Karten	15
4.8. Benutzeranzeige am Terminal	15
5. Hardware-Integrationen	15
5.1. Relais und Eingänge	15
5.2. IP-Link-Integration	16
5.3. PIN-Steuerung	16
5.4. USB-C Erweiterung (USB 2.0 kompatibel)	16
5.5. Bluetooth Mesh-Integration	16
5.6. Vario Modul-Slot	16
6. Kernfunktionen	17
6.1. Funktionen der Zutrittskontrolle	17
6.2. SIP-Telefoniefunktionen	17
6.3. Funktionen für Aufnahme und Ereignisverwaltung	18
6.4. SIP-Telefonie-Registrierung und Kosten	18

<b>7.</b>	<b>Zutrittskontrollmanagement</b>	<b>18</b>
7.1.	Cloud-basiertes Zutrittskontrollmanagement (frogAccessControl)	18
7.2.	Lokale Benutzerverwaltung (frogEasyAccess)	18
7.3.	RFID-Kartenverschlüsselung	19
7.4.	Initialisierung und Authentifizierung von RFID-Karten	19
7.5.	Auf der Karte gespeicherte Informationen	20
7.6.	Terminal-Einstellungen	20
7.7.	Hinzufügen und Sperren von Karten	21
7.8.	Benutzeroberfläche für die Zutrittskontrolle	21
<b>8.</b>	<b>Inbetriebnahme</b>	<b>22</b>
8.1.	Einrichtungsprozess	22
8.2.	Initiale Einrichtungsanforderungen	22
<b>9.</b>	<b>Vorteile &amp; Differenzierung</b>	<b>23</b>
<b>10.</b>	<b>Zusätzliche Funktionen</b>	<b>24</b>
10.1.	Mehrparteien-Türklingelfunktionalität	24
10.2.	Erweiterte SIP-Telefoniefunktionen	24
10.3.	Innovationen in der Zutrittskontrolle	24
10.4.	Integration mit Drittanbietersystemen	25
10.5.	Cloud-basiertes Management	25
10.6.	Lokale Management-Funktionen	25
10.7.	Strom- und Anschlussoptionen	26
10.8.	Zeiterfassung und Anwesenheitsmanagement	26
<b>B.</b>	<b>Installationsszenarien</b>	<b>27</b>
1.	frogTerminal: Erste Schritte	27
2.	frogTerminal mit FRITZ!Phone & FRITZ!Box	27
3.	Von frogTerminal zu frogDisplay / frogStation	28
4.	frogTerminal Integration in MOBOTIX Management Center (MxMC)	31
5.	Kopplung frogTerminal und KNX	32
<b>C.</b>	<b>Technisches Installationshandbuch</b>	<b>35</b>
1.	Einführung	35
1.1.	Zweck des Handbuchs	35
1.2.	Sicherheit & Konformität	35
1.3.	Benötigte Werkzeuge & Ausrüstung	35
1.4.	Systemübersicht	36
1.5.	Installationsablauf	36
1.6.	Support & Dokumentation	36

<b>2.</b>	<b>Vor-Installationsanforderungen</b>	<b>37</b>
2.1.	Standortanforderungen	37
2.2.	Strom & Konnektivität	37
2.3.	Abmessungen & Gewicht	38
2.4.	Standortbewertung	39
2.5.	Benötigte Komponenten für die Installation	39
2.6.	Lieferumfang	39
<b>3.</b>	<b>Physischer Installationsprozess</b>	<b>40</b>
3.1.	Montage des Geräts	40
3.1.1.	Standardmontage an der Oberfläche	40
3.1.2.	Aufsatzmontage	41
3.2.	Anschluss von Strom & Netzwerk	41
<b>4.</b>	<b>Ersteinrichtung &amp; Konfiguration On-Device Touchscreen-Installationsassistent</b>	<b>42</b>
4.1.	Installationsassistent – Schritt 1: Sprache und Zeitzone einstellen	42
4.2.	Installationsassistent – Schritt 2: Admin-PIN festlegen	43
4.3.	Installationsassistent – Schritt 3: Web-Passwort / HTTPS Admin-Passwort festlegen	44
4.4.	Installationsassistent – Schritt 4: frogblue Mesh Setup	45
4.5.	Installationsassistent – Schritt 5: Gerätenamen festlegen	46
4.6.	Installationsassistent – Schritt 6: Startbildschirm-Layout festlegen	46
4.7.	Installationsassistent – Schritt 7: frogTerminal mit Ihrem Netzwerk verbinden	47
4.8.	Installationsassistent – Schritt 8: Verbindung zur frogCloud herstellen	48
4.9.	Installationsassistent – Schritt 9: Login zu oder Registrierung eines frogCloud-Kontos	48
4.10.	Installationsassistent – Schritt 10: Bestätigen Sie die Aktivierungs-E-Mail des Kontos	49
4.11.	Installationsassistent – Schritt 11: Cloud-Projekt erstellen	49
4.12.	Installationsassistent – Schritt 12: Türklingeltasten erstellen	49
4.13.	Installationsassistent – Schritt 13: Mit einem smarten Gerät koppeln	50
4.14.	Startansicht und Erklärungen der Anzeigemodi	50
4.15.	Installationsassistent – Schritt 14: Startansicht auswählen	52
4.16.	Installationsassistent – Schritt 15: Assistent abschließen	52
<b>5.</b>	<b>frogSIP App Benutzeroberfläche</b>	<b>53</b>
5.1.	Einführung in frogSIP	53
5.2.	Übersicht des Begrüßungsbildschirms	53
5.3.	Neues frogCloud-Benutzerkonto über die frogSIP App erstellen	54
5.4.	Anmeldung in der frogSIP App mit einem bestehenden frogCloud-Benutzerkonto	56
5.5.	Übersicht der Hauptbenutzeroberfläche der App	58
5.5.1.	In-Call Symbolleiste	60
5.5.2.	Logs & Wiedergabe Symbolleiste	60
5.6.	Kopplung des Terminals mit der frogSIP App	61
5.7.	Anrufe und Wiedergabe mit dem frogTerminal	64
5.7.1.	Empfang von Anrufen	64
5.7.2.	Automatische Anrufannahme-Konfiguration	64
5.7.3.	Anrufe initiieren	64

5.7.4.	Zutritts- & Ereignisprotokolle und Wiedergabe eines frogSIP-Anrufs	66
5.8.	Terminal-Geräteeinstellungen	67
5.9.	Terminal-Nutzereinstellungen	70
5.9.1.	Einstellungen für Klingelschilder	71
5.9.2.	Einstellungen für die Zugangskontrolle per PIN	72
5.9.3.	Türöffner	72
<b>6.</b>	<b>Zeitprofile</b>	<b>73</b>
6.1.	Zeitpläne	73
6.2.	Sonderprogramme	75
6.3.	Zeitprofile	76
<b>7.</b>	<b>Zutrittskontrollkonfiguration</b>	<b>77</b>
7.1.	Einführung in die Zutrittskontrolle von frogTerminal	77
7.2.	PINs, Zutrittscodes	77
7.3.	Grafisches Feedback für Zutrittsereignisse	77
7.4.	Dezentrale Zutrittskontrolle	80
7.5.	Karteninformationen	80
7.6.	Zutritts-Funktionen	81
7.7.	Spezialfunktionen	81
7.8.	RFID-Verschlüsselung und Zonen	81
7.8.1.	RFID-Verschlüsselung und Zonen über den Webbrowser (Terminal-Einstellungen)	82
7.8.2.	RFID-Verschlüsselung und Zonen über den On-Device-Touchscreen	85
7.9.	Formatieren von Schlüsseln/Karten über den On-Device-Touchscreen	86
7.10.	Hinzufügen und Sperren von Karten	88
7.10.1.	Hinzufügen und Sperren von Karten über den Webbrowser	88
7.10.2.	Hinzufügen und Sperren von Schlüsseln/Karten über den On-Device-Touchscreen	90
<b>8.</b>	<b>Anrufziele einrichten</b>	<b>92</b>
8.1.	Klingelschilder	92
8.1.1.	Klingelaktionen: frogSIP-Kontakt einladen	93
8.1.2.	Klingelaktionen: frogCloud SIP-Konto anrufen	94
8.1.3.	Klingelaktionen: SIP-Gerät per IP anrufen	94
8.1.4.	Klingelaktionen: Benutzerdefinierten SIP-Server verwenden	95
8.1.5.	Klingelaktionen: frogMessage senden	96
8.1.6.	Klingelaktionen: Hardware-Relais auslösen	96
8.1.7.	Klingelaktionen: Türöffner auslösen	97
8.1.8.	Klingelaktionen: HTTP-Anfrage senden	97
8.1.9.	Klingelaktionen: Sende IP-Notify	98
8.1.10.	Klingelaktionen: Bild oder Clip anzeigen	99
8.1.11.	Klingelaktionen: → Nächste Anrufaktion	99
8.1.12.	Klingelaktionen: MOBOTIX-MxMC-Benachrichtigung	100
8.1.13.	Klingelaktionen: Sound Aktion	100
8.2.	Authentifizierungs-Anrufziel	101
8.3.	Automatische Aktionen	101

<b>9.</b>	<b>Ereignismanagement</b>	<b>102</b>
9.1.	Ereignisse	104
9.1.1.	frogMessage empfangen	104
9.1.2.	Cube Zugang	105
9.1.3.	IP Notify Ereignis	105
9.1.4.	KNX-Systemereignis	106
9.1.5.	Lokaler Eingangsauslöser	106
9.1.6.	SIP-Anrufereignis	107
9.1.7.	Annäherungsauslöser	108
9.1.8.	Intervall-Timer-Ereignis	108
9.1.9.	Zeitprofil-Ereignis	109
9.2.	Aktionen	109
9.2.1.	FrogMessage Aktion	109
9.2.2.	HomeObject Aktion	110
9.2.3.	HTTP Aktion	110
9.2.4.	HTTP Post Camera Aktion	110
9.2.5.	IP Notify Aktion	111
9.2.6.	KNX Aktion	111
9.2.7.	Lokaler Ausgang Aktion	112
9.2.8.	SIP Aktion	113
9.2.9.	Sound Aktion	113
9.2.10.	RecordImage Aktion	113
9.2.11.	StoreVariable Aktion	113
<b>10.</b>	<b>Kameraeinstellungen und Aufnahmeverwaltung</b>	<b>114</b>
10.1.	Konfiguration der Kameraeinstellungen	114
10.2.	Optimale Einstellungen für geringe Latenz und hohe Bildrate	115
10.3.	Ereignis-Aufnahmeeinstellungen	115
<b>11.</b>	<b>Funktions-PINs</b>	<b>116</b>
<b>12.</b>	<b>Hardware</b>	<b>117</b>
12.1.	Näherungssensor & Touchscreen-Display	117
12.2.	Ein- / Ausgabe-Einstellungen	117
<b>13.</b>	<b>Touchscreen-Display-Layout</b>	<b>118</b>
<b>14.</b>	<b>Allgemeine Terminal-Einstellungen</b>	<b>119</b>
<b>15.</b>	<b>Türsteuerungseinstellungen</b>	<b>120</b>
<b>16.</b>	<b>Onboard-Medieneinstellungen</b>	<b>120</b>
16.1.	Audio-Dateien	120
16.2.	Bilddateien	121
16.3.	Video-Dateien	121
16.4.	Streamliste	121
16.5.	Ereignisbilder	122

<b>17.</b>	<b>Konfiguration des frogTerminals für Automatisierung via frogCast/frogMesh123</b>	
<b>18.</b>	<b>Netzwerkconfiguration</b>	<b>124</b>
18.1.	Ethernet- oder WLAN-Einrichtung	124
18.1.1.	Netzwerkconfiguration über den Webbrowser	124
18.1.2.	Netzwerkconfiguration über den On-Device-Touchscreen.	125
18.1.3.	Ethernet-Konfiguration über den On-Device-Touchscreen.	126
18.1.4.	WLAN-Konfiguration über den On-Device-Touchscreen.	126
18.1.5.	Fehlersuche bei Netzwerkverbindungsproblemen	126
18.2.	SIP-Server-Registrierung	127
18.2.1.	SIP-Grundlagen	127
18.2.2.	SIP-Einrichtung über den Webbrowser	128
18.3.	Benutzerdefinierte Root-Zertifikate	129
<b>19.</b>	<b>Sicherheit</b>	<b>131</b>
19.1.	Admin PIN	131
19.2.	Admin Passwort	131
<b>20.</b>	<b>Integration mit Drittanbieter-Videosystemen</b>	<b>132</b>
20.1.	HTTPS- oder Web-Integration - Unverschlüsselter MJPEG-Stream	132
20.2.	RTSP-Einstellungen	132
20.3.	RTSP-Stream-Integration	134
20.4.	Integration mit MOBOTIX MxManagementCenter	139
20.4.1.	Übersicht	139
20.4.2.	Integration Schritt für Schritt	140
<b>21.</b>	<b>Erweiterte Integration und API-Funktionen</b>	<b>147</b>
21.1.	Benutzerdefinierte Anzeigeoberflächen	147
21.2.	Zeiterfassung und Anwesenheitsmanagement	147
<b>22.</b>	<b>Wartung und Fehlersuche</b>	<b>147</b>
22.1.	Firmware-Updates	147
22.2.	Systemsteuerung - Konfigurationsdateien, Neustart und Werkseinstellungen	147
<b>D.</b>	<b>Terminal Versionen</b>	<b>150</b>

# A. Einführung, Systemübersicht und Hauptmerkmale

---

## 1. Übersicht

Das **frogTerminal** bietet Funktionalitäten, die weit über ein herkömmliches Video-Gegensprechanlagensystem hinausgehen. Sein Hauptmerkmal ist die Netzwerkanbindung und die direkte Nutzung des globalen IP-Telefonie-Standards SIP - ohne dass ein zusätzliches Gerät erforderlich ist. Dadurch können alle SIP-kompatiblen Geräte direkt angerufen werden, ohne dass ein Server oder eine Cloud benötigt wird.

In gewerblichen **Mehrparteien-Szenarien** haben Mieter oft ihre eigenen IP-Telefonanlagen mit integrierten SIP-Servern. In solchen Fällen verbinden sich Gegensprechanlagen typischerweise über externe Anrufe mit diesen Systemen. Das **frogTerminal** hingegen kann sich gleichzeitig als **Nebenstelle** bei mehreren SIP-Servern registrieren, um die Funktionen des Telefonesystems optimal zu nutzen.

Die integrierte **8-Megapixel-Kamera** mit hemisphärischer Optik bietet eine 180°-Panoramaansicht, und alle Aktionen am Terminal können eine Aufnahme auslösen. Es lässt sich auch in Video-Management-Software wie MxMC® integrieren und unterstützt Echtzeit-Video-Streaming in Full HD via RTSP/H.264.

Verbindungsoptionen für das frogTerminal umfassen:

- 1-Gbit Ethernet mit **Power over Ethernet (PoE)** über das Netzkabel
- 12-24VDC (12W) (mit Schutz vor umgekehrter Polarität)
- 24VAC (12W)

Für einfache Anwendungen kann das integrierte Relais direkt die Türentriegelung steuern, während zwei Eingangsports den direkten Anschluss an externe Türklingentaster oder magnetische Türkontakte ermöglichen.

Das **integrierte Touch-Display** erlaubt die virtuelle Gestaltung von Türklingelbeschriftungen. Alternativ kann eine Partei diskret über eine Wohnungsnummer angerufen werden. PIN-Codes können ebenfalls eingegeben werden, um die Tür zu entriegeln oder spezielle Funktionen zu aktivieren.

Ein **Smartphone**-Anruf wird als Standard-Telefonanruf initiiert, wenn die Türklingel betätigt wird. Dies erfordert eine Registrierung in der frogCloud (mit SIP-Server) und die Installation der frogSIP-App auf dem Smartphone.

Der **integrierte RFID-Leser** erleichtert die Zutrittskontrolle und Zeiterfassung. Durch die Kombination von RFID mit einer über das Display eingegebenen PIN ermöglicht das System eine Zwei-Faktor-Authentifizierung. Die Zutrittskontrolle kann zusätzlich durch individuell angepasste Wochenpläne eingeschränkt werden. Für erhöhte Sicherheit kann auch eine Drei-Faktor-Authentifizierung aktiviert werden, bei der zusätzlich ein automatischer Telefonanruf als weitere Verifizierungsstufe erfolgt. Diese Drei-Faktor-Authentifizierung kann so konfiguriert werden, dass sie zu festgelegten Zeiten, beispielsweise nach Geschäftsschluss, aktiviert wird, um eine strengere Zutrittskontrolle in kritischen Zeiträumen zu gewährleisten.

Das frogTerminal unterstützt Mehrparteien- und Mehrmieter-Fähigkeiten, da jede Partei ihre Zutrittsdaten individuell konfigurieren kann. Hardware von Drittanbietern, wie Schrankenanlagen oder KNX-basierte Lichtsteuerungen, kann über IP-Befehle integriert werden. Die bauintegrierten

frogblue-Steuerungskomponenten werden direkt über Bluetooth verbunden, was eine einfache Implementierung von frogblue-Modulen für Funktionen wie Torsteuerung oder Türentriegelung ermöglicht. DALI-Leuchten werden direkt mit unserem DALI frog unterstützt. Für eine detaillierte Übersicht über die Integrationsoptionen verweisen wir auf die frogblue API-Dokumentation sowie unsere Wettbewerbsanalyse.

Der Inbetriebnahmeprozess wird durch einen benutzerfreundlichen Assistenten geführt, der den Administrator Schritt für Schritt durch die notwendigen Konfigurationsschritte des Terminals leitet.

## 2. Hauptvorteile des frogTerminals

- **Integrierte 8-MP-Kamera** - Bietet visuelle Verifizierung und 180°-Panoramabilder
- **Eingebaute Video-SIP-Telefonie** - Ermöglicht den Remote-Betrieb durch eine Rezeption oder einen Sicherheitsmitarbeiter
- **Erweiterte Multi-Faktor-Authentifizierung** - Unterstützt Multi-Faktor-Authentifizierung, einschließlich RFID, PIN, Video-Verifizierung per Anruf und weitere Integrationen
- **Weltweite Videoanrufe** - Verbindet direkt mit Smartphones oder SIP-Telefonen weltweit
- **Echtzeit-Sicherheitswarnungen** - Sendet Anrufbenachrichtigungen bei unbefugten Zugriffsversuchen oder eingeschränktem Benutzerzugang
- **Flexibles Mehrterminal-Zutrittskontrollmanagement** - Unterstützt bis zu neun Zutrittszonen, auch ohne IP-Verbindung
- **Optionale Benutzergruppenverwaltung** - Zentrale Speicherung in der frogCloud (in Entwicklung)
- **Nahtlose Hardware-Integration** - Unterstützt IP- oder Bluetooth-basierte Geräte für Lichtsteuerung, Torschaltung und mehr
- **Eigenständiger Betrieb** - Keine zusätzliche Hardware oder externe Computersysteme erforderlich
- **Hochgeschwindigkeits-Konnektivität** - 1-Gbit-Netzwerkverbindung mit PoE Class 3 oder WLAN-Unterstützung (auch kompatibel mit 24V AC/12V DC Stromversorgung)
- **Energieeffizientes Design** - Der Stromverbrauch liegt zwischen 5 und 8 Watt

## 3. Telefonie-Übersicht

### 3.1. Weltweiter Telefonie-Standard

Das frogTerminal nutzt den internationalen **Telefonie-Standard SIP** für Video- und Audio-Kommunikation. Dadurch werden alle SIP-kompatiblen Endgeräte direkt zugänglich, ohne zusätzliche Hardware. Nahezu alle modernen Telefonsysteme basieren auf diesem Standard, was die einfache Integration von Geräten Dritter ermöglicht.

Typischerweise registrieren sich alle Geräte bei einem **SIP-Server**, der die Anrufweiterleitung übernimmt. Dieser SIP-Server kann lokal installiert oder weltweit über das Internet bereitgestellt werden, um weltweite Telefonie zu ermöglichen.

Das frogTerminal ist so konzipiert, dass es lokale Telefonie unterstützt, ohne auf eine Internetverbindung angewiesen zu sein, was eine standortbezogene Kommunikation **ohne Cloud**

ermöglicht. Für die Verbindung mehrerer Unternehmensstandorte bietet ein „Virtual Private Network“ (VPN) eine sichere Lösung. Nur bei der Integration unabhängiger Standorte oder Smartphones ohne VPN wird ein internetbasierter Cloud-Service mit SIP-Server erforderlich. Um dies zu erleichtern, bietet frogblue einen eigenen SIP-Cloud-Service mit automatischen Konfigurationsoptionen an, gehostet in einem sicheren deutschen Rechenzentrum.

### 3.2. Direkte Integration von Endgeräten

IP-Telefone, wie beispielsweise die von Grandstream®, können direkt vom frogTerminal angerufen werden, ohne dass zusätzliche Komponenten erforderlich sind. Ein SIP-Server wird nicht benötigt, da die **Funktion des Direct SIP Call** verwendet wird, sofern das Gerät über eine IP-Adresse erreichbar ist.

Für kleine Setups besteht die einfachste Konfiguration aus einem frogTerminal und einem SIP-Desktop-Telefon. Damit entfällt die Notwendigkeit für SIP-Server-Hardware und -Management.

### 3.3. Das frogDisplay

Mit einem einfachen Software-Update kann das bestehende **frogDisplay** so aufgerüstet werden, dass es als Innenstation fungiert. Es verbindet sich via **WLAN** und arbeitet mit **100 - 240V Strom**. Die aktualisierte Software ermöglicht eine **automatische Konfiguration** mit dem **frogTerminal**, und ein einfacher Umschalter erlaubt den Betrieb als **Türklingel**.

Derzeit werden Geräte manuell zu den **Türklingeltasten** über ihre **IP-Adresse** hinzugefügt. Ein kommendes Software-Update wird die automatische Konfiguration ermöglichen.

Das **frogTerminal** bietet vier Modi zur automatischen Displaykonfiguration (derzeit in Entwicklung):

1. **Klingelmodus** - Alle entdeckten Displays werden automatisch in einem zyklischen Prozess unter einer Standard-Türklingelbeschriftung gruppiert.
2. **Raum-Modus** - Der dem Display zugewiesene Raumname (z. B. "**Foyer**") wird als Türklingelbeschriftung verwendet. Wenn mehrere Displays denselben Raumnamen haben, werden sie unter einer Klingeltaste zusammengefasst.
3. **Namensmodus** - Displays können mit einem individuellen Namen (z. B. "**Tom Smith**" oder "**Rezeption**") registriert werden, der automatisch als Türklingelbeschriftung dient. Displays mit demselben Namen werden unter einer Beschriftung gruppiert.
4. **Terminal-Modus** - Der im **Terminal** eingegebene Name wird als Türklingelbeschriftung verwendet. Ist kein Name konfiguriert, greift das System auf den **Namen des Displays** zurück, und wenn dieser nicht verfügbar ist, fällt es auf den **Raumnamen** zurück.

### 3.4. Die frogStation

Die **frogStation** ist ein frogblue-Gerät, das als primäre Gegenstelle für das **frogTerminal** dient. Sie wird z.B. in einer Wohnung installiert und bietet eine Benutzerschnittstelle für die Interaktion mit dem **frogTerminal** am Eingang. Sie ist ähnlich aufgebaut wie das frogTerminal, jedoch ohne ein Kameramodul. Im Gegensatz zum frogDisplay verfügt sie über erweiterte Audiofunktionen für eine bessere Tonqualität und unterstützt sowohl WLAN als auch kabelgebundene Netzwerkverbindungen mit PoE für erhöhte Zuverlässigkeit.

Sie verfügt über **zwei Schalteingänge** und ein **24V/1A-Relais** für externe Steuerungen, was eine nahtlose Integration mit zusätzlichen Systemen ermöglicht.

Dank ihres **verbesserten mechanischen und akustischen Designs** liefert die **frogStation** eine **überlegene und lautere Klangqualität** im Vergleich zum frogDisplay.

### 3.5. Integration mit Telefonesystemen

IP-Telefonesysteme verfügen typischerweise über eine PBX mit integriertem SIP-Server zur Registrierung von Geräten und zur Anrufweiterleitung. Das frogTerminal kann sich bei solchen SIP-Servern registrieren und als Erweiterung bestehender Telefonesysteme fungieren.

In Mehrparteien-Umgebungen verlassen sich Mieter oft auf separate Telefonesysteme. Die Lösung: Das frogTerminal unterstützt die gleichzeitige Registrierung und arbeitet mit mehreren SIP-Servern gleichzeitig, was eine nahtlose Integration über verschiedene Telefonesysteme hinweg ermöglicht.

### 3.6. frogSIP-App und das Anrufen eines Smartphones

Smartphone-Anrufe erfordern Push-Benachrichtigungen vom Gerätehersteller, um das Telefon zu aktivieren und die Telefonie-App zu starten. Zur Erleichterung dieses Prozesses betreibt frogblue eine dedizierte Telefonie-Cloud inklusive SIP-Server, die eine zuverlässige Zustellung der erforderlichen Push-Benachrichtigungen gewährleistet.

Das Smartphone muss die **frogSIP-App** installiert haben, welche die Anrufe auf dieselbe vertraute Weise wie reguläre Telefonanrufe entgegennimmt. Dieses Setup ist kostenlos und bleibt – abgesehen von der E-Mail-Verifizierung – anonym.

**frogSIP** ist für die **nahtlose Integration mit dem frogTerminal** konzipiert und bietet zahlreiche erweiterte Funktionen:

- **Nahtlose Geräte-Paarung:** Geräte können einfach verbunden und gekoppelt werden für ein reibungsloses Setup.
- **Integrierte Automatisierung:** Vollständig in das frogblue-Automatisierungssystem integriert, optimiert frogSIP die zentrale Verwaltung.
- **Direkter Zugriff & Protokollkontrolle:** Ermöglicht die unmittelbare Steuerung von Zugriffsberechtigungen, Anrufprotokollen, Aufnahmen und deren Wiedergabe.
- **Unterstützung für mehrere Türen:** Erleichtert die Verwaltung mehrerer Türen und erhöht so Sicherheit und Komfort.

Um persönliche Geräte über das Internet zu verbinden, ist frogCloud unerlässlich. Das frogTerminal registriert sich automatisch in der Cloud, sobald es vom Installateur oder Systemadministrator konfiguriert wurde.

### 3.7. Mischbetrieb

Das frogTerminal unterstützt den simultanen Betrieb aller Modi:

- Direkte SIP-Anrufe zu lokalen Geräten
- Registrierung bei mehreren Telefonesystemen (unter Verwendung verschiedener SIP-Server)
- Smartphone-Anrufe über die frogCloud

### 3.8. Video-Gegensprechanlage

Mit einer integrierten Kamera, Audio und Display bietet das **frogTerminal** umfassende Video-Gegensprechfunktionen. Im Gegensatz dazu unterstützen frogStation und frogDisplay den Videoempfang, sind jedoch für reine Audioübertragung optimiert. Neue Funktionen wie Durchsagen und Babyphone-Funktionen befinden sich in der Entwicklung.

## 4. Überblick über die Zutrittskontrolle

### 4.1. Einführung

Das frogTerminal bietet eine komfortable, zeitgesteuerte und multifaktorielle Zutrittskontrolle mittels PIN-Codes, RFID-Karten und Telefonanrufen. Für diese Funktionen ist **keine dauerhafte Cloud- oder Netzwerkanbindung erforderlich**.

Das Terminal unterstützt den internationalen **Mifare DESFire EV2** Kartentyp. RFID-Karten oder Schlüsselanhänger müssen nur an einem frogTerminal konfiguriert werden und können **ohne zusätzliche Einrichtung** an allen Terminals im selben Projekt verwendet werden. Eine Netzverbindung ist zwar nicht zwingend erforderlich, vereinfacht jedoch die Administration für den Fernzugriff.

### 4.2. Dezentrale Zutrittskontrolle

Mit frogblue werden Benutzerdaten direkt auf RFID-Karten oder Schlüsselanhängern gespeichert. Die Terminals lesen die Daten während eines Kartenlesevorgangs, was die Notwendigkeit einer Netzwerk- oder Cloud-Verbindung überflüssig macht.

Damit alle Terminals in einem Projekt die verschlüsselten Daten lesen können, müssen sie dieselben Verschlüsselungseinstellungen teilen, die Folgendes umfassen:

- Einen zehnstelligen RFID-Code
- Projekt-Zeitstempel

Änderungen an den Benutzerdaten – wie aktualisierte PINs oder Zutrittsbefugnisse – müssen nur an einem Terminal (zum Beispiel am Haupteingang) vorgenommen werden. Das System aktualisiert daraufhin automatisch die Karte mit den neuen Daten beim nächsten Einsatz, dies gewährleistet einen reibungslosen Aktualisierungsprozess. Das Sperren einer Karte erfolgt auf dieselbe Weise.

**Hinweis:** Die Synchronisation über IP-Netzwerke und lokal via Bluetooth sowie ein cloud-basiertes Zutrittskontrollsystem mit Zeiterfassung befinden sich derzeit in Entwicklung.

### 4.3. NFC/RFID-Karteninformationen

Die RFID-Karte speichert alle wesentlichen Benutzerzutrittsdaten, einschließlich:

- Name, Vorname und Personalnummer
- Ausgabedatum
- Gültigkeitszeitraum (von Startdatum/-zeit bis Enddatum/-zeit)
- Persönlicher PIN-Code für den Zutritt
- Wöchentliche Zutrittspläne
- Bis zu neun Zutrittszonen

Jedes **frogTerminal** liest und interpretiert den Inhalt der Karte bei jedem Scan. Änderungen, wie etwa aktualisierte PINs oder Zutrittspläne, werden **automatisch** beim Lesen der Karte übernommen.

Das Terminal protokolliert den Karteninhalt, einschließlich Zeitstempeln für jede Aktion. Benutzerinformationen und Zutrittszeiten können direkt am Terminaldisplay oder über die frogSIP-App eingesehen werden. Falls eine Netzwerkverbindung vorhanden ist, können diese Protokolle auch remote über einen Webbrowser abgerufen werden.

#### 4.4. Zutritts-Funktionen

RFID-Karten oder Schlüsselanhänger definieren benutzerspezifische Zutrittsregeln. Diese beinhalten PINs, Wochenpläne und Zutrittszonen. Zusätzliche Terminal-spezifische Einstellungen können diese Regeln überschreiben oder anpassen (**Zutrittskontrolle** → **Terminal-Einstellungen**):

- PIN-Anforderungen
  - Bestimmte Türen können so konfiguriert werden, dass der Zutritt ohne die persönliche PIN des Benutzers ermöglicht wird, z. B. für interne Türen. (PIN-Code Quelle: **None**).
  - Alternativ kann eine Tür mit einem Terminal-spezifischen Code gesichert werden. Diese PIN gilt für alle Benutzer gleich und überschreibt die persönlichen PINs. (PIN-Code Quelle: **Terminal**).
- Zeitbeschränkungen
  - Zutrittszeiten können auf Basis des individuellen Kartenplans oder global für alle Benutzer am Terminal konfiguriert werden (Zeitplan Quelle: **Card** oder **Terminal**).
  - Zeitbeschränkungen können für bestimmte Terminals auch vollständig deaktiviert werden (Zeitplan Quelle: **None**).

#### 4.5. Besondere Zutrittsfunktionen

RFID-Karten können zusätzliche Funktionen speichern:

- Automatischer SIP-Telefonanruf (SIP URI)
- Eine Telefonnummer, die automatisch gewählt wird, wenn die Karte präsentiert wird
- IP-Link - löst automatisch externe Systeme aus oder integriert diese (z. B. Zeiterfassung oder spezielle Funktionen).

Diese Funktionen ermöglichen es, dass RFID-Karten als Funktionstrigger wirken und nicht nur als benutzerspezifische Zutrittstools. Beispielsweise könnte eine RFID-Karte mit der Bezeichnung "Lagereingang" je nach Bedarf geteilt werden.

Spezielle Funktionseinstellungen an Terminals bieten drei allgemeine Optionen:

1. **None**: Besondere Funktionalitäten sind deaktiviert.
2. **Card**: Die auf der RFID-Karte gespeicherte Funktion wird aktiviert.
3. **Terminal**: Die auf dem Terminal gespeicherte Funktion wird anstelle der auf der Karte gespeicherten Funktion aktiviert.

## 4.6. Übersicht der frogTerminal Zutrittskontrolleinstellungen

Die Einstellungen des Terminals können über das Display und remote über die Web-Oberfläche konfiguriert werden. Folgende zentrale Zutrittsdaten müssen während der Initialisierung festgelegt werden:

- RFID-Code: zehnstelliger Verschlüsselungscode für Karten (aus Sicherheitsgründen gehasht)
- Projektdatum: Gemeinsames Datum für die Kartenverschlüsselung für alle Geräte im Projekt
- Projekt-Nummer: Gemeinsame ID zur Identifizierung des Projekts für alle Geräte im Projekt (1-32.767)
- Zone: Weisen Sie dem Terminal eine von neun Zutrittszonen zu
- PIN-Code Quelle: None, Card, Terminal
- Terminal-PIN-Code: sechsstelliger Zutrittscode
- Zeitplan-Quelle: None, Card, Terminal
- Terminal-Zeitplan: Zeitplan für den Zutritt an diesem Terminal
- Zeitplan-Ausnahme: None, PIN oder Request, z. B. für den Zutritt außerhalb regulärer Pläne
- Authentifizierungsanruf: Never, Card, On Exception, Always
- URL-Quelle: None, Card, Terminal - Die Quelle für die Web-Hook URL
- Terminal-URL: Web-Hook URL zur Echtzeitintegration von Zutrittsvorgängen
- Ausgabedatum: Mindestausgabedatum - Karten, die vor diesem Datum ausgegeben wurden, sind ungültig.

Für unterschiedliche Sicherheitsniveaus an verschiedenen Terminals können folgende Einstellungen angewendet werden:

- **None:** Funktion ist nicht erforderlich, z. B. Zutritt ohne PIN-Überprüfung an einem bestimmten Terminal.
- **Card:** Der Funktionsparameter wird von der RFID-Karte gelesen.
- **Station:** Der Parameter wird vom Terminal selbst abgerufen - z. B. eine globale PIN für alle Benutzer an einem bestimmten Standort oder die direkte Integration an diesem spezifischen Zutrittspunkt, d. h. Zeiterfassung, Arbeitsplatzmanagement, Rufanlage im Pflegebereich oder Logistiksysteme.
- **PIN-Authentifizierung:** Der Zutritt kann auch ohne RFID-Karte erfolgen, indem nur eine im Terminal gespeicherte PIN verwendet wird.

## 4.7. Hinzufügen und Sperren von RFID-Karten

### Hinzufügen von Karten:

Ein Benutzer kann eine RFID-Karte selbst registrieren, sofern eine autorisierte Station den Vorgang per SIP-Telefonanruf bestätigt. Der Benutzer gibt seine persönlichen Daten (z. B. Name, Personalnummer) ein, während ein Administrator die Daten freigibt und zusätzliche Parameter festlegt.

### Sperren von Karten:

Das Sperren einer Karte kann lokal an allen Terminals erfolgen, da jedes Terminal seine eigene Sperrliste verwaltet. Eine Remote-Sperrung über die Web-Oberfläche ist möglich.

**Hinweis:** In einer cloud-basierten Lösung erfolgt das Sperren zentral und erfordert keine Aktion an jedem einzelnen Terminal.

## 4.8. Benutzeranzeige am Terminal

Das Terminal zeigt für die Benutzer Folgendes an:

- Großes Klingelsymbol: Für nicht authentifizierte Benutzer
- Tastenfeld-Menü: Zur Eingabe der PIN
- Einstellungsmenü: Für den Administratorzugang
- Datums- und Zeitanzeige: Hilft, falsche Terminaleinstellungen zu identifizieren
- Zeiterfassungsoptionen: Menüs **Check-in**, **Break** und **Check-out** zur Zeiterfassung

**Hinweis:** Zum Beispiel beinhaltet das ODOO ERP-System ein Zeiterfassungsmodul; eine integrierte Lösung mit frogblue und ODOO befindet sich derzeit in der Entwicklung.

## 5. Hardware-Integrationen

### 5.1. Relais und Eingänge

Das frogSIP-Terminal beinhaltet einen potentialfreien Relaisausgang (24V/1A), der bei Anschluss an eine externe Stromversorgung (12V oder 24V) direkt ein Türschloss steuern kann.

Es verfügt außerdem über zwei lokale Eingänge am Terminal, die direkt an Taster oder magnetische Kontakte angeschlossen werden können, ohne dass eine zusätzliche Stromversorgung erforderlich ist. Diese Eingänge können konfiguriert werden für:

- Das Auslösen einer Türklingel via externem Taster zur Anrufinitiierung an einer SIP-Gegenstelle
- Automatische Anrufe, die durch Sensoren (z. B. Bewegungsmelder oder Lichtschranken) ausgelöst werden
- Das Senden von Signalen via Bluetooth Mesh (z. B. für Lichtsteuerung) oder IP
- Die Überwachung des Türstatus mittels magnetischer Kontakte (offen/geschlossen); mit dem zweiten Eingang kann registriert werden, ob die Tür verriegelt ist.

## 5.2. IP-Link-Integration

Das Terminal unterstützt das Auslösen externer Systeme via IP-Links. Beispielsweise kann das Scannen einer RFID-Karte oder das Drücken eines Tasters Funktionen auslösen wie:

- Das Öffnen einer Parkschanke
- Das Hochziehen einer Rolltür
- Den Start von Videoaufnahmen an einer externen Kamera

## 5.3. PIN-Steuerung

Vorkonfigurierte Funktions-PIN-Codes, die bestimmten IP-Befehlen oder Mesh-Nachrichten zugeordnet sind, können zur Steuerung externer Systeme oder Hardware verwendet werden. Funktions-PINs können unter allen Benutzern geteilt werden und beispielsweise zur Steuerung von Licht, Toren, Sicherheitskameras oder Software von Drittanbietern genutzt werden.

## 5.4. USB-C Erweiterung (USB 2.0 kompatibel)

Der USB-C-Anschluss des Terminals ermöglicht den Anschluss von frogblue-Hardware-Erweiterungen, einschließlich:

- Interner Hardware (z. B. Sensoren, mechanische Tastenfelder)
- Externer USB-Geräte (z. B. lokaler Datenspeicher oder zusätzliche Steuerungsmodule)

## 5.5. Bluetooth Mesh-Integration

Das Terminal beinhaltet eine frogblue Bluetooth Mesh-Schnittstelle zur Integration in frogblue-Projekte. Über die ProjectApp wird es vollständig in frogblue-Projekte integriert.

## 5.6. Vario Modul-Slot

Das frogSIP Terminal Vario beinhaltet einen dedizierten Slot für ein Vario-Modul, der die Integration von Modulen Dritter ermöglicht, wie zum Beispiel:

- Zeiterfassungssysteme
- Fingerabdruckleser

Derzeit wird die Integration nur für die Siedle 1- und 2-Reihen über direkte Schalt-Eingänge/-Ausgänge unterstützt.

Diese Module können eigenständig funktionieren oder an die Hardware des Terminals gekoppelt werden, um vordefinierte Aktionen auszulösen.

## 6. Kernfunktionen

### 6.1. Funktionen der Zutrittskontrolle

Das frogTerminal unterstützt Mehrparteien-Türklingelfunktionalitäten, die Anrufe an SIP-Gegenstellen oder Smartphones für die Zutrittskontrolle ermöglichen. Eine Zwei-Wege-Video- und Audio-Kommunikation ist im Freisprechbetrieb möglich. Zu den Zutritts-Funktionen gehören:

- Türklingel und manuelle Türentriegelung: Anrufe an Smartphones oder SIP-Telefone mit Umleitung außerhalb der Zutrittszeiten
- PIN-gesteuerter Zutritt: Geteilte oder benutzerspezifische PINs mit individuellen Zeitplänen
- RFID-Karten oder -Transponder (DESFire EV2 Standard): Unterstützt wöchentliche Zeitpläne
- Zwei-Faktor-Authentifizierung: RFID-Karte + persönliche PIN mit Zeitplänen
- Drei-Faktor-Authentifizierung: RFID-Karte + PIN + visuelle Verifizierung via Telefonanruf
- Visuelle Verifizierung via Telefonanruf: Außerhalb regulärer Zutrittszeiten
- frogKey (Bluetooth-Transponder): Für fahrzeugbasierten Zutritt mit Zeitbeschränkungen

### 6.2. SIP-Telefoniefunktionen

Das frogSIP-Terminal verfügt über ein weltweit standardisiertes SIP-Telefonie-Modul mit Zwei-Wege-Video-Unterstützung über das Netzwerk. Zu den Hauptvorteilen gehören:

- Direkte Kompatibilität mit SIP-Endgeräten (z. B. Grandstream IP-Video-Telefone)
- Hohe Video- und Audioqualität ohne externe Konversionsmodule zur Vermeidung von Qualitätsverlusten
- Direktes IP-Anrufen ohne SIP-Server für einfachere Setups
- Unterstützung mehrerer SIP-Server für komplexe Installationen
- Smartphone-Integration über die frogSIP-App und den frogblue SIP-Server, gehostet in einem sicheren deutschen Rechenzentrum
- Die frogSIP-App bietet eine direkte Integration von frogblue Funktionen wie:
  - Türentriegelung
  - Lichtsteuerung
  - Kameraeinstellungen
  - Aufnahmesteuerung und Wiedergabe

Drittanbieter-SIP-Apps wie LinPhone, 3CX, Bria usw. können ebenfalls verwendet werden, erfordern jedoch möglicherweise DTMF-basierte Bedienung für zusätzliche Funktionen.

### 6.3. Funktionen für Aufnahme und Ereignisverwaltung

Das Terminal kann Aufnahmen für jede Aktion auslösen. Zu den Funktionen gehören:

- Speicherung von Rohbildern in voller Auflösung (4 MB) für die Nachbearbeitung und Zoomfunktionen
- Konfigurierbare Vor- und Nachalarm-Snapshots
- Detaillierte Metadaten für jede Aufnahme, einschließlich:
  - RFID-Karteninformationen
  - Video-Stream-Parameter (z. B. Belichtungseinstellungen)

### 6.4. SIP-Telefonie-Registrierung und Kosten

Die Registrierung von Smartphones erfolgt schnell und einfach über einen vom Terminal generierten QR-Code. Dies konfiguriert die Türklingel automatisch so, dass Anrufe an das Smartphone weitergeleitet werden.

Eine einzelne Smartphone-Registrierung pro Terminal ist kostenlos und anonym, erfordert lediglich eine E-Mail-Bestätigung innerhalb von zwölf Stunden. Erweiterte Funktionen wie externe Cloud-Speicherung oder zusätzliche frogblue SIP-Benutzer werden monatlich abgerechnet.

## 7. Zutrittskontrollmanagement

### 7.1. Cloud-basiertes Zutrittskontrollmanagement (frogAccessControl)

Für große Netzwerke mit mehreren Terminals an verschiedenen Standorten ist die zentrale Verwaltung über die cloudbasierte frogAccessControl die optimale Lösung. Dieses System ermöglicht:

- Sofortige Updates an alle Terminals mit einer einzigen Aktion
- Unmittelbares Sperren von RFID-Karten über alle Terminals hinweg

Diese Cloud-Lösung befindet sich derzeit in Entwicklung und baut auf der Funktionalität von frogControl und dem frogSIP-Server auf, wobei eine Datenbank für die zentrale Verwaltung integriert wird.

### 7.2. Lokale Benutzerverwaltung (frogEasyAccess)

Für kleinere Setups ohne intensives Management bietet die Lösung frogEasyAccess eine einfache und effiziente Benutzerverwaltung ohne Cloud-Integration. Dieser Ansatz ermöglicht, dass RFID-Karten, die an einem Terminal konfiguriert wurden, nahtlos an anderen Terminals im selben Projekt funktionieren, ohne dass eine zusätzliche Einrichtung erforderlich ist, und speichert Benutzerdaten direkt auf RFID-Karten, einschließlich:

- PIN-Code
- Wöchentliche Zeitpläne
- Zonenzutrittsberechtigungen
- Alle Terminals innerhalb eines Projekts müssen dieselben RFID-Verschlüsselungseinstellungen (RFID-Code und Projektdatum) teilen, um kompatibel zu sein.

## Hauptvorteile:

- Karten, die an einem Terminal initialisiert wurden, funktionieren automatisch an anderen Terminals im selben Projekt.
- Terminals können in bis zu neun Zutrittszonen gruppiert werden, wobei Karten mehreren Zonen zugewiesen werden können.
- Sicherheitseinstellungen können für jedes Terminal individuell angepasst werden (z. B. Deaktivierung der PIN-Anforderungen an bestimmten Terminals).
- Multi-Faktor-Authentifizierung kann für zusätzliche Sicherheit aktiviert werden, z. B. durch Anforderung einer Video-Verifizierung via SIP-Telefonanruf.

**Hinweis:** Zur Gewährleistung der Synchronisation von Zeit und Datum über die Terminals hinweg wird ein IP-Netzwerk oder Bluetooth Mesh empfohlen.

### 7.3. RFID-Kartenverschlüsselung

RFID-Karten werden aus Sicherheitsgründen verschlüsselt. Terminals in einem Projekt müssen dieselben Verschlüsselungseinstellungen verwenden, die sich aus:

- Einem zehnstelligen **Master Key**
- Dem Ausgabedatum des Projekts
- Der Projekt-ID (1-32.767) ergeben.

Diese Kombination erzeugt durch einen Hash-Algorithmus einen einzigartigen Schlüssel. Mehrere Projekte können ohne Konflikte koexistieren, da das Projektdatum und die ID für die Einzigartigkeit sorgen, selbst wenn der Master Key versehentlich wiederverwendet wird.

### 7.4. Initialisierung und Authentifizierung von RFID-Karten

Bei der Initialisierung an einem Terminal speichern RFID-Karten:

- Benutzerdaten (Name, Personalnummer)
- Zutrittsinformationen (PIN, Zonen, wöchentliche Zeitpläne)

Terminals lesen die Kartendaten für lokale, dezentrale Zutrittsentscheidungen, auch ohne Netzverbindung. Damit entfällt die Notwendigkeit einer manuellen Registrierung an jedem Terminal.

Der Fernzugriff der Benutzerdaten ist auch über:

- die Web-Oberfläche des Terminals sowie
- die frogSIP-App auf einem Smartphone möglich.

Diese bildet die Grundlage für erweiterte Cloud-Funktionalitäten.

## 7.5. Auf der Karte gespeicherte Informationen

RFID-Karten enthalten folgende Informationen:

- Benutzerdaten: Name, Vorname, Personalnummer
- Gültigkeitszeitraum: Start- und Enddaten
- Zonenzuweisungen (bis zu neun Zonen)
- Ein sechstelliger persönlicher PIN
- Wöchentliche Zutrittspläne
- IP-Link zur Auslösung von Funktionen über das Netzwerk
- SIP-Telefonnummer für automatische Anrufe beim Kartenscan
- Terminal-ID und Ausgabedatum des initialisierenden Terminals
- Eine AllStation-Kennzeichnung, die es der Karte ermöglicht, an allen Terminals im Projekt zu funktionieren
- Anpassungen pro Terminal: Spezifische Parameter (z. B. PIN-Anforderungen oder Zutrittspläne) können an einzelnen Terminals angepasst werden, ohne die Karte zu verändern.

## 7.6. Terminal-Einstellungen

Konfigurationsdaten für Terminals umfassen:

- RFID-Code: Verschlüsselungscode, der im gesamten Projekt geteilt wird
- Projektdatum: Wird zusammen mit dem RFID-Code zur Generierung der Verschlüsselungsschlüssel verwendet
- Authentifizierungsmodi: ***PIN, Card, Terminal, Cloud, PIN request, Card request***
- Zonenzuweisung: Eine von neun Zonen für das Terminal
- PIN-Quelle: ***None, Card, Terminal*** oder ***Cloud***
- Zutrittszeit-Quelle: ***None, Card, Terminal*** oder ***Cloud***
- Ausnahmebehandlung: ***None, PIN, Cloud*** oder ***Request*** (z. B. für Notfälle)
- Ausgabedatum: Nur Karten, die nach diesem Datum ausgegeben wurden, sind gültig.

## 7.7. Hinzufügen und Sperren von Karten

Benutzer können RFID-Karten selbst hinzufügen, wenn dies von einer autorisierten Station per SIP-Telefonanruf bestätigt wird

### Hinzufügen von RFID-Karten:

- Lokal durch den Administrator
- Administrator über einen RFID-Leser eines Drittanbieters (zukünftig/typische Hotellösung/ Web/Cloud)
- In Entwicklung: frogCast Mesh (IP-Verteilung von Zugangsregeln)

### Sperren von RFID-Karten:

- Kann lokal an allen Terminals erfolgen
- Kann remote über die Web-Oberfläche des Terminals durchgeführt werden
- Sperren aller Karten mit Gültigkeitszeitangabe

In einem cloud-basierten System erfolgt das Sperren zentral und erfordert kein Update an jedem einzelnen Terminal.

## 7.8. Benutzeroberfläche für die Zutrittskontrolle

Das Terminal zeigt benutzerfreundliche Optionen an, wie:

- Türklingelsymbole für nicht authentifizierte Benutzer
- Tastenfeld-Menü zur PIN-Eingabe
- Einstellungsmenü für Administratorzugang
- Datums- und Zeitanzeige zur schnellen Erkennung falscher Einstellungen
- Zeiterfassungsoptionen (z. B. "Check-in", "Break", "Check-out") für das Anwesenheitsmanagement

## 8. Inbetriebnahme

### 8.1. Einrichtungsprozess

Das frogTerminal verfügt über einen intuitiven Einrichtungs-Assistenten, folgend genannt „Wizard“, der Administratoren Schritt für Schritt durch den Konfigurationsprozess führt. Der Assistent vereinfacht die Initialisierung zentraler Einstellungen wie:

- Netzwerk- und Stromanschlüsse
- SIP-Registrierungen
- RFID-Verschlüsselungsparameter
- Zutrittszonen und -pläne

Sobald die Erstkonfiguration abgeschlossen ist, können Administratoren weitere Einstellungen über die Web-Oberfläche oder das Touch-Display des Terminals verfeinern.

### 8.2. Initiale Einrichtungsanforderungen

Während der Inbetriebnahme müssen folgende Parameter konfiguriert werden:

Netzwerkconfiguration: IP-Adresse, PoE- oder WLAN-Einstellungen

SIP-Registrierung: Integration mit SIP-Servern oder Aktivierung direkter SIP-Anrufe

**RFID-Verschlüsselungseinstellungen:**

- zehnstelliger RFID-Verschlüsselungscode
- Projektdatum (gemeinsam über alle Terminals im Projekt)
- Zonen und Zeitpläne
- Zuordnung des Terminals zu einer der neun Zonen
- Konfiguration wöchentlicher Zutrittspläne

**PIN- und Zutrittseinstellungen:**

- Standard PIN-Modi: **None, Card, Terminal** oder **Cloud**
- Zeitplan-Quelle: **None, Card, Terminal** oder **Cloud**
- Ausnahmebehandlung (z. B. Notfallzutritt): **None, PIN** oder **Request**

**Physischer Aufbau:**

- Stromversorgung anschließen (PoE oder externe Versorgung)
- Überprüfen der Ein- und Ausgangsverbindungen für Relais, Taster oder Sensoren

## 9. Vorteile & Differenzierung

Das frogTerminal bietet mehrere Vorteile gegenüber konkurrierenden Zutrittsterminals:

- Integrierte 8 MP Kamera: Bietet visuelle Verifizierung und 180°-Hemisphäraufnahmen
- Integrierte Video-SIP-Telefonie: Ermöglicht den Fernbetrieb durch Rezeptionisten oder Sicherheitskräfte
- Drei-Faktor-Authentifizierung: Kombiniert RFID-Karte, PIN und Telefonanruf (mit Video)
- Direkte weltweite Videoanrufe: Zu Smartphones oder SIP-Telefonen (Mac- und PC-Unterstützung in Entwicklung)
- Anruftenachrichtigungen bei unbefugtem Zutritt: Warnungen bei falschen PINs oder eingeschränktem Benutzerzugang
- Einfache Verwaltung mehrerer Terminals: Zutrittskontrolle über bis zu neun Zonen, auch ohne IP-Netzwerk
- Gruppenverwaltung mit zentraler Speicherung: Verfügbar über die frogCloud in Phase zwei
- Integration externer Hardware: IP- oder Bluetooth-basierte Steuerung für Licht, Tore oder Schranken
- Keine zusätzliche Hardware erforderlich: Erspart den Bedarf an externen Computern oder Servern
- Hochgeschwindigkeits-Netzwerkanbindung: 1-Gbit Ethernet mit PoE- oder WLAN-Unterstützung (24V AC/12V DC)
- Geringer Stromverbrauch: Nur 5-8 Watt

## 10. Zusätzliche Funktionen

### 10.1. Mehrparteien-Türklingelfunktionalität

Das frogSIP-Terminal unterstützt Mehrparteien-Konfigurationen, die unterschiedlichen Mietern oder Benutzern Folgendes ermöglichen:

- Personalisierte Türklingelbeschriftungen auf dem Touch-Display
- Wohnungswahl mit benutzerdefinierten oder vorgegebenen Nummern
- Integration externer Taster für spezifische Anrufe oder Auslöser

### 10.2. Erweiterte SIP-Telefoniefunktionen

Das frogSIP-Terminal nutzt den SIP-Telefonie-Standard für eine robuste Kommunikation:

- Direktes IP-Anrufen: Ermöglicht in kleinen Setups das Wegfallen eines SIP-Servers, was Hardwarekosten und administrativen Aufwand reduziert.
- Mehrfache SIP-Server-Registrierung: Unterstützt die Registrierung bei mehreren SIP-Servern gleichzeitig für komplexe Systeme oder Mehrparteien-Szenarien.
- Smartphone-Integration via frogSIP-App: Verfügbar für iOS und Android. Erleichtert Anrufe an Smartphones mit integrierten Türsteuerungsoptionen.
- Desktop-Kompatibilität: Die frogSIP-App ist für Mac verfügbar. PC-Unterstützung befindet sich in Entwicklung.
- Browserbasierte SIP-Funktionalität (ähnlich wie bei WhatsApp) ist in Arbeit, dies erfordert keine Browser-Plugins.
- Aufnahme- und Ereignisverwaltung: Aufnahmen in voller Auflösung, ausgelöst durch Aktionen am Terminal
- Konfigurierbare Vor- und Nachaufnahmen für detaillierte Analysen
- Metadaten werden bei jeder Aufnahme gespeichert, einschließlich der Nutzung der RFID-Karte und der aktuellen Videoeinstellungen.

### 10.3. Innovationen in der Zutrittskontrolle

Das frogTerminal ermöglicht zeitgesteuerten Zutritt unter Verwendung von RFID-Karten, PINs oder Telefonanrufen. Erweiterte Funktionen umfassen:

- Zwei-Faktor-Authentifizierung: RFID-Karte + PIN für erhöhte Sicherheit
- Drei-Faktor-Authentifizierung: RFID-Karte + PIN + Videoanruf-Verifizierung für kritische Zutrittspunkte
- Ereignisbasierte Benachrichtigungen: Warnungen bei fehlgeschlagenen Zutrittsvorgängen, Missbrauch oder spezifischen Benutzerzugängen

## 10.4. Integration mit Drittanbietersystemen

Das frogSIP-Terminal unterstützt die Integration mit externer Hardware und Systemen über:

- IP-Links: Zur Steuerung externer Geräte wie Parkschranken oder Lichtsysteme
- Bluetooth Mesh: Für die nahtlose Integration mit frogblue-Gebäudesteuerungsmodulen wie:
  - frogRelay für die Torsteuerung
  - frogDim für die Lichtsteuerung
- Hardware-Erweiterung via USB-C: Unterstützt interne und externe Hardwareerweiterungen (z. B. Bewegungsmelder, zusätzliche Kameras oder Tastenfelder)
- MQTT und JSON REST API für erweiterte Softwareintegrationen und Zukunftssicherheit

## 10.5. Cloud-basiertes Management

Das frogTerminal ist für die nahtlose Integration mit der frogCloud konzipiert, um erweiterte Funktionen zu ermöglichen wie:

- Zentrale Benutzer- und Gruppenverwaltung
- Synchronisierte Updates über alle Terminals hinweg
- Remote-Verwaltung und Sperrung von RFID-Karten in Echtzeit

## 10.6. Lokale Management-Funktionen

Für kleinere Systeme bietet die Lösung frogEasyAccess:

- Dezentrale Benutzerverwaltung mit verschlüsselten Daten, die auf RFID-Karten gespeichert sind
- Keine Abhängigkeit von der Cloud für die Funktionalität
- Kompatibilität zwischen Terminals im selben Projekt ohne erneute Registrierung

Warum keine Abhängigkeit vom Server oder der Cloud?

Einer der Hauptvorteile eines **dezentralen Zutrittskontrollsystems**, welches Zutrittsdaten, Zeitregeln und Berechtigungen direkt auf der Karte speichert, besteht darin, dass es keine **serverbasierte Authentifizierung** oder dauerhafte Serververbindung benötigt. Hier sind die Vorteile:

1. Funktioniert unabhängig von der Netzwerkkonnektivität  
Traditionelle cloudbasierte Zutrittskontrollsysteme erfordern eine stabile **Verbindung** zur Benutzer-Authentifizierung, Berechtigungsüberprüfung und Protokollierung von Zutrittsvorgängen.  
Im Gegensatz dazu arbeitet ein **dezentrales System komplett offline**, sodass Benutzer auch bei **Internetausfall oder Netzwerkunterbrechung** sicheren Zutritt erhalten.
2. Beseitigt Fehlerquellen  
**Cloud-abhängige Systeme bergen das Risiko**, dass bei Ausfall oder Latenz des Cloud-Servers der Zutritt **verzögert oder verweigert** wird.  
Durch die Speicherung der Daten **direkt auf der Karte** sind Benutzer nicht von **Serverausfällen**, Netzwerkausfällen oder Cyberangriffen auf die Cloud-Infrastruktur betroffen.

3. Verbesserter Datenschutz und Datensicherheit  
Cloudbasierte Zutrittssysteme erfordern zentrale Datenspeicherung, was sie zu einem Ziel für Cyberangriffe, Datenlecks oder unbefugten Zugriff macht.
4. Schnellere Authentifizierungszeiten  
Bei der **Authentifizierung** direkt auf der Karte liest das Terminal die Karte **augenblicklich** aus, wodurch **Netzwerklatenz** vermieden und der Zutritt beschleunigt wird.
5. Nahtloser Mehrterminal-Zutritt ohne erneute Registrierung  
Bei zentralisierter oder cloudbasierter Authentifizierung muss jedes Terminal sich mit dem Server **synchronisieren**, um die Benutzerzutrittsdaten zu überprüfen.  
Ein dezentrales System ermöglicht den Terminals im selben Projekt, eine Karte automatisch zu erkennen, ohne dass eine erneute Registrierung oder Datenbanksynchronisation erforderlich ist.

Wichtigste Erkenntnis: Durch die **Speicherung der Zutrittsdaten auf der Karte** wird das System

- **Resilient** - Funktioniert auch bei Ausfall der Cloud
- **Sicher** - Keine zentrale Datenbank, die gehackt werden kann
- **Schnell** - Keine Netzwerklatenz
- **Privat** - Keine Übertragung persönlicher Daten über das Internet
- **Unabhängig** - Keine Anbieterbindung oder Abhängigkeit von Cloud-Diensten.

Dieser Ansatz gewährleistet **maximale Betriebszeit, Zuverlässigkeit und nahtlosen Zutritt über mehrere Terminals** hinweg und ist damit eine überlegene Alternative zu cloudabhängigen Zutrittskontrollsystemen.

## 10.7. Strom- und Anschlussoptionen

Das frogTerminal unterstützt mehrere Strom- und Anschlussoptionen für flexible Installationen:

- Power over Ethernet (PoE): Vereinfacht die Verkabelung und reduziert den Bedarf an separaten Stromversorgungen
- WLAN-Unterstützung: Für Installationen ohne Netzkabel
- 12V DC oder 24V AC: Alternative Stromversorgungen für unterschiedliche Umgebungen

## 10.8. Zeiterfassung und Anwesenheitsmanagement

Das Terminal kann für die Zeiterfassung konfiguriert werden, sodass Benutzer folgende Funktionen nutzen können:

- Ein- und Auschecken für Anwesenheitszwecke
- Pausenzeiten erfassen
- Anwesenheitsdaten in kompatible Systeme wie die ODOO-Datenbank exportieren

## B. Installationsszenarien

### 1. frogTerminal: Erste Schritte

Unser Installationsassistent führt Sie Schritt für Schritt durch die wesentlichen Einstellungen. Dadurch wird eine reibungslose Installation gewährleistet – auch für Anwender mit geringen technischen Vorkenntnissen.

Eine detaillierte Anleitung finden Sie in **Abschnitt 4 des Technischen Installationshandbuchs**.

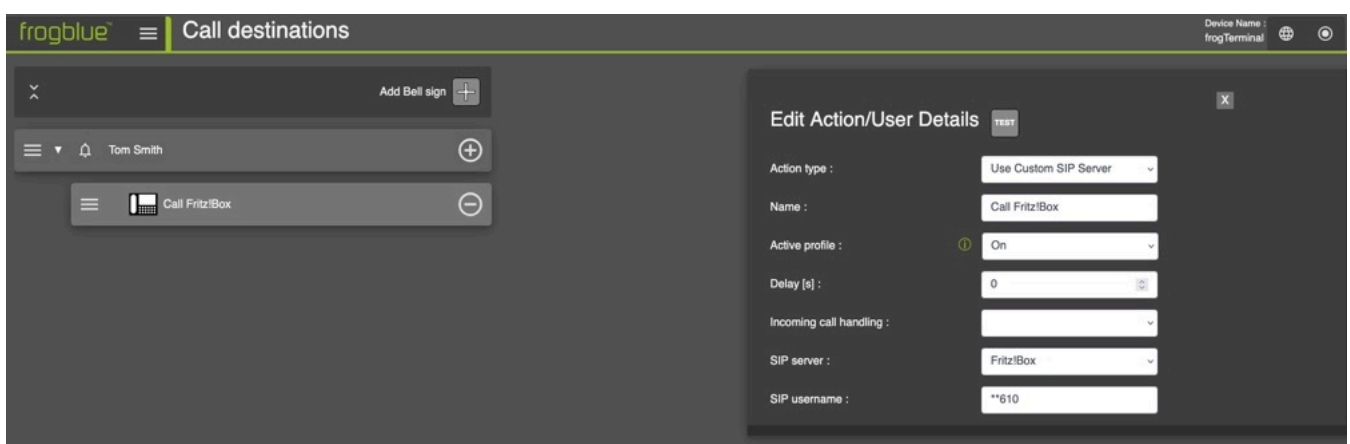
### 2. frogTerminal mit FRITZ!Phone & FRITZ!Box



In diesem Beispiel wird das frogTerminal mit einer FRITZ!Box verbunden. Wird das Klingelschild am frogTerminal gedrückt, klingelt ein mit der FRITZ!Box verbundenes FRITZ!Phone.

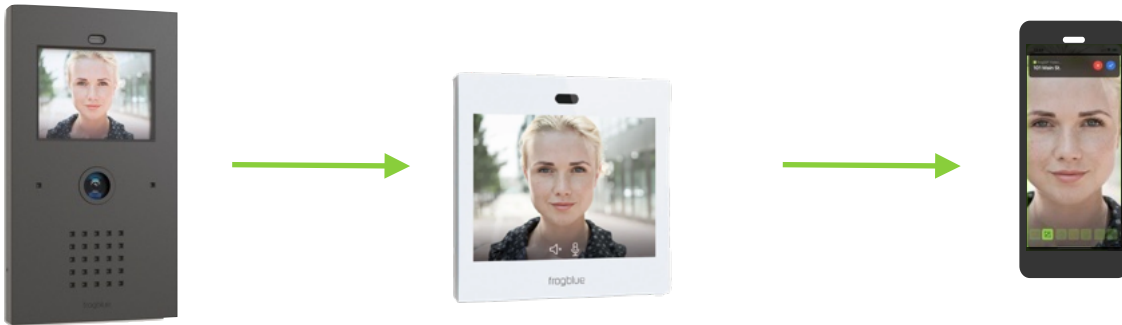
#### Konfigurationsschritte:

- frogTerminal: SIP-Server hinzufügen (**C. Technisches Installationshandbuch, Abschnitt 18.2**)
- frogTerminal: Klingelschild hinzufügen (**C. Technisches Installationshandbuch, Abschnitt 7.1**)
- frogTerminal: Klingelaktion zum Anrufen eines Telefons hinzufügen (**C. Technisches Installationshandbuch, Abschnitt 8.1.1**)
  - **Aktionstyp:** Verwenden Sie Ihren benutzerdefinierten SIP-Server
  - **SIP-Server:** Wählen Sie Ihre FRITZ!Box
  - **SIP-Benutzername:** z.B. „\*\*610“ (interne Nebenstelle der FRITZ!Box)



### 3. Von frogTerminal zu frogDisplay / frogStation

In diesem Szenario klingelt bei Betätigung des Klingelschilds am frogTerminal die frogStation oder das frogDisplay. Wird der Anruf nicht entgegengenommen, wird er an das Smartphone weitergeleitet.

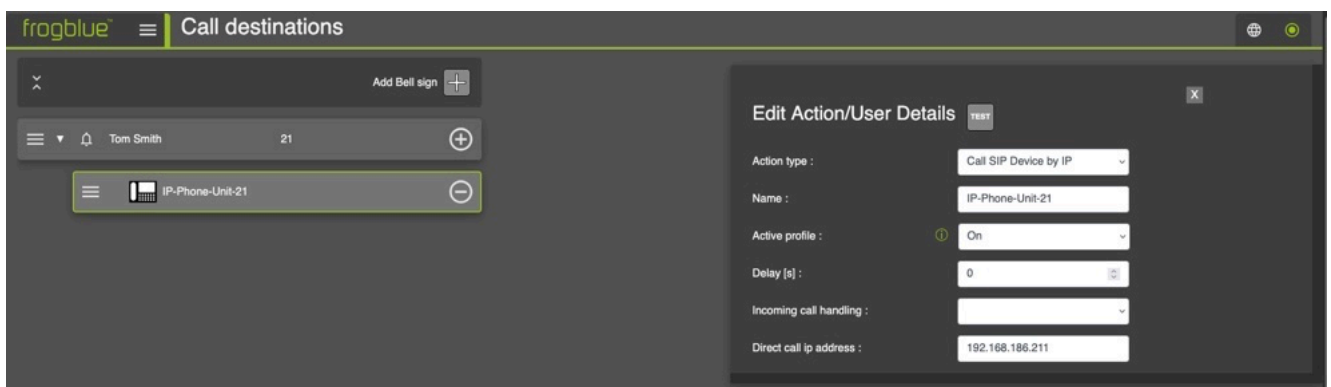


#### Konfigurationsschritte - Kurzübersicht:

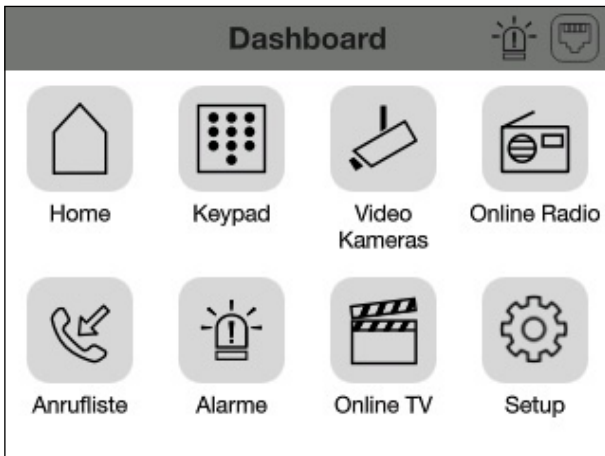
- frogTerminal: Klingelschild hinzufügen (*C. Technisches Installationshandbuch, Abschnitt 8.1*)
- frogTerminal: Klingelaktion zum Anrufen des frogDisplay hinzufügen (*C. Technisches Installationshandbuch, Abschnitt 8.1.3*)
- frogDisplay/frogStation: Siehe Einstellungen des frogDisplay/der frogStation (Schritte unten)
- frogTerminal: Klingelaktion zur Weiterleitung hinzufügen (*C. Technisches Installationshandbuch, Abschnitt 8.1.11*)
- Smartphone mit dem frogTerminal koppeln (*C. Technisches Installationshandbuch, Abschnitt 5.6*)

#### Konfigurationsschritte:

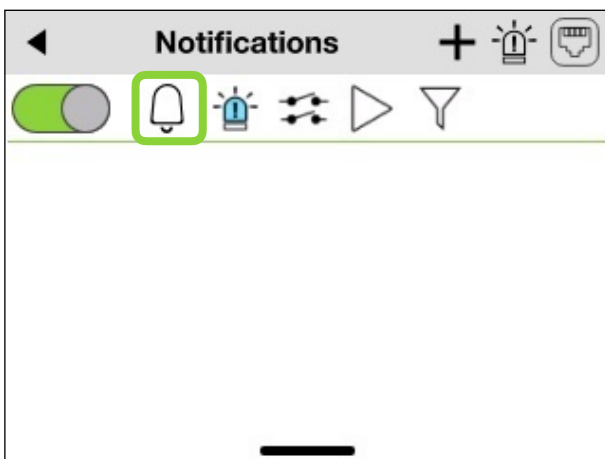
Schritte 1 & 2: Öffnen Sie Ihren Webbrowser und geben Sie die IP-Adresse des Terminals ein, um auf die Konfigurationsoberfläche zuzugreifen. Fügen Sie anschließend ein Klingelschild hinzu und konfigurieren Sie eine Aktion. Tragen Sie im Feld **Direct call IP address** die IP-Adresse Ihres frogDisplay/Ihrer frogStation ein. Siehe dazu *C. Technisches Installationshandbuch, Abschnitte 8.1* und *8.1.3*.



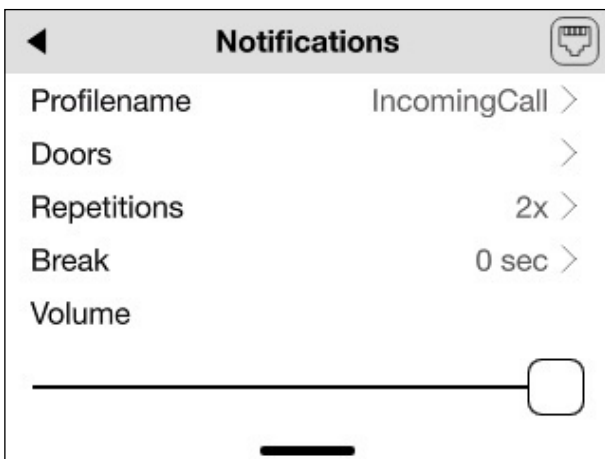
Schritt 3: Einstellungen von frogDisplay / frogStation: Das frogDisplay / die frogStation verwendet die folgenden Standardeinstellungen. Bitte prüfen Sie, ob diese Einstellungen weiterhin Ihrer gewünschten Konfiguration entsprechen:



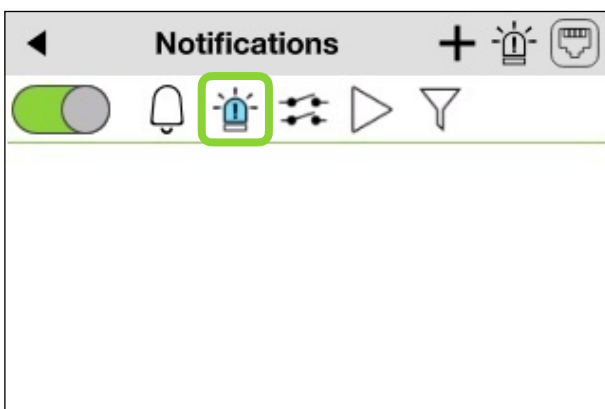
- Wählen Sie auf Ihrem Dashboard **Alarme**.



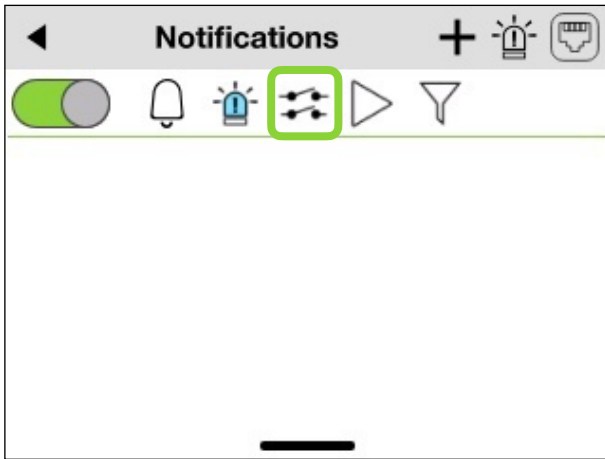
- Wählen Sie das Glocken-Symbol.



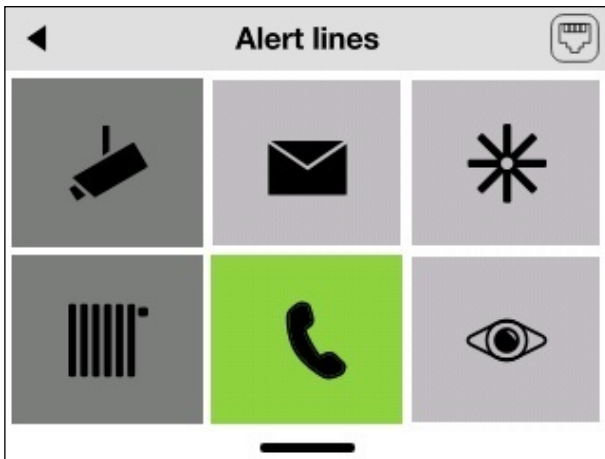
- Vergeben Sie einen Profilnamen.
- Legen Sie die Anzahl der Klingelwiederholungen fest.
- Legen Sie die Länge der Pause zwischen den Klingelsignalen fest.
- Passen Sie die Klingellautstärke an.



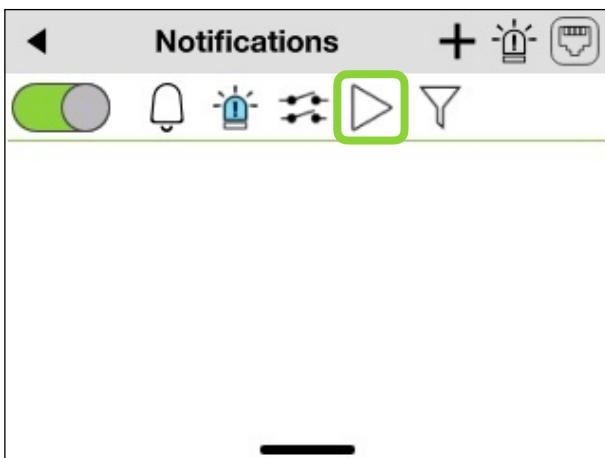
- Stellen Sie sicher, dass der Alarm aktiv ist (Alarm-Symbol muss blau sein).



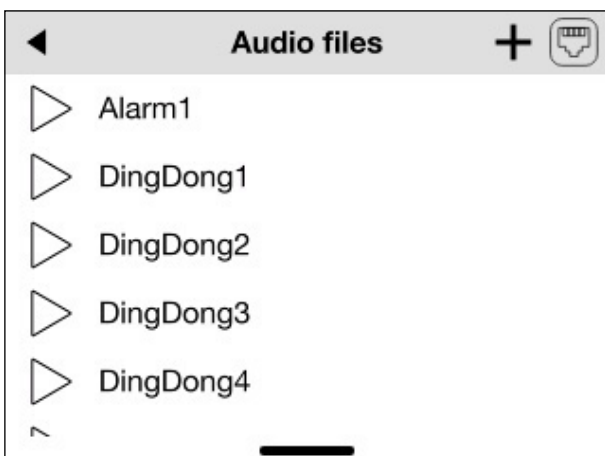
- Klicken Sie auf die Alarmlinien.



- Wischen Sie nach links, um den Telefonhörer auszuwählen.



- Klicken Sie auf das Play-Symbol und halten Sie gedrückt, um einen Klingelton auszuwählen.



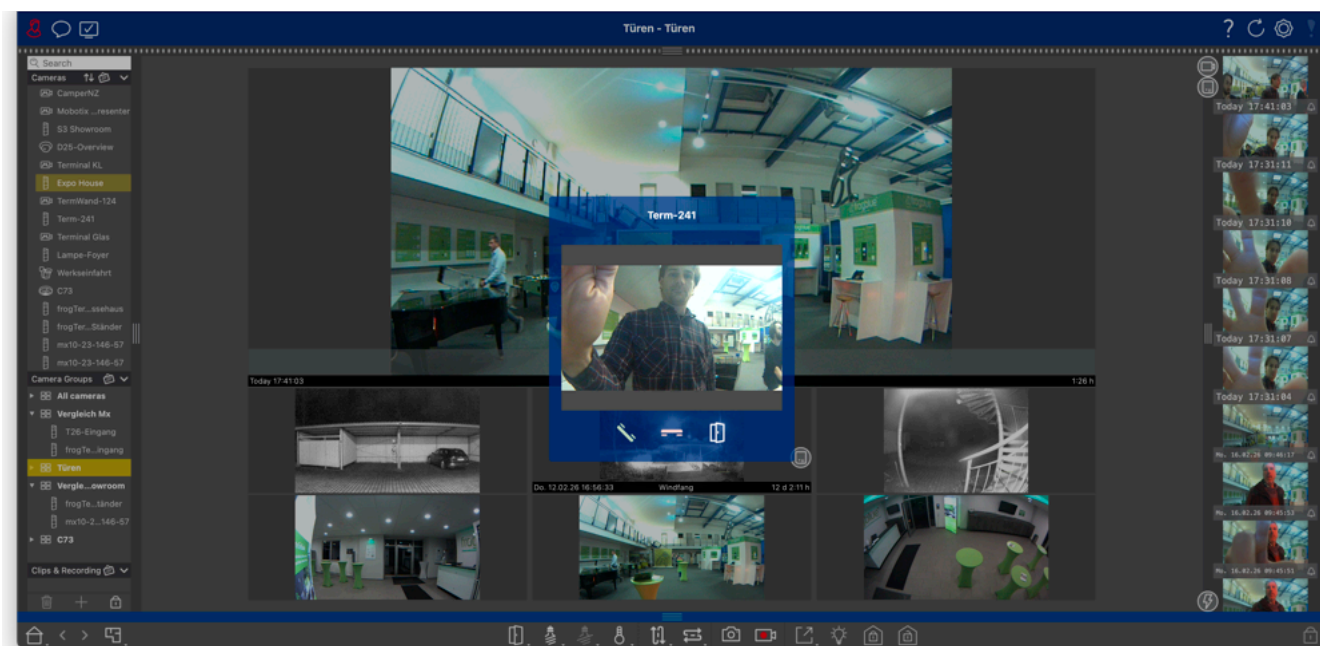
- Klicken Sie auf den Namen des Klingeltons, um diesen auszuwählen. Der Name erscheint dann in grün.

Schritt 4: Führen Sie über die Weboberfläche des Terminals die Schritte zum Hinzufügen einer Klingelaktion zur Weiterleitung durch (**C. Technisches Installationshandbuch, Abschnitt 8.1.11**).

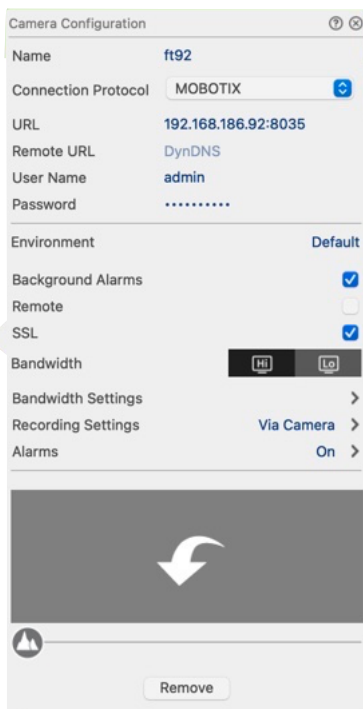
Schritt 5: Um den Anruf an Ihr Smartphone weiterzuleiten, fügen Sie eine zusätzliche Klingelaktion hinzu, indem Sie auf **+** neben dem Kontakt (z. B. „Tom Schmidt“) klicken. Wählen Sie dann den gewünschten **Aktionstyp**: *frogSIP-Kontakt einladen* oder *frogCloud-SIP-Konto anrufen*. Um Ihr Smartphone mit dem frogTerminal zu koppeln, beachten Sie bitte **C. Technisches Installationshandbuch, Abschnitt 5.6**.

## 4. frogTerminal Integration in MOBOTIX Management Center (MxMC)

Das frogTerminal lässt sich über den EventStream auf **Port 8035** in MxMC integrieren.



Um Ihr frogTerminal in MxMC zu integrieren, führen Sie die folgenden Schritte durch:



- Öffnen Sie MxMC und fügen Sie ein neues Gerät hinzu.
- Vergeben Sie einen **Namen** für Ihr Terminal.
- Tragen Sie **Benutzernamen** und **Passwort** ein.
- Aktivieren Sie die Option **Background Alarms** (Events).
- Aktivieren Sie **SSL**, um eine sichere Verbindung zu verwenden.
- Speichern und aktualisieren Sie. Klicken Sie anschließend auf **SSL-Zertifikat vertrauen**.

Weitere Informationen, wie Sie Ihr frogTerminal in MxMC einbinden, finden Sie im **C. Technischen Handbuch, Abschnitt 20.4**.

## 5. Kopplung frogTerminal und KNX

Um Ihr frogTerminal und ein KNX-System zu koppeln, installieren Sie bitte zunächst die aktuellste Version der frogOS Firmware auf Ihrem frogTerminal. Binden Sie weiterhin ein KNX-IP-Gateway in Ihr KNX-Projekt ein. Stellen Sie bitte außerdem sicher, dass sich alle Geräte im selben Netzwerk befinden und das frogTerminal in einem frogProject eingebunden ist.

### Von KNX zu frogTerminal

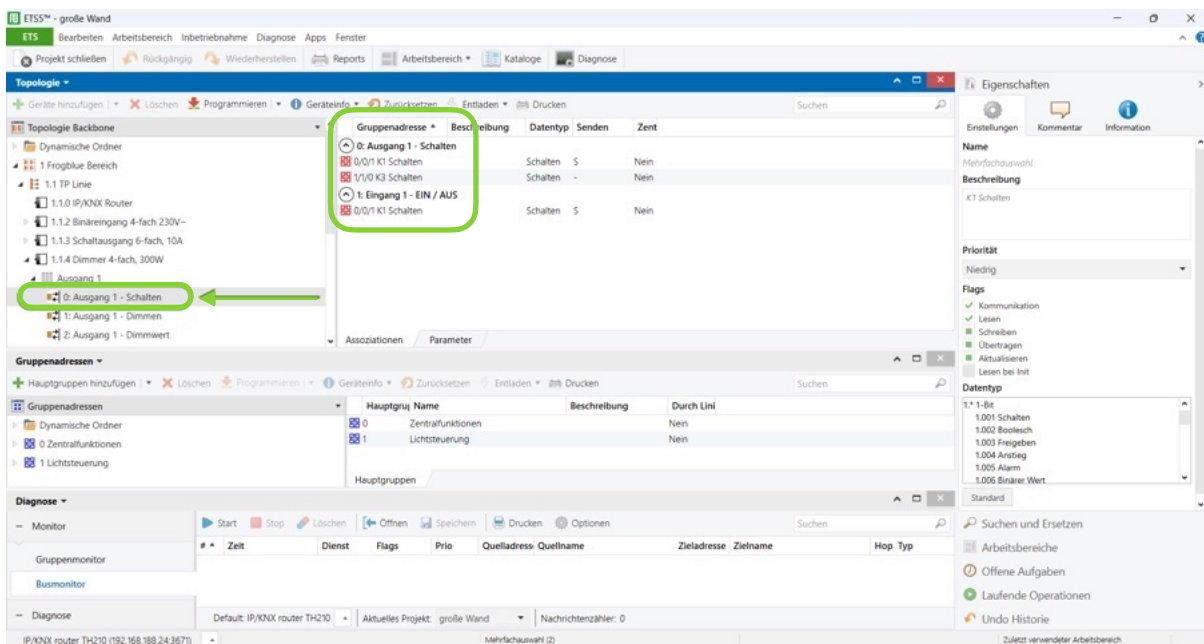
Wenn beispielsweise KNX das Licht an der Haustür steuert, kann, sobald das Licht dort angeschaltet wird, eine frogMessage versendet werden, mit der zusätzlich das Licht im Treppenhaus geschaltet wird.

### Konfigurationsschritte Kurzübersicht:

- KNX-Gruppenadressen auslesen
- KNX-Gruppenadressen in frogblue Ereignismanagement Einfügen.

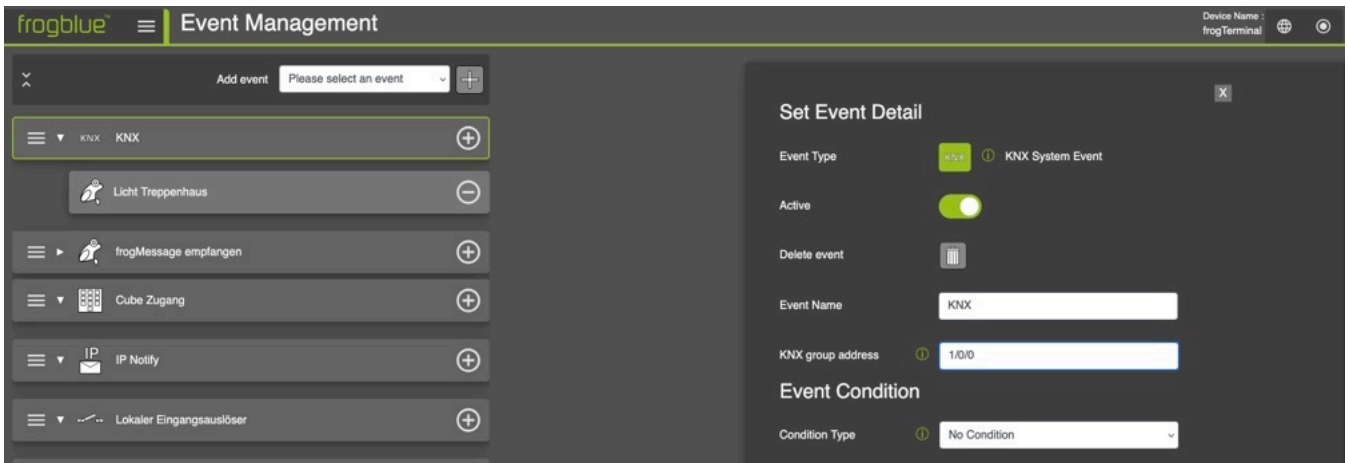
Um die KNX-Gruppenadressen auszulesen, wird hier **ETS** verwendet, die Standard-Software zur Konfiguration von KNX-Gebäudesystemtechnik.

- Starten Sie *ETS* und navigieren Sie zu **Topologie**.
- Wählen Sie in der linken Leiste den zu schaltenden Ausgang (hier: Ausgang 1). Die KNX-Gruppenadressen erscheinen dann in (ETS5 → mittleres Fenster, ETS6 → **rechte Listenansicht**). Wir nutzen hier „1/0/0“.

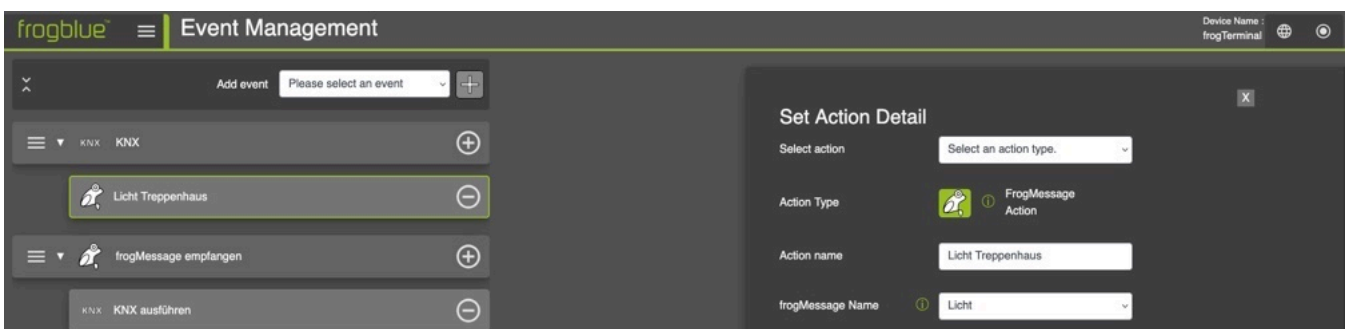


Öffnen Sie Ihren Webbrowser und geben Sie die IP-Adresse des Terminals ein, um auf die Konfigurationsoberfläche zuzugreifen.

- Navigieren Sie zu **Einstellungen** → **Ereignismanagement**
- Fügen Sie ein **KNX-Systemereignis** hinzu: Wählen Sie dazu **KNX-Systemereignis** aus dem Dropdown-Menü und fügen Sie das Ereignis mit einem Klick auf das **+**-Symbol hinzu.
- Als **KNX-Gruppenadresse** verwenden Sie bsw. **1/0/0**.



- Mit einem Klick auf **+**-rechts neben *KNX* fügen Sie eine **FrogMessage Aktion** zum **KNX-Ereignis** hinzu.
- Wählen Sie aus dem Dropdown-Menü bei *frogMessage Name* die entsprechende *frogMessage* aus.

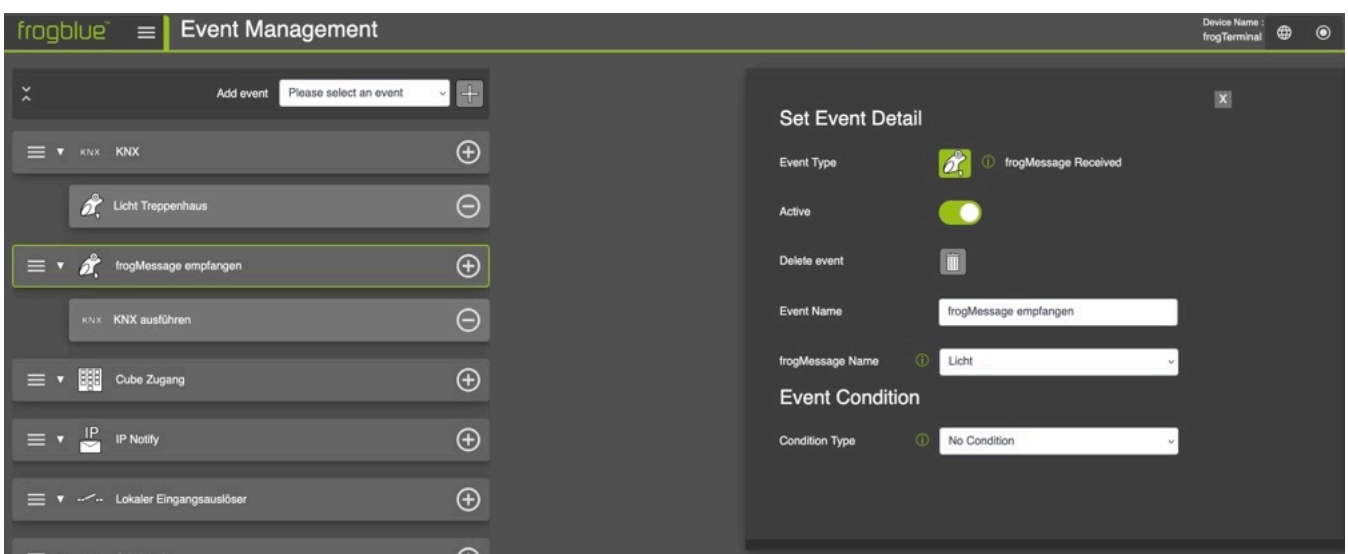


## Von frogTerminal zu KNX

Sie können zum Beispiel mit unserer Multifunktions-Fernbedienung frogKey das KNX-gesteuerte Licht an der Haustür fernsteuern.

### Konfigurationsschritte:

- Im Ereignismanager des frogTerminals das Ereignis *frogMessage empfangen* einrichten



- Eine **KNX Aktion** zum Ereignis hinzufügen.

frogblue **Event Management** Device Name: frogTerminal

Add event  +

- KNX KNX +
- Licht Treppenhaus -
- frogMessage empfangen +
- KNX KNX ausführen** -
- Cube Zugang +
- IP IP Notify +
- Lokaler Eingangsauslöser +
- SIP SIP Anruf +

### Set Action Detail

Select action

Action Type KNX ⓘ KNX Action

Action name

KNX action type ⓘ

KNX group address ⓘ

## C. Technisches Installationshandbuch

---

### 1. Einführung

#### 1.1. Zweck des Handbuchs

Dieses Handbuch liefert Schritt-für-Schritt-Anleitungen zur Installation, Inbetriebnahme und Konfiguration des frogTerminals. Es richtet sich an professionelle Installateure, Systemintegratoren und technische Mitarbeiter, die für die Bereitstellung und Wartung des Systems verantwortlich sind.

Das Handbuch deckt Montage, Verkabelung, Netzwerkeinrichtung, Zutrittskontrolle, SIP-Telefonie, Video- und Aufnahmesteuerung sowie erweiterte Funktionen und Integrationen ab.

#### 1.2. Sicherheit & Konformität

Lesen Sie vor der Installation und Konfiguration des frogTerminals folgende Sicherheitshinweise:

- **Elektrische Sicherheit:** Trennen Sie die Stromversorgung, bevor Sie Verkabelungsarbeiten oder Wartungen durchführen.
- **Sichere Installation:** Verwenden Sie starke Passwörter oder Schlüssel für Administratoren. Stellen Sie sicher, dass beide Seitenschrauben fixiert sind. Ziehen Sie Einbauvarianten in Betracht, um unbefugte Entfernung zu verhindern.
- **Konformität:** Stellen Sie sicher, dass der Installationsort alle lokalen und elektrischen Sicherheitsvorschriften erfüllt.

#### 1.3. Benötigte Werkzeuge & Ausrüstung

Stellen Sie bitte sicher, dass folgende Werkzeuge und Materialien vorhanden sind:

- Bohrmaschine und passende Bohrer für die Montage
- Sicherheitsbit oder Schraubendreher (kann separat bestellt werden – frogTerminal TM-Sec).
- Wasserwaage und Maßstab/Maßband
- Netzkabel (Cat 5e oder höher, wenn Ethernet verwendet wird)
- 8-Pin Phoenix-Steckverbinder für den Netzkabelanschluss (im Lieferumfang enthalten)
- PoE-Switch/Injector oder 12V-24V DC (oder 24V AC) Stromversorgung
- RFID-Schlüssel, -Karten oder -Anhänger zum Testen der Zutrittskontrollfunktionen
- Laptop oder Tablet für die webbasierte Konfiguration
- Tablet (oder Laptop + frogLINK) mit installierter frogProject App zur Konfiguration der Automatisierung via Bluetooth (empfohlen: iPad mit iOS 12.1 oder höher)
- Smartphone oder Gerät mit installierter frogSIP-App zum Testen der Anrufaktionen
- Smartphone oder Gerät mit installierter frogControl-App für Fernsteuerung und Cloud-Automatisierungsfunktionen

**Hinweis:** Ein frogDisplay wird derzeit für die Fernsteuerung via Cloud benötigt, wenn es mit der frogControl-App gekoppelt wird; die lokale Steuerung funktioniert wie gewohnt. Die Terminalunterstützung befindet sich in Entwicklung und wird in einem zukünftigen Software-Update enthalten sein.

## 1.4. Systemübersicht

Das frogTerminal ist ein vernetztes Zutrittskontroll- und Kommunikationsgerät, das SIP-Telefonie, Video-Gegensprechfunktion, kartenbasierte Zutrittskontrolle und Integrationen mit Systemen Dritter vereint.

Zentrale Funktionen umfassen:

- **SIP-Telefonie:** Direktes IP-Anrufen und Mehrfach-SIP-Server-Registrierung für fortschrittliche Mehrparteien-Setups
- **Zutrittskontrolle:** Dezentrales Berechtigungsmanagement mit Verschlüsselung via PINs, Telefon/NFC, RFID
- **Multi-Faktor-Authentifizierung:** RFID, PIN, Telefon, Video-Verifizierung und mehr via Integrationen
- **Mesh-Integration:** Bietet netzwerkunabhängige Kommunikation mittels frogCast®, frogblue's einheitlicher BLE + IP Mesh-Technologie
- **Cloud- & Lokales Management:** Unterstützt den Fernzugriff über die frogCloud sowie den eigenständigen Betrieb für sofortige Redundanz oder vollständig private Setups mit VPN-Unterstützung

## 1.5. Installationsablauf

Installation und Inbetriebnahme des frogTerminals folgen diesen Schritten:

- **Vorbereitende Planung:** Überprüfen Sie den Montageort und die Strom- und Netzwerkanforderungen.
- **Physische Installation:** Montieren Sie das Gerät sicher, schließen Sie Strom und Netzkabel an.
- **Ersteinrichtung:** Verwenden Sie den Touchscreen-Assistenten, um die initialen Admin-Zugangsdaten und Netzwerkeinstellungen zu konfigurieren.
- **Systemkonfiguration:** Richten Sie Zutrittskontrolle, SIP-Telefonie und Integrationen über den Touchscreen oder die Web-Oberfläche ein.
- **Test & Verifikation:** Stellen Sie sicher, dass alle Funktionen, einschließlich Türsteuerung und Gegensprechanlage, korrekt funktionieren.
- **Endgültige Bereitstellung:** Sichern und speichern Sie die Konfigurationseinstellungen und informieren Sie die Endnutzer über die Betriebsanweisungen.

## 1.6. Support & Dokumentation

Für weitere Unterstützung konsultieren Sie bitte:

- Die neuesten Firmware-Updates und Dokumentationen auf [frogblue.com](https://frogblue.com)
- Technischen Support über **autorisierte Partner** oder das nächstgelegene **frogblue KompetenzCenter**
- Online-Fehlerbehebung und FAQs

## 2. Vor-Installationsanforderungen

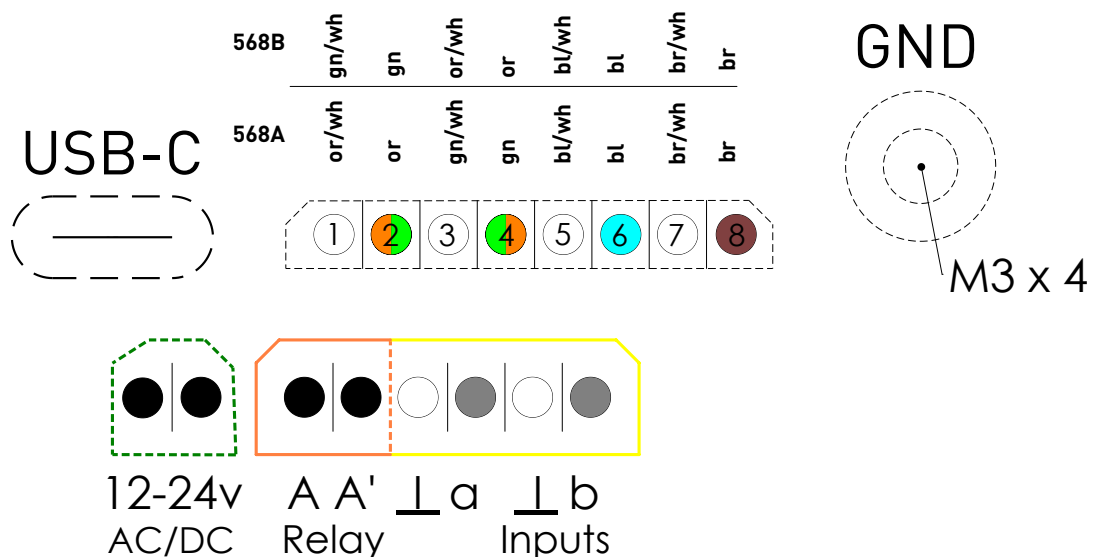
### 2.1. Standortanforderungen

Stellen Sie vor der Installation sicher, dass folgende Bedingungen erfüllt sind:

- **Montagefläche:** Die Fläche muss stabil und für die sichere Montage des frogTerminals geeignet sein.
- **Stromversorgung:** Bestätigen Sie die Verfügbarkeit von PoE (Power over Ethernet) oder einer 12V-24V DC Stromquelle.
- **Netzwerkonnektivität:** Eine stabile Netzwerkverbindung muss via Ethernet oder WLAN verfügbar sein, um die volle Funktionalität zu gewährleisten. Der autonome Betrieb von Automatisierung & Zutrittskontrolle wird jedoch auch ohne Netzwerkverbindung unterstützt.

### 2.2. Strom & Konnektivität

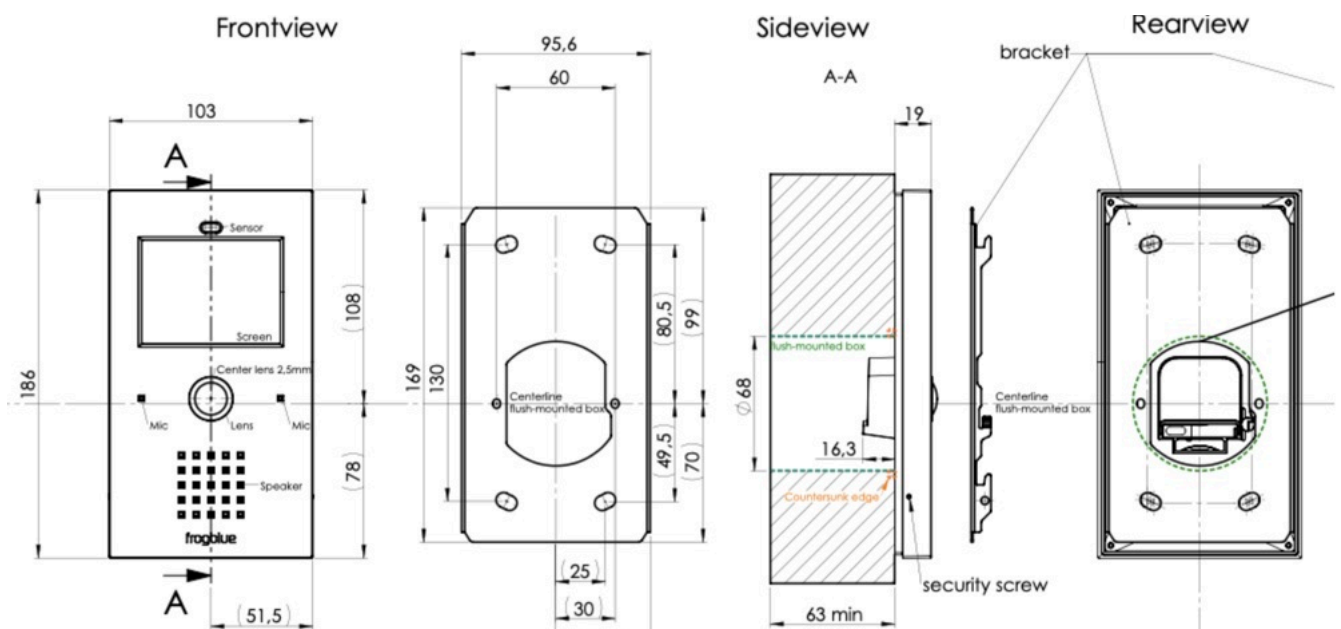
Das frogTerminal unterstützt mehrere Strom-, I/O- und Netzwerkkonfigurationen mit Anschlüssen für Strom, Eingänge, Ausgänge, Netzwerk und zusätzliche Erweiterungsoptionen:



- Stromoptionen:
  - Power over Ethernet (PoE 802.3af, Class 3) über 8-Pin-Steckverbinder (PTSM 0.5/8-P-2.5)
  - 12V-24V DC externe Stromversorgung über 2-Pin-Steckverbinder (PTSM 0.5/2-P-2.5)
  - 24V AC Stromquelle über 2-Pin-Steckverbinder (PTSM 0.5/2-P-2.5)
  - Standby-Verbrauch beträgt ca. 5W
- Netzwerkooptionen:
  - Gigabit Ethernet für kabelgebundene Verbindungen
  - Dual-Band WLAN (2.4 GHz und 5 GHz, 802.11 b/g/n)
  - Bluetooth Mesh für lokale frogblue-Gerätekommunikation, Automatisierung & Zutritt

- Onboard Ein-/Ausgänge:
  - Eingänge: zwei potentialfreie Niederspannungskontakte (Eigenversorgung 2 V / max. 1mA, max. 30W / 50VDC)
  - Relais-Ausgang: ein potentialfreier Relaisausgang (maximale Last: 30 W / 50 VDC)
- Zusätzliche Anschlüsse:
  - M3 x 5 Erdungsschraubenkonnektor: Gewährleistet eine ordnungsgemäße Erdung und Abschirmung des PoE-Kabels
  - USB-C-Port: Reserviert für zukünftige Erweiterungen oder Zubehör
- Anschlussstipps:
  - Schrauben an Ein-/Ausgangsverbindern festziehen, um eine stabile Verbindung sicherzustellen.
  - Stellen Sie sicher, dass die Erdungsschraube verbunden ist, um für Sicherheit und Abschirmung zu sorgen.
  - Ein kleiner Klecks nicht-permanenten Silikonklebers kann an den Seiten der Phoenix-Steckverbinder aufgetragen werden, um diese zu fixieren. Verwenden Sie einen Typ, der für Wartungsarbeiten leicht zu entfernen ist, wie z. B. neutral härtendes Silikon, das das Gehäuse oder die Stecker nicht beschädigt.
  - Für PoE-Setups verwenden Sie einen kompatiblen Netzwerk Switch oder Injector, der dem 802.3af / Class 3 Standard entspricht.

### 2.3. Abmessungen & Gewicht



- Abmessungen (L x B x H): 186 x 103 x 35,3 mm
- Gewicht: 360 g
- Rückwandmodul-Abmessungen: Standard  $\varnothing$  68 mm Durchmesser für Sockel- und Schalterinstallationen (DIN 49073-1 / EN 60670-1). Minimale Tiefe 53 mm für die Montage im Rückwandmodul. Empfohlene Tiefe 63 mm für eine optimale Installation des Rückwandmoduls.

## 2.4. Standortbewertung

Führen Sie vor der Installation eine Standortbewertung durch, um Folgendes zu prüfen:

- Die optimale Montagehöhe für eine einfache Bedienung
- Die beste Methode der Netzwerkverbindung (kabelgebunden vs. kabellos)
- Ausreichende Zugänglichkeit für Wartungsarbeiten
- Die Einhaltung von Sicherheitsvorschriften und Bauordnungen
- Telefonie-Bewertung:
  - Mehrparteien-Setup: Überprüfen Sie die Kommunikationsoptionen (SIP, DECT oder PSTN-Telefonsysteme).
  - Smartphone-Kompatibilität: Bestätigen Sie, dass Smartphones mit der frogSIP-App verfügbar sind.
  - Cloud/Internet-Konnektivität: Stellen Sie sicher, dass für Remote-Telefoniefunktionen eine Verbindung möglich ist, falls erforderlich.

## 2.5. Benötigte Komponenten für die Installation

Stellen Sie sicher, dass alle erforderlichen Komponenten vor der Installation vorhanden sind:

- frogTerminal mit aktueller Firmware oder frogOS-Datei (bereitgestellt auf [frogblue.com](https://frogblue.com) → **Support** → **Software**)
- Montagehalterung und Schrauben (im Lieferumfang enthalten)
- Stromquelle (PoE-Injector, DC-Netzadapter oder AC-Stromanschluss)
- Netzkabel (Cat 5e oder höher für Ethernet-Setups)
- RFID-Karten oder Schlüsselanhänger (falls Zutrittskontrollfunktionen benötigt werden)

## 2.6. Lieferumfang

Für die Modelle frogStation KL, frogTerminal KL, frogTerminal Glas und frogTerminal ALU. Folgende Artikel sind im Lieferumfang enthalten:

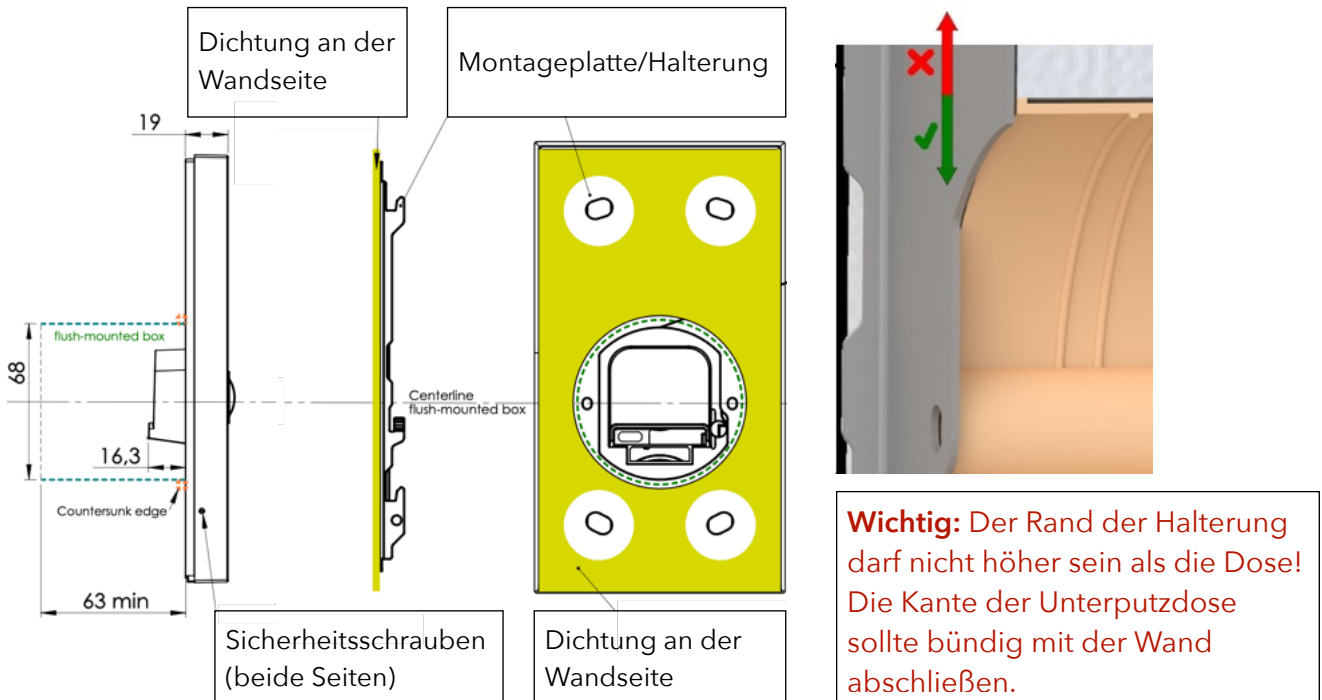
- Paketbeilage-Aufkleber mit Seriennummer, Barcode, Versionsinformation
- frogTerminal, Aluminium-Montageplatte mit angebrachtem Dichtungseinsatz
- 4 × Schrauben (Ø4,5 × 40 mm)
- 4 x Isolationsbefestigungen - Kunststoff-Spreizdübel
- 4 × Dübel (UX6)
- 1,5 mm Inbusschlüssel (für die Verriegelung der Seitenschrauben)
- 2-Pin, 6-Pin und 8-Pin Phoenix-Steckverbinder (für Strom, I/Os und Ethernet)
- 1 x RFID frogblue Karte
- Paketbeilage mit Betriebsanleitung

### 3. Physischer Installationsprozess

#### 3.1. Montage des Geräts

Schritte:

- Montieren Sie das Terminal.
- Schließen Sie die Stromversorgung an (PoE oder extern).
- Verkabeln Sie Eingänge/Ausgänge für Relais oder Taster.



##### 3.1.1. Standardmontage an der Oberfläche

Standard-Schritte für eine an der Wand montierte Installation mit folgenden frogTerminal-Modellen: frogStation KL, frogTerminal KL, frogTerminal Glas und frogTerminal ALU.

- Bereiten Sie eine Aussparung mit einer Mindestdiefe von 53 mm (empfohlen 63 mm) und eine Unterputz-Abzweigdose vor.
- Schrauben Sie die Montageplatte/Halterung mit zwei Schrauben an der UP-Dose fest.
- Richten Sie die Platte aus und markieren Sie die vier Bohrlöcher (verwenden Sie die Löcher als Vorlage).
- Entfernen Sie die Montageplatte/Halterung und bohren Sie die vier Löcher.
- Setzen Sie die Dübel (UX6) ein. Wenn an Dämmmaterial (z. B. Styropor) befestigt, verwenden Sie die mitgelieferten Dämmstoffdübel (größerer Spiraltyp Dübel).
- Befestigen und richten Sie die Montageplatte/Halterung mit den zwei Geräteschrauben (im Lieferumfang enthalten) aus.
- Sichern Sie die Montageplatte/Halterung, indem Sie die vier mitgelieferten Schrauben (Ø4,5 x 40) in die zuvor installierten Dübel (UX6) eindrehen.
- Schließen Sie die Kabel an das Terminal KL an (PoE-Kabel, Erdungsschraube, Strom, Eingänge & Ausgang).

- Stellen Sie eine ordnungsgemäße Erdung sicher (verwenden Sie die zusätzliche Schraube in der Rückwand).
- Setzen Sie das Terminal KL auf die Montageplatte/Halterung und schieben Sie es, bis es einrastet.
- An der linken und rechten Seite der Türstation verwenden Sie den Inbusschlüssel, um die Feststellschrauben anzuziehen, und sichern so die Türstation gegen Diebstahl. Drehen Sie die Schrauben gegen den Uhrzeigersinn, um den Diebstahlschutz zu aktivieren, und im Uhrzeigersinn, um ihn zu deaktivieren.

### 3.1.2. Aufsatzmontage

- Bereiten Sie die Vertiefung in der Wand gemäß den angegebenen Abmessungen vor.
- Setzen Sie die Unterputzdose ein und befestigen Sie sie mit Schrauben.
- Montieren Sie das frogTerminal in die UP-Dose und richten Sie sie korrekt aus.

### 3.2. Anschluss von Strom & Netzwerk

- Falls Power over Ethernet (PoE) verwendet wird, schließen Sie das Ethernet-Kabel an einen PoE-Switch oder Injector an, der den 802.3af/Class 3 Standard erfüllt, und verbinden Sie es mit dem Terminal über den 8-Pin Phoenix-Steckverbinder.
- Bei Verwendung eines 12-24V DC oder 24V AC Netzadapters verbinden Sie die Leitungen über den 2-Pin Phoenix-Steckverbinder mit dem Terminal.
- Überprüfen Sie, ob das Terminal hochfährt und der Start-Assistent oder eine vorkonfigurierte Benutzeroberfläche erscheint, was auf einen ordnungsgemäßen Betrieb hinweist.
- Anlusstipps:
  - Ziehen Sie die Schrauben an den Phoenix-Steckverbindern fest.
  - Ein kleiner Klecks nicht-permanenter Silikonkleber (neutral härtendes Silikon) kann zur Stabilisierung der Stecker angebracht werden.

## 4. Ersteinrichtung & Konfiguration

### On-Device Touchscreen-Installationsassistent

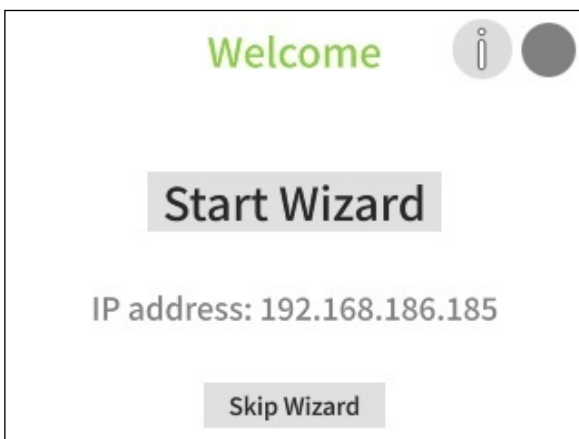
Der On-Device-Assistent vereinfacht die initiale Konfiguration des frogTerminals, indem er Sie schrittweise durch die wesentlichen Einstellungen führt. Dieser Abschnitt sorgt für ein reibungsloses Installationserlebnis, selbst für Benutzer mit geringen technischen Kenntnissen.

Der Assistent kann jederzeit erneut aufgerufen werden, z. B. nach einem Factory Reset. Aktuell in Entwicklung, werden Teile des Assistenten direkt zugänglich sein – sodass Sie spezifische Schritte, wie Cloud-Registrierung, Smartphone-Pairing oder andere wichtige Konfigurationen, wiederholen können.

#### Schrittübersicht:

- Lokalisierungseinstellungen konfigurieren: Sprache, Datum und Uhrzeit
- Die Benutzeroberfläche absichern, indem ein Admin-PIN für die Konfiguration über den Touchscreen und ein Web-Passwort für den Fernzugriff via Browser festgelegt wird
- Netzwerkeinstellungen & frogblue Mesh einrichten
- Das Terminal bei SIP-/Cloud-Diensten registrieren
- Türklingel-Einstellungen konfigurieren
- Die Einrichtung abschließen und das Gerät testen


Um den Installationsassistenten zu starten: Schalten Sie das Gerät ein und tippen Sie auf „Start Wizard“.



- Tippen Sie auf **Start Wizard**.

#### 4.1. Installationsassistent - Schritt 1: Sprache und Zeitzone einstellen



- Tippen Sie auf die Dropdown-Menüs, um Ihre bevorzugte Sprache und Zeitzone auszuwählen.
- Tippen Sie auf .

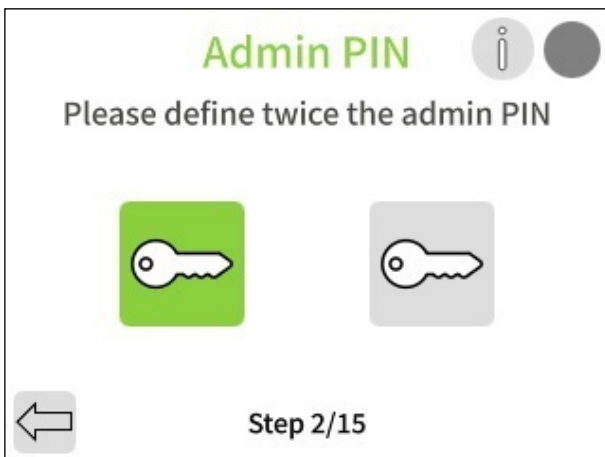
#### 4.2. Installationsassistent - Schritt 2: Admin-PIN festlegen



- Tippen Sie auf das erste Schlüssel-Symbol.



- Geben Sie Ihre gewählte sechsstellige Admin-PIN mittels der Bildschirmtastatur ein und tippen Sie auf **OK**.



- Tippen Sie auf das zweite Schlüssel-Symbol.



- Geben Sie Ihre sechsstellige Admin-PIN nochmals ein und tippen Sie auf **OK**.



- Tippen Sie auf .

#### 4.3. Installationsassistent - Schritt 3: Web-Passwort / HTTPS Admin-Passwort festlegen



- Tippen Sie auf das hellgraue Texteingabefeld *Password* (rechte Seite).



- Geben Sie mit der Bildschirmtastatur Ihr gewähltes Passwort für den Benutzer *admin* ein.

**Hinweis:** Passwörter müssen mindestens acht Zeichen lang sein und mindestens einen Großbuchstaben, einen Kleinbuchstaben und eine Zahl enthalten.



- Tippen Sie auf .

**Hinweis:** Notieren Sie sich Ihr angegebenes Web-Passwort, da es später zur Administration des Terminals über einen Webbrowser benötigt wird.

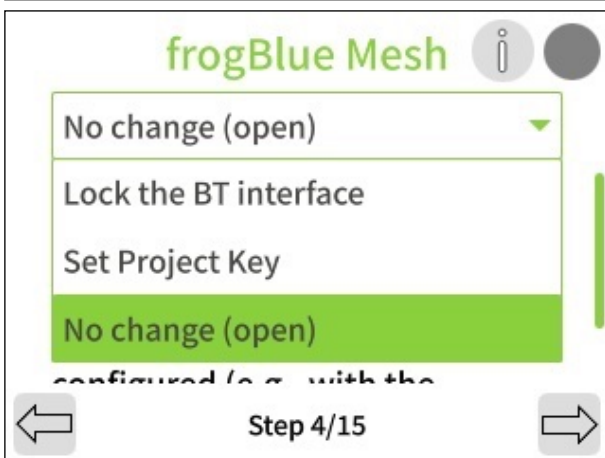
Die werkseitigen Standard-Login-Daten für den Zugriff auf die Kamera via Webbrowser lauten:



- Benutzername: admin
- Passwort: frogblue

#### 4.4. Installationsassistent - Schritt 4: frogblue Mesh Setup



- Tippen Sie auf den Dropdown-Pfeil (▼ oben rechts).



- Wählen Sie die gewünschte Option.
- Tippen Sie entweder auf  oder geben Sie den *Project Key* ein und tippen Sie auf .

**Lock the BT interface:** Das frogblue Mesh ist gesperrt und muss durch einen Factory Reset freigeschaltet werden (siehe [Abschnitt 22.2 „Systemsteuerung - Konfigurationsdateien, Neustart und Werkseinstellungen“](#)).


**Set Project Key:** Das frogblue Mesh ist verschlüsselt und Sie legen im nächsten Schritt den Projekt-Schlüssel fest - frogblue Mesh ist einsatzbereit und das frogTerminal kann in ein Projekt mit diesem spezifizierten Projekt-Schlüssel integriert werden.

**No change (open):** Das frogblue Bluetooth Mesh bleibt offen und unverschlüsselt. Jeder mit der frogProject App oder Konfigurationstools kann das System via Bluetooth in Betrieb nehmen.

**Warnung!:** Bei Auswahl von **No change (open)** bleibt das **System unsicher**, bis die Konfiguration abgeschlossen und das Terminal **in Betrieb** genommen wurde (z. B. mit der **frogProject App**).

#### 4.5. Installationsassistent - Schritt 5: Gerätenamen festlegen




- Tippen Sie in den Textbereich **Main Door** und verwenden Sie die Bildschirmtastatur, um einen Namen für Ihr Terminal einzugeben.
- Tippen Sie auf .

#### 4.6. Installationsassistent - Schritt 6: Startbildschirm-Layout festlegen

Definieren Sie das Layout des Startbildschirms, also die Standardansicht, die angezeigt wird, wenn das Terminal im Standby-Modus ist und per Berührung, Annäherung, Bewegung, Eingabe etc. aktiviert wird.

**Hinweis:** Derzeit in Entwicklung - ein Software-Update befindet sich in Arbeit, durch das der Startbildschirm Optionen zur Anpassung von Bildern, Logos, Stilen, Suchfunktionen und scrollbaren Anruflisten enthalten wird.





- Der Startbildschirm definiert die Standby-Ansicht.
- Tippen Sie, um Ihren Text für jede Zeile festzulegen.
- Tippen Sie auf **Preview**, um Ihre Einrichtung anzusehen.
- Tippen Sie auf , um fortzufahren

Preview-Ansicht:

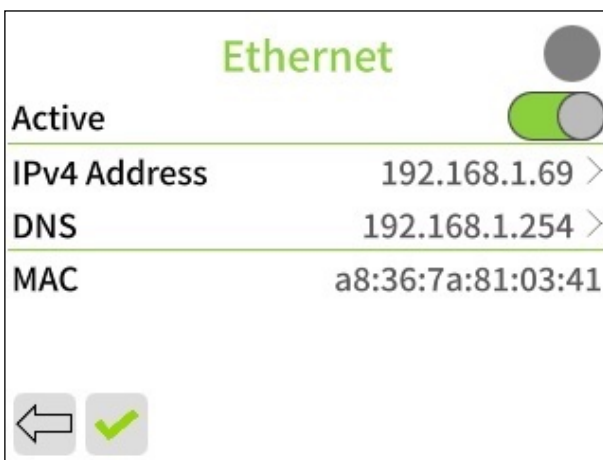




#### 4.7. Installationsassistent - Schritt 7: frogTerminal mit Ihrem Netzwerk verbinden



- Tippen Sie auf die Symbole für Ethernet  und WLAN , um die Einstellungen für die jeweilige Schnittstelle zu konfigurieren.



##### Ethernet-Konfiguration:



- Lassen Sie Ethernet aktiviert oder deaktivieren Sie es über den Umschalter, wenn WLAN verwendet wird.
- Tippen Sie auf die Zeilen, um die IPv4-Adresse oder DNS-Einstellungen zu ändern.
- Tippen Sie auf  oder  zum Speichern der Änderungen und Rückkehr zur Netzwerkeinrichtung.

##### WLAN-Konfiguration:



- Stellen Sie sicher, dass zwei grüne Häkchen  für die Verbindung und frogCloud erscheinen.
- Tippen Sie auf , um fortzufahren.

**Hinweis:** Sollten Verbindungsprobleme auftreten, siehe [Abschnitt 18.1.5 „Fehlersuche bei Netzwerkverbindungsproblemen“](#).

#### 4.8. Installationsassistent - Schritt 8: Verbindung zur frogCloud herstellen

Für eine schnelle und einfache Verbindung mit einem smarten Gerät wird ein frogCloud-Konto empfohlen.

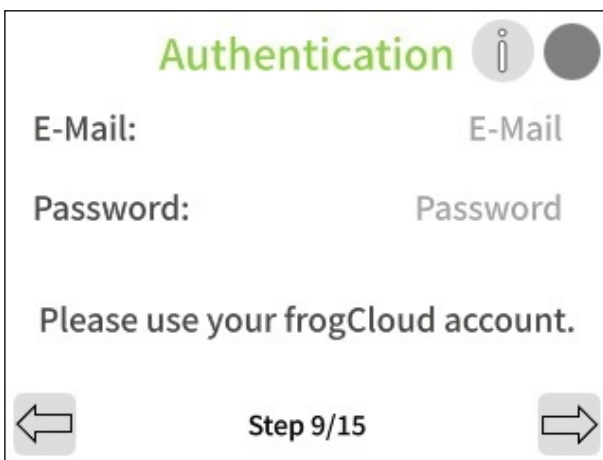



- Um ein bestehendes oder ein neues frogCloud-Projekt für diese Installation hinzuzufügen, tippen Sie auf **Login to frogCloud**.
- Um ein neues frogCloud-Konto zu registrieren und ein neues frogCloud-Projekt zu erstellen, tippen Sie auf **Register a frogCloud account**.
- Um ohne den kostenlosen frogCloud-Dienst mit einem benutzerdefinierten oder erweiterten Setup fortzufahren, tippen Sie auf **Skip frogCloud** und gehen Sie zu **Abschnitt 4.16**.

**Hinweis:** Für frogCloud ist eine bestätigte E-Mail erforderlich. Erstellen und verwalten Sie Konten über die frogSIP-App (iOS/Android) oder unter [frogblue.cloud/login](https://frogblue.cloud/login).

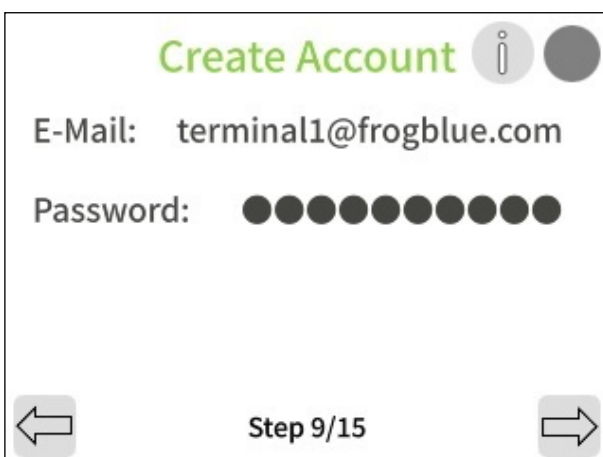
#### 4.9. Installationsassistent - Schritt 9: Login zu oder Registrierung eines frogCloud-Kontos


Login zu einem bestehenden frogCloud-Konto:



- Tippen Sie in die Texteingabefelder **E-Mail** und **Password**.
- Geben Sie mit der Bildschirmtastatur Ihre bestehenden frogCloud-Kontodaten ein.
- Tippen Sie auf , um fortzufahren.

Registrierung für ein neues frogCloud-Konto:




- Tippen Sie in die Texteingabefelder **E-Mail** und **Password**.
- Geben Sie mit der Bildschirmtastatur Ihre E-Mail-Adresse und ein von Ihnen gewähltes Passwort für Ihr frogCloud-Konto ein.
- Tippen Sie auf , um fortzufahren.

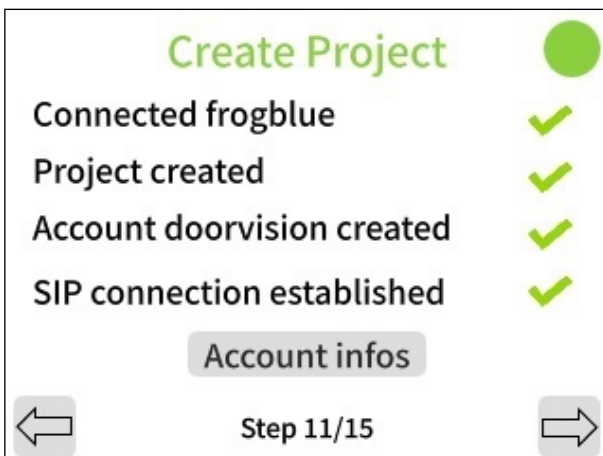
#### 4.10. Installationsassistent - Schritt 10: Bestätigen Sie die Aktivierungs-E-Mail des Kontos


Öffnen Sie Ihr E-Mail-Postfach, klicken Sie auf den bereitgestellten Bestätigungslink und loggen Sie sich mit Ihrer E-Mail und Ihrem Passwort ein, um Ihr frogCloud-Konto mit SIP-Anruffunktionalität zu aktivieren.



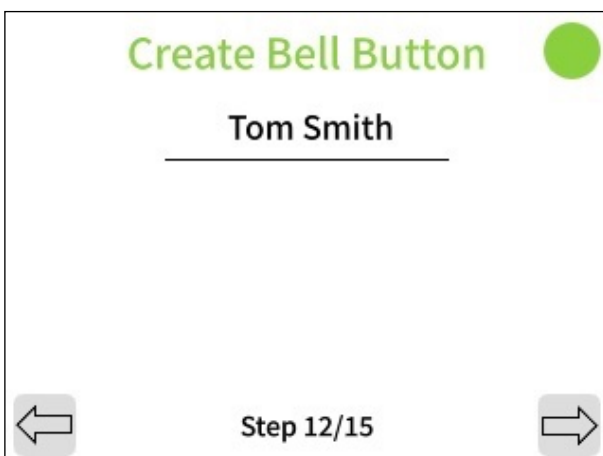
- Warten Sie auf die Bestätigungsmeldung, dass eine E-Mail an Ihre Adresse gesendet wurde.
- Überprüfen Sie Ihre E-Mails, klicken Sie auf den Link und loggen Sie sich dann mit Ihrem Benutzernamen und Passwort ein, um Ihr neues frogCloud-Konto zu aktivieren.
- Tippen Sie auf , um fortzufahren.


#### 4.11. Installationsassistent - Schritt 11: Cloud-Projekt erstellen



- Warten Sie, bis grüne Häkchen für jeden Punkt erscheinen, die Folgendes anzeigen: eine erfolgreiche Verbindung zur frogCloud, die Erstellung des Projekts, sowie des Terminal-SIP-Kontos und eine erfolgreiche SIP-Telefonieverbindung.
- Tippen Sie auf **Account infos**, um erweiterte SIP-Kontodetails anzuzeigen.
- Tippen Sie auf , um fortzufahren.


#### 4.12. Installationsassistent - Schritt 12: Türklingeltasten erstellen



- Tippen Sie auf **Tom Smith** und verwenden Sie die Tastatur, um eine Bezeichnung für Ihre erste Klingeltaste einzugeben.
- Tippen Sie auf , um fortzufahren.

#### 4.13. Installationsassistent - Schritt 13: Mit einem smarten Gerät koppeln







- Verwenden Sie Ihr smartes Gerät mit der frogSIP-App, um den Einladungscode einzugeben oder den QR-Code zu scannen, um die Verbindung mit Ihrem Terminal herzustellen.
- Sobald gekoppelt, können Sie einen Testanruf initiieren, indem Sie auf die Schaltfläche **Testanruf** tippen.
- Wenn Sie fertig sind, tippen Sie auf , um fortzufahren.

#### 4.14. Startansicht und Erklärungen der Anzeigemodi

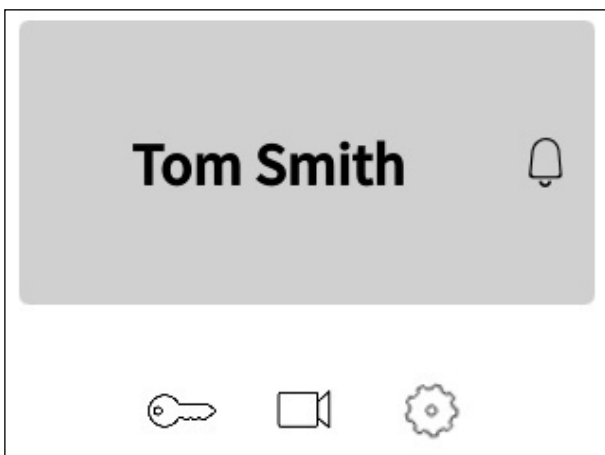
Die Startansicht erscheint, wenn das Terminal durch Annäherungserkennung oder Berührung aktiviert wird. Ansichten bestehen aus einem Hauptbereich und einer Symbolleiste. Das System unterstützt vier Anzeigemodi, wobei die Symbolleiste über den Webbrowser weiter angepasst werden kann.

##### Symbolleisten-Tasten:

-  Ermöglicht die Eingabe von Funktions-PINs
-  Öffnet den Kamera-Dialog. (Siehe **Abschnitt 10 „Kameraeinstellungen und Aufnahmeverwaltung“** für Details zur Konfiguration von In-Stream-Einstellungen)
-  Öffnet die Konfigurations- und Administrationsseiten des Touchscreens.
-  Ermöglicht das Wählen von Wohnungen oder Einheiten. **HINWEIS!** Funktioniert nur, wenn für jeden Anruf-Eintrag im Feld **Apartment** in den **Einstellungen** → **Anrufziele** Nummern definiert wurden.

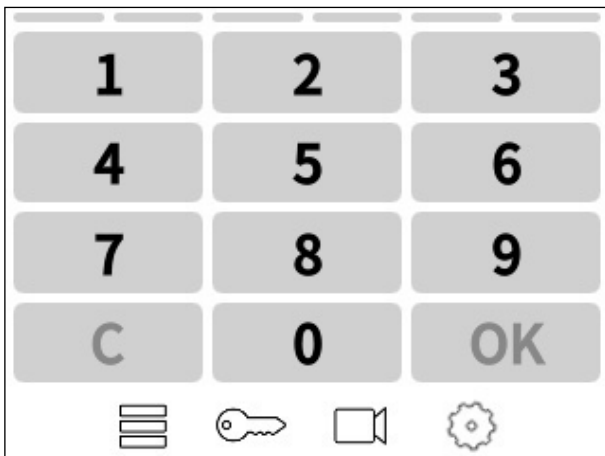
##### Anzeigemodus 1: Klingeltasten („Bell Buttons“)

Diese Ansicht zeigt Klingeltasten im Hauptbereich und drei Symbolleisten-Tasten an.



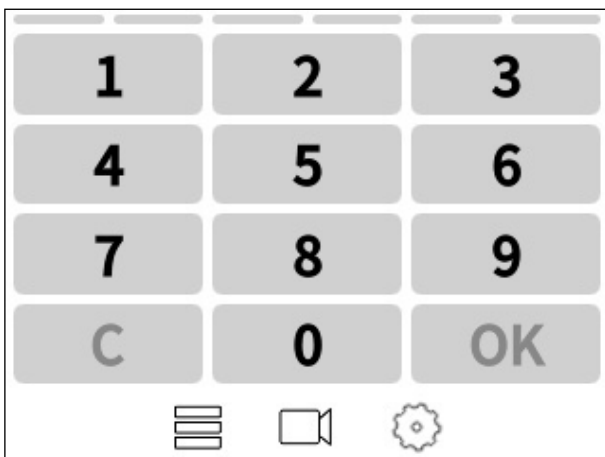
### Anzeigemodus 2: App + PINs

Diese Ansicht ermöglicht die Eingabe von PINs und Wohnungs-/Einheitsnummern im Hauptbereich und zeigt vier Symbolleisten-Tasten an.



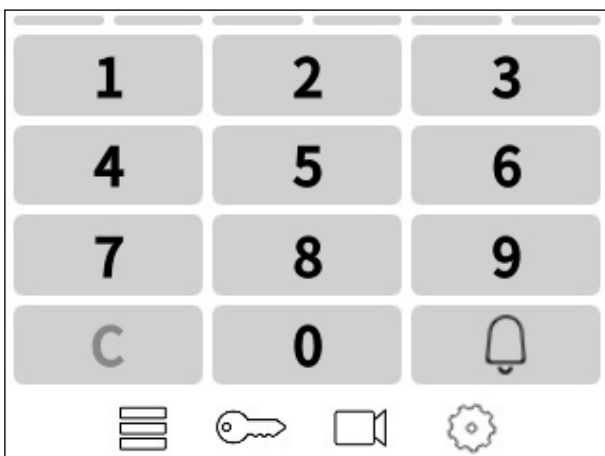
### Anzeigemodus 3: PINs

Diese Ansicht ermöglicht die Eingabe von PINs im Hauptbereich und zeigt drei Symbolleisten-Tasten an.

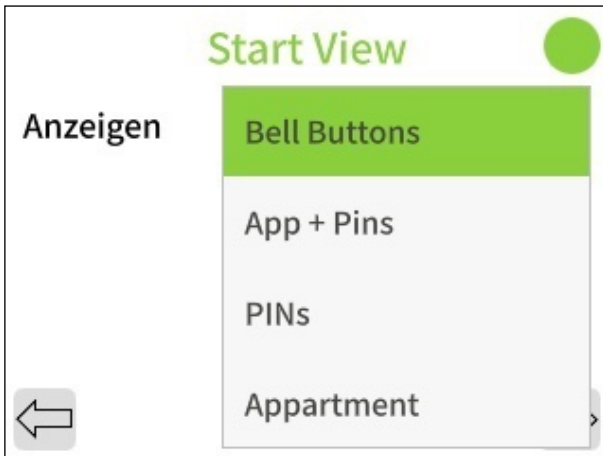



### Anzeigemodus 4: Apartment

Diese Ansicht ermöglicht die Eingabe von Wohnungs-/Einheitsnummern im Hauptbereich und zeigt vier Symbolleisten-Schaltflächen an.




#### 4.15. Installationsassistent - Schritt 14: Startansicht auswählen



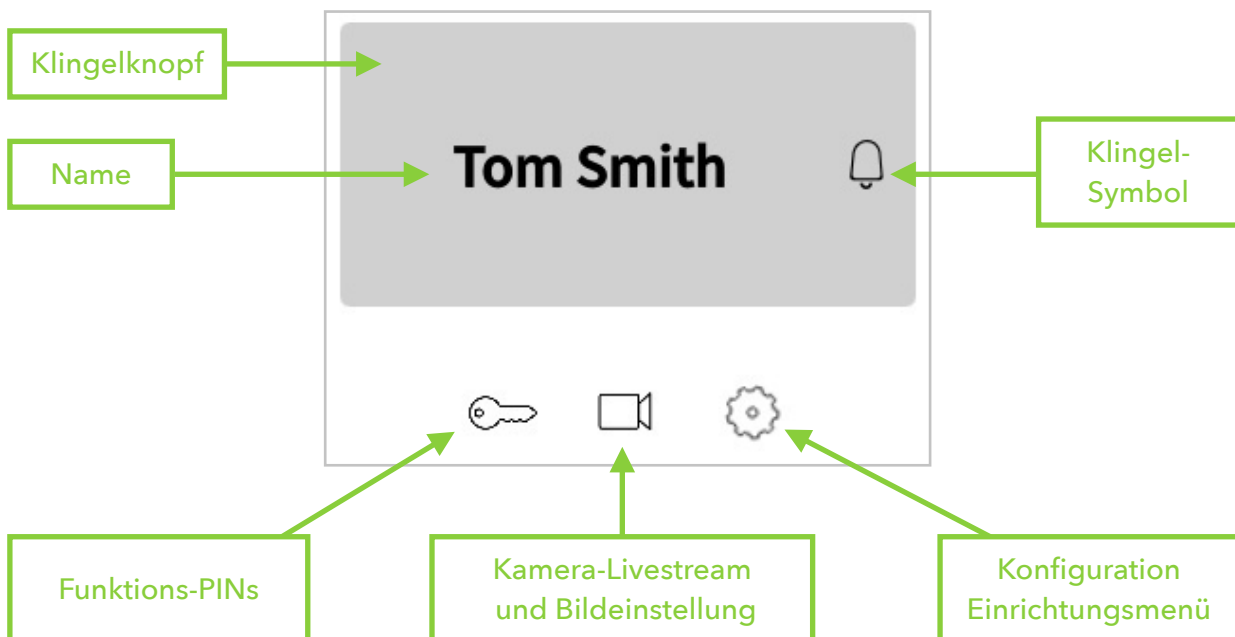
- Wählen Sie Ihre gewünschte Startansicht.
- Tippen Sie auf , um fortzufahren.




#### 4.16. Installationsassistent - Schritt 15: Assistent abschließen



- Fertig! Der Begrüßungsbildschirm erscheint und bestätigt den Abschluss des Assistenten.
- Tippen Sie auf , um fortzufahren.

Assistent abgeschlossen!



Herzlichen Glückwunsch zum Abschluss des frogTerminal Installationsassistenten! Sie können nun Anrufe durch das Drücken der Klingeltaste (z. B. „Tom Smith“) tätigen, Funktions-PINs  auslösen und mittels Admin-PIN auf die On-Screen-Kamera  und Systemeinstellungen  zugreifen.

## 5. frogSIP App Benutzeroberfläche

### 5.1. Einführung in frogSIP

Die frogSIP App dient als primäre Schnittstelle zur Verwaltung und Interaktion mit frogTerminal-Geräten. Dieser Abschnitt bietet eine schrittweise Anleitung zum Koppeln der App mit dem frogTerminal, zur Konfiguration der Benutzereinstellungen, zur Verwaltung von Sicherheitsprotokollen und zur Überprüfung der Anrufliste.

### 5.2. Übersicht des Begrüßungsbildschirms

Beim Start der frogSIP App wird den Benutzern der Begrüßungsbildschirm angezeigt. Die Benutzeroberfläche passt sich automatisch an die Sprache des Smartphones an. Um die Sprache zu ändern, tippen Sie auf das Burger-Menü → **Einstellungen** → **Allgemein** → **Sprache** und wählen Sie die gewünschte Sprache aus.

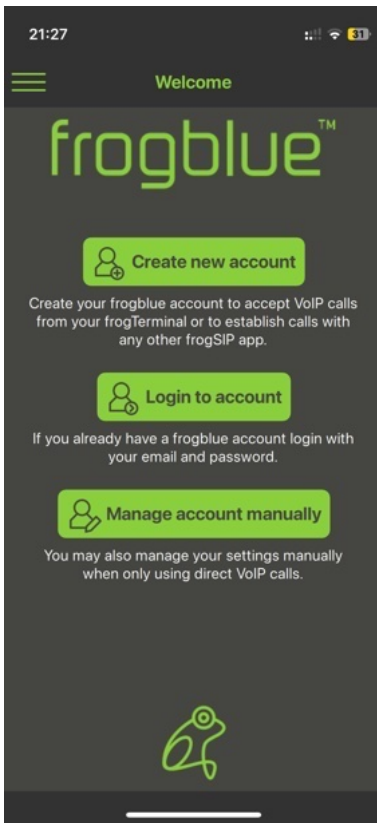


**Hinweis:** Zu Beginn werden wir die **Erstellung und Anmeldung von frogCloud-Konten** behandeln. **Manage account manually** wird für kundenspezifische SIP-Integrationen verwendet und in einem späteren Abschnitt behandelt.

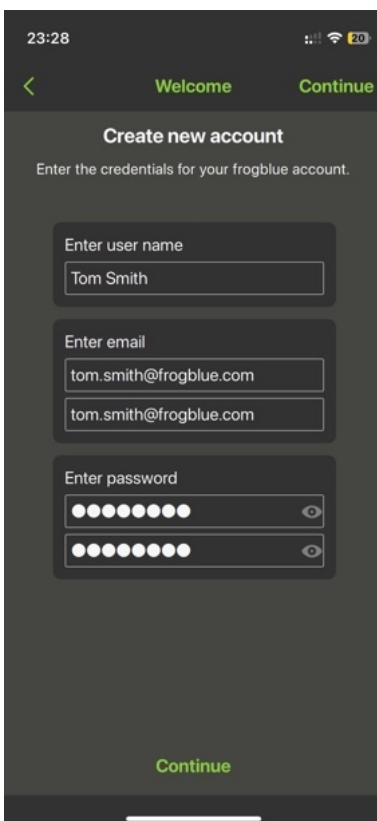
### 5.3. Neues frogCloud-Benutzerkonto über die frogSIP App erstellen

Dieser Abschnitt führt Sie durch die Erstellung eines frogCloud-Kontos über den Begrüßungsbildschirm der frogSIP App.

Wenn Sie den Begrüßungsbildschirm übersprungen haben und zurückkehren möchten, tippen Sie einfach auf das Burger-Menü → **Account** → **Logout** und bestätigen Sie durch erneutes Tippen auf **Logout**.

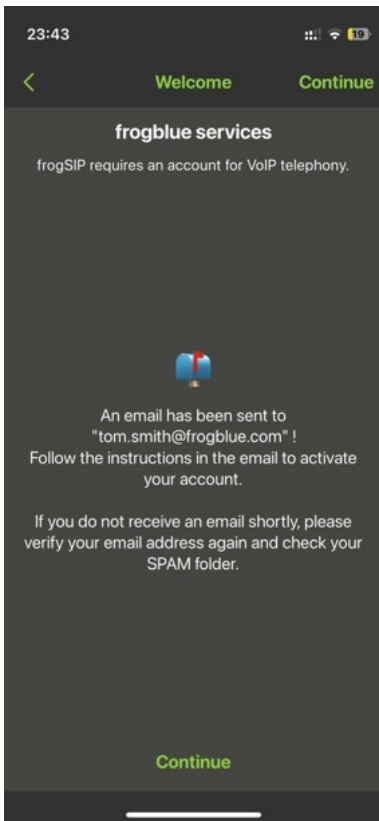


- Tippen Sie auf **Create new account**.

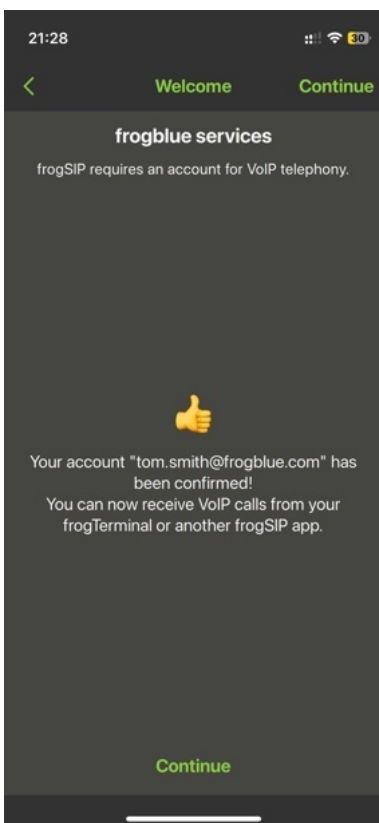


Geben Sie Ihre Informationen ein:

- **User name:** Der Benutzer- und Anzeigename für dieses frogCloud-Benutzerkonto.
- **E-Mail:** Geben Sie die mit diesem frogCloud-Benutzerkonto verbundene E-Mail-Adresse ein und wiederholen Sie diese.
- **Passwort:** Geben Sie das Passwort für dieses frogCloud-Benutzerkonto ein und wiederholen Sie es.
- Tippen Sie auf **Continue**.



- Warten Sie auf die folgende Meldung, die bestätigt, dass eine E-Mail an Ihre Adresse gesendet wurde.
- **Rufen Sie Ihre E-Mails auf** und klicken Sie auf den Link, um den frogCloud-Anmeldebildschirm in Ihrem Webbrowser zu öffnen.
- Melden Sie sich mit Ihrem Benutzernamen und Passwort an, um Ihr neues **frogCloud-Konto zu aktivieren**.
- Tippen Sie auf **Continue**.



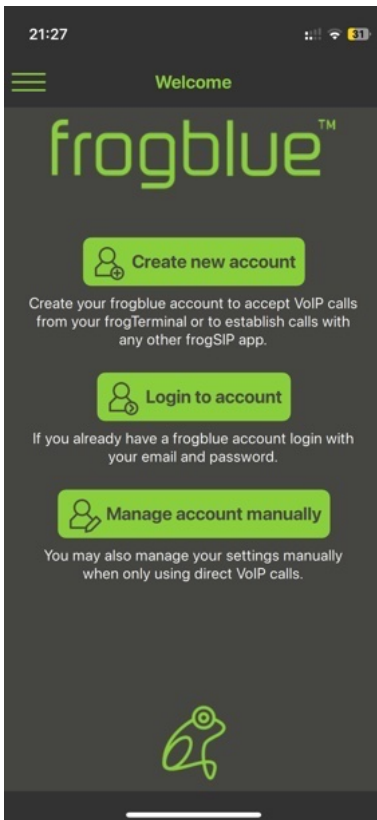
- Warten Sie auf die folgende Meldung, die bestätigt, dass Ihr neues Konto **aktiviert** ist.
- Tippen Sie auf **Continue**.

Falls Sie einen Fehler erhalten, stellen Sie bitte sicher, dass:

1. Ihr **frogTerminal** auf die **neueste frogOS-Version aktualisiert** wurde, erhältlich unter [frogblue.com](http://frogblue.com).
2. Ihre **frogSIP App** ebenfalls auf die **neueste Version** aktualisiert wurde.

#### 5.4. Anmeldung in der frogSIP App mit einem bestehenden frogCloud-Benutzerkonto

Falls Sie bereits angemeldet sind und sich abmelden möchten, tippen Sie auf das Burger-Menü → **Account** → **Logout** und bestätigen Sie durch erneutes Tippen auf **Logout**.

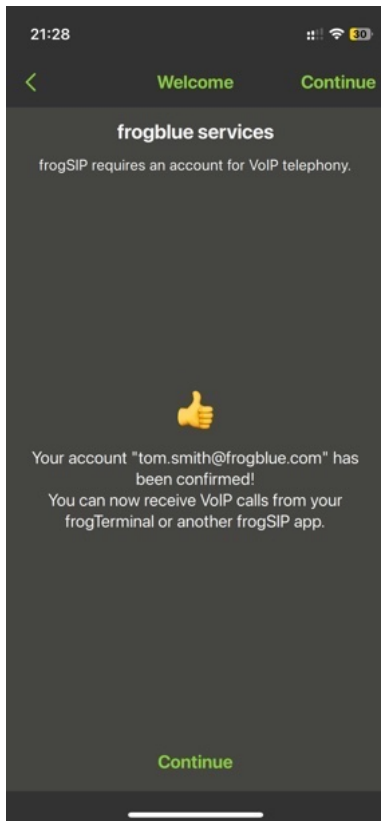


- Tippen Sie auf **Login to account**.



Geben Sie Ihre Informationen ein:

- **E-Mail:** Geben Sie die mit diesem frogCloud-Benutzerkonto verbundene E-Mail-Adresse ein.
- **Passwort:** Geben Sie das Passwort für dieses frogCloud-Benutzerkonto ein.
- Tippen Sie auf **Login**.



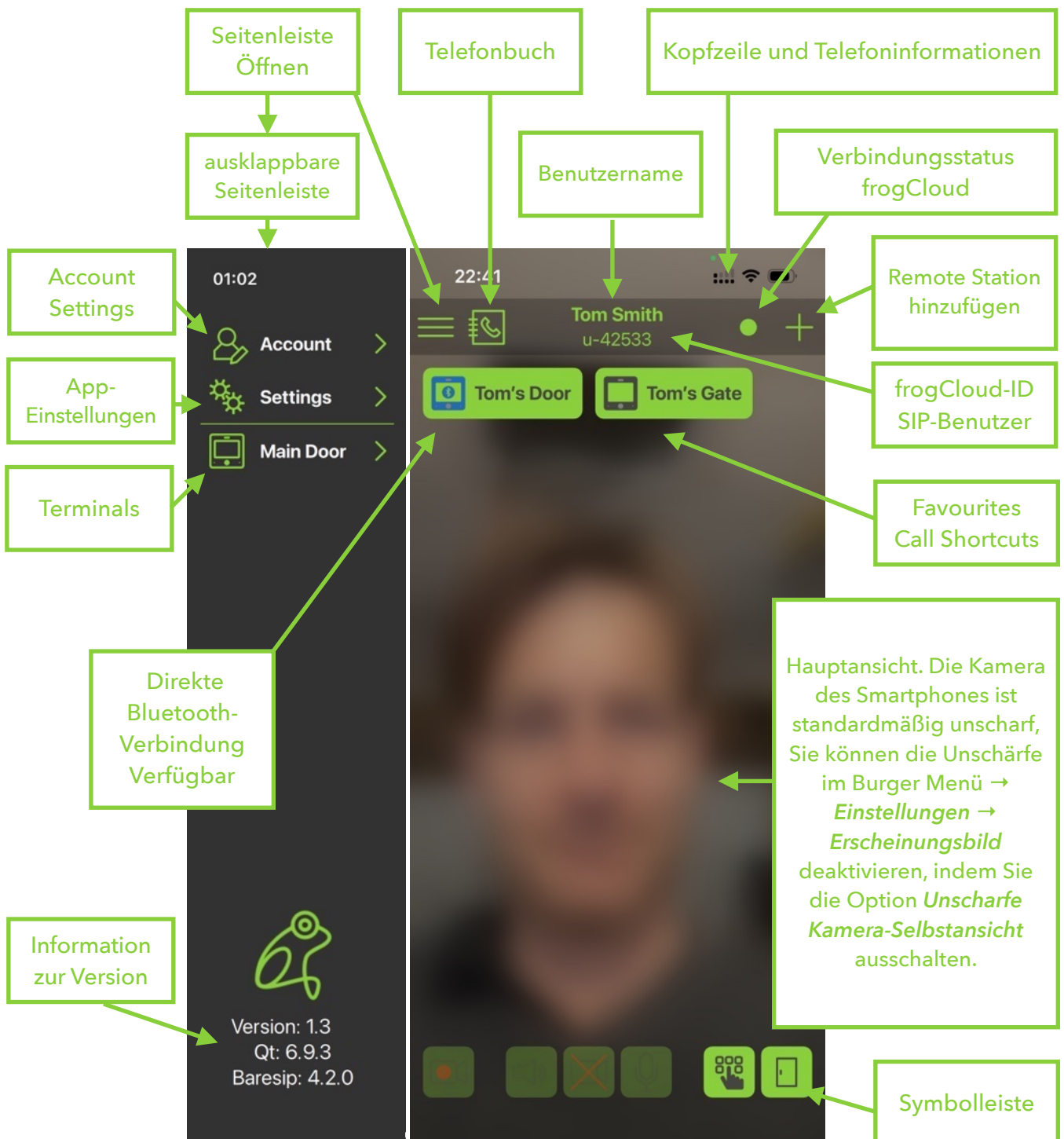
- Warten Sie auf die folgende Meldung, die bestätigt, dass Ihr Konto **aktiviert** wurde.
- Tippen Sie auf **Continue**.

## 5.5. Übersicht der Hauptbenutzeroberfläche der App

Die frogSIP App bietet eine übersichtliche Benutzeroberfläche zur Verwaltung von SIP-basierten Video-Gegensprechanlagen und Zutrittskontrollsystemen. Die Benutzeroberfläche ist auf Effizienz ausgelegt und verfügt über eine ausklappbare Seitenleiste, die schnellen Zugriff auf wichtige Funktionen ermöglicht.

- Touchfreundliches Design für die Nutzung auf Mobilgeräten und Tablets.
- Unterstützung von Dunkel- und Hellmodus für bessere Sichtbarkeit in verschiedenen Umgebungen.
- Mehrsprachige Unterstützung für internationale Einsätze.
- Echtzeit-Benachrichtigungen für Anrufalarme, Zutrittsprotokolle und Systemereignisse.

Die Hauptansicht besteht aus folgenden Abschnitten:

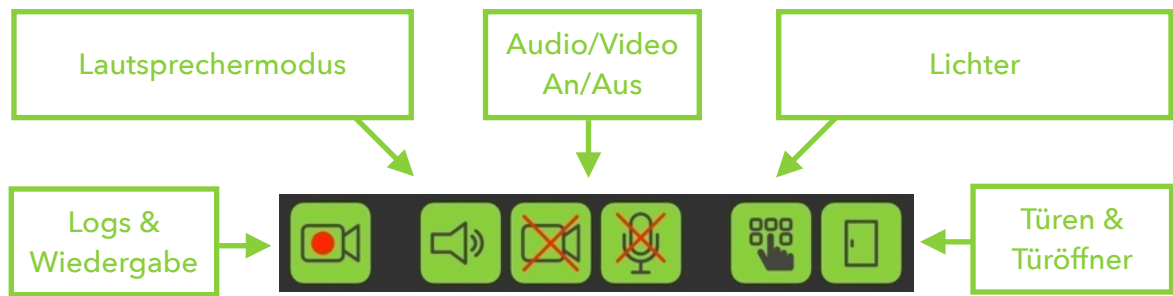


## Details:

- Seitenleiste öffnen (Burger-Menü): Zeigt die ausklappbare Seitenleiste, um schnellen Zugriff auf Konto-, App- und Terminal-Einstellungen zu erhalten.
- **Ausklappbare Seitenleiste:**
  - **Kontoeinstellungen:** Verwalten Sie Ihr frogCloud-Konto.
  - **App-Einstellungen:** Verwalten Sie Benutzer- & Passwort-Einstellungen, melden Sie sich ab oder löschen Sie Ihr Konto.
  - **Terminals:** Zeigen Sie eine Liste der mit der App gekoppelten Terminals an.
  - **Versionsinformationen:** Rufen Sie Details zu den App-Versionen und deren Bundles ab.
- **Telefonverzeichnis:** Rufen Sie schnell beliebige gekoppelte Benutzer oder Geräte über ein Telefonverzeichnis an.
- **Kopfzeile und Telefoninformationen:** Zeigt Standarddetails des iOS-/Android-Geräts an.
- **Benutzername:** Der mit Ihrem frogCloud- oder SIP-Konto verknüpfte Benutzername.
- **frogCloud-Verbindungsstatus:**
  - Undefined (undefiniert)
  - No connection (keine Verbindung)
  - Connected (verbunden)

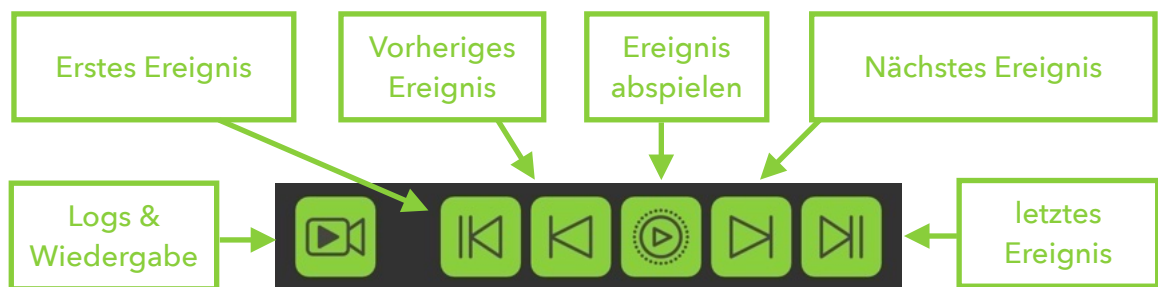
Der Verbindungsstatus-Indikator zeigt die Verbindung zwischen der App und der frogCloud an. Ein grünes Licht bedeutet, dass die Verbindung aktiv ist, Rot weist auf eine fehlende Verbindung hin, und Grau zeigt an, dass die App nicht korrekt konfiguriert ist.
- **Remote Station oder Benutzer hinzufügen:** Fügen Sie schnell eine neue Remote Station oder einen neuen Benutzer hinzu bzw. koppeln Sie diese.
- **frogCloud-ID / SIP-Benutzername:** Ihre frogCloud-ID oder SIP-Autorisierungsbenutzername.
- **Favoriten / Anrufkurzbefehle:** Schnellzugriffstasten zum Anrufen Ihrer Favoriten.
- **Hauptansicht:** Die Smartphone-Kamera ist standardmäßig unscharf, wenn kein Anruf aktiv ist. Um die Unschärfe zu deaktivieren, gehen Sie zu dem Burger-Menü → **Einstellungen** → **Erscheinungsbild** und schalten Sie **Unschärfe Kamera-Selbstansicht** aus.
- **Symbolleiste:** Aktiv während Anrufen mit einem frogTerminal. Zugriff auf Steuerelemente zum Aktivieren/Deaktivieren von Video und Mikrofon sowie zum schnellen Anzeigen von Aufnahmen, Protokollen, Lichtern und Türsteuerungen.

### 5.5.1. In-Call Symbolleiste



- **Logs & Wiedergabe**: Überprüfen Sie Zutritts- und Klingelprotokolle sowie die Wiedergabe von Videoaufnahmen.
- **Lautsprechermodus**: Schaltet den Lautsprechermodus für freihändige Kommunikation während Anrufen an/aus.
- **Audio/Video**: Aktivieren oder deaktivieren Sie die Übertragung von Audio und Video von Ihrem Gerät zum Terminal.
- **Funktions-PINs**: Aktivieren Sie Ihre vordefinierten Funktions-PINs.
- **Türen & Türöffner**: Steuern Sie die Türöffner des Terminals oder von Relais (frogEntry).

### 5.5.2. Logs & Wiedergabe Symbolleiste

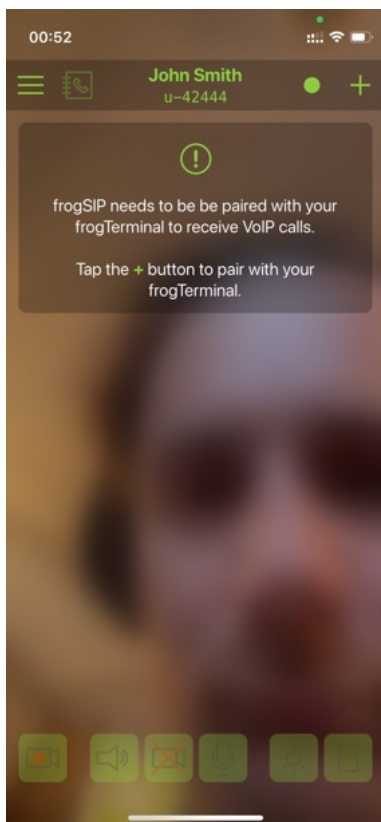


- **Logs & Wiedergabe**: Wechselt zwischen der Research-Player-Ansicht - verwendet für die Wiedergabe von Videoaufnahmen und die Überprüfung von Zutritts- oder Ereignisprotokollen - und der Live-Anruf-Ansicht.
- **Erstes Ereignis**: Springt zum frühesten aufgezeichneten Ereignis im System.
- **Ereignis abspielen**: Spielt die Aufnahme-Sequenz ab, wenn für dieses Ereignis mehr als ein Bild aufgezeichnet wurde.
- **Letztes Ereignis**: Springt zum zuletzt aufgezeichneten Ereignis im System.
- **Nächstes Ereignis**: Springt zum nächsten aufgezeichneten Ereignis im System.
- **Vorheriges Ereignis**: Springt zum vorherigen aufgezeichneten Ereignis im System.

## 5.6. Kopplung des Terminals mit der frogSIP App

In diesem Abschnitt erfahren Sie, wie Sie Ihr Terminal mit der frogSIP App auf Ihrem Smartphone koppeln. Sie können den Kopplungsvorgang entweder durch Eingabe eines Kopplungs-PIN-Codes oder durch Scannen eines QR-Codes über die frogCloud abschließen. Diese sichere Verbindung gewährleistet eine nahtlose Integration, sodass Sie Anrufe effizient verwalten und Einstellungen von Ihrem mobilen Gerät aus konfigurieren können.

Die frogCloud erleichtert das Koppeln und Verbinden mehrerer Standorte und Terminals erheblich.



- Tippen Sie oben rechts auf **+** *Add remote station*.

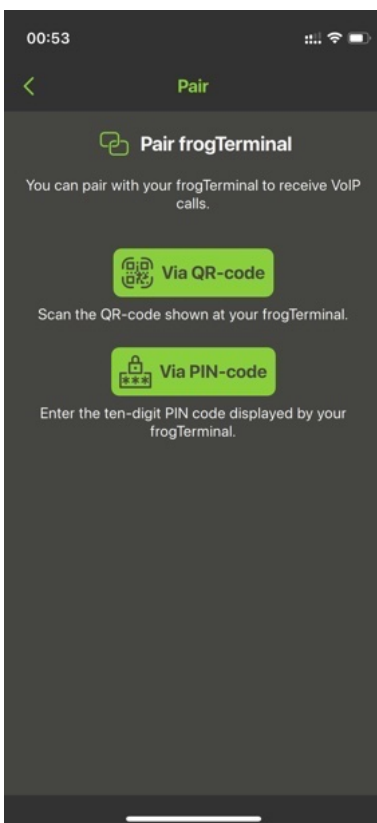


frogSIP kann sowohl mit frogTerminals als auch mit anderen frogSIP-Benutzern für Anruffunktionen verknüpft werden.

Verwenden Sie **Invite frogSIP user**, um sich mit einem anderen App-Benutzer zu verbinden, und **Accept frogSIP Invitation**, um eine Einladung anzunehmen.

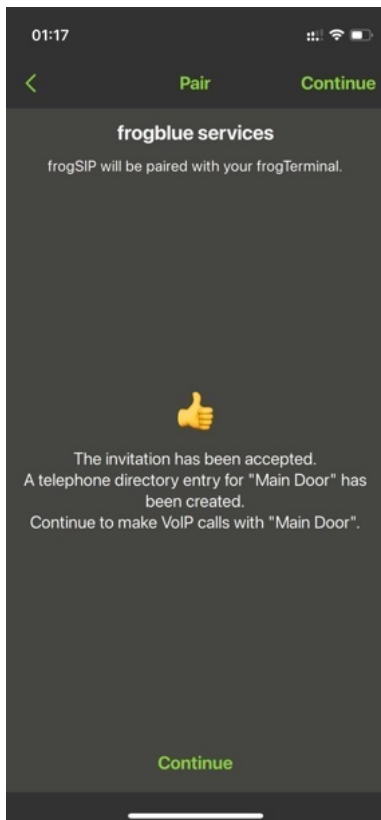
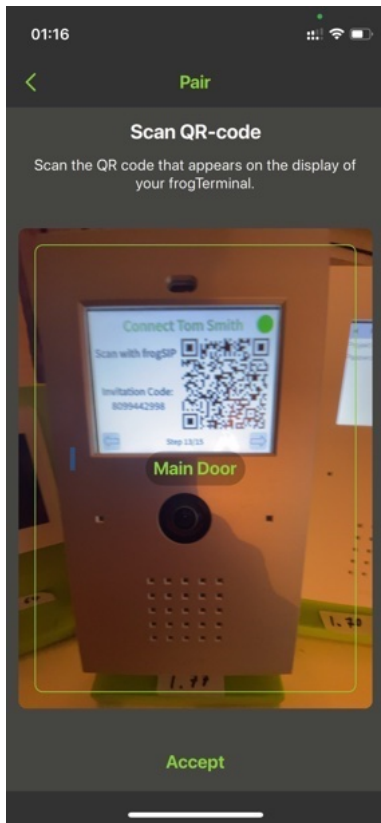
Benutzer können entweder über einen einfachen QR-Code oder über einen Einladungs-PIN-Code verbunden werden.

- Tippen Sie auf **Pair with frogTerminal**, um mit der Verbindung zu Ihrem frogTerminal fortzufahren.



Das Terminal kann auf zwei bequeme Arten gekoppelt werden:

- **Via QR-Code:** Ideal für eine schnelle und einfache Kopplung, wenn sich das Smartphone, auf dem frogSIP läuft, während der Wizard-Einrichtung am selben Ort wie das Terminal befindet.
- **Via PIN-Code:** Perfekt, wenn sich das Smartphone an einem anderen Ort befindet. Senden Sie einfach den Einladungscode an die Person mit dem Smartphone, um den Kopplungsprozess remote abzuschließen.



Verwenden Sie die Kamera Ihres Smartphones, um den auf dem Bildschirm des frogTerminals angezeigten QR-Code zu scannen.

Tipps:

- Sobald der Gerätename auf dem Bildschirm erscheint und die Schaltfläche **Accept** durchgehend grün wird, wurde der QR-Code erfolgreich erkannt. Sie müssen den QR-Code nicht mehr im Kamerarahmen halten und können einfach die Schaltfläche **Accept** drücken.
- Wenn Sie Probleme beim Scannen des QR-Codes haben, halten Sie Ihr Smartphone möglicherweise zu nah oder zu weit entfernt. Passen Sie den Abstand an, indem Sie Ihr Smartphone näher heran- oder weiter wegbewegen. Der ideale Abstand ist in der Regel erreicht, wenn der gesamte frogTerminal-Bildschirm in Ihren Kamerarahmen passt.
- Wenn Sie sich mit einem Einladungs-PIN-Code koppeln, geben Sie einfach den Code ein und tippen Sie auf **Continue**.
- **Bitte beachten Sie:** Der QR-Code ist nur einmal gültig und läuft nach 72 Stunden ab.

Wenn Sie die Meldung "The invitation has been accepted ..." sehen, wurden Ihr Terminal und die frogSIP-App erfolgreich gekoppelt. Sie können nun auf **Continue** tippen.

Wenn Sie eine Fehlermeldung erhalten, wie z. B. „The invitation code is not valid for this version! ...“, stellen Sie Folgendes sicher:

1. Ihr **frogTerminal** wurde auf die neueste frogOS-Version **aktualisiert**, erhältlich bei [frogblue.com](http://frogblue.com).
2. Ihre **frogSIP-App** wurde ebenfalls auf die neueste Version **aktualisiert**.

Gerätespezifische Einstellungen wie Gerätename, SIP-Adresse, Admin-Passwort, Mieterpasswort, Favoritenstatus oder das Entfernen des Geräts können unter Bürger-Menü → Einstellungen → Geräte → frogTerminals → <Ihr frogTerminal> verwaltet werden. Siehe **Abschnitt 5.8 „Terminal-Geräteeinstellungen“**.

Benutzerspezifische Terminal-Funktionen, wie z. B. Klingeltastennamen, Zugangs-PINs, Zeitpläne und Türöffner-Funktionen, werden separat in **Abschnitt 5.9 „Terminal-Nutzereinstellungen“** beschrieben.

## 5.7. Anrufe und Wiedergabe mit dem frogTerminal

In diesem Abschnitt wird erklärt, wie Sie frogSIP mit Ihrem frogTerminal für Anrufe, Wiedergabe und die Ereignisübersicht verwenden. Er behandelt das Empfangen und Starten von Anrufen, den Zugriff auf Aufzeichnungen sowie die Überprüfung von Zugriffs- oder Ereignisprotokollen.

### 5.7.1. Empfang von Anrufen

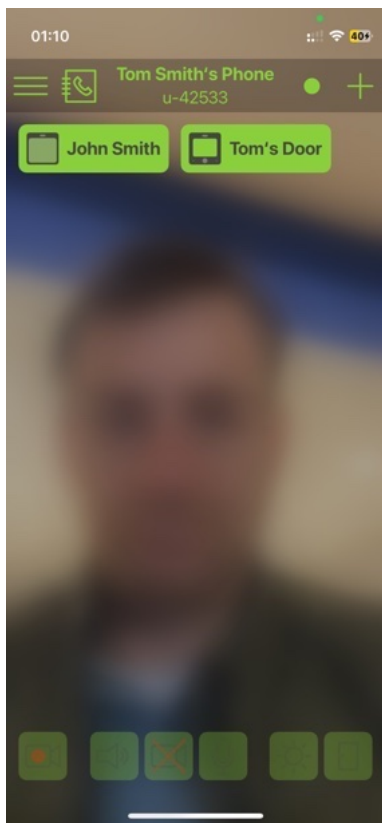
Anrufe entgegenzunehmen ist so einfach wie einen Telefonanruf zu beantworten. Nachdem die Kopplung mit dem Wizard erfolgt ist, funktionieren Anrufe an Ihr Smartphone automatisch. Für weitere Konfigurationen siehe **Abschnitt 8, „Anrufziele einrichten“**. Anrufe können über frogSIP oder von einer frogStation, einem frogDisplay, einem SIP-Telefon oder selbstverständlich einem anderen frogTerminal empfangen werden.

Sobald der Anruf verbunden ist, ist die Benutzeroberfläche identisch mit der der initiierten Anrufe – die folgenden Abschnitte erläutern die Benutzeroberfläche für sowohl initiierte als auch empfangene Anrufe.

### 5.7.2. Automatische Anrufannahme-Konfiguration

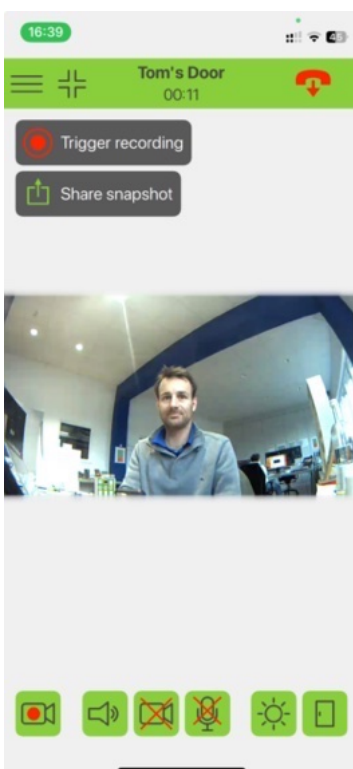
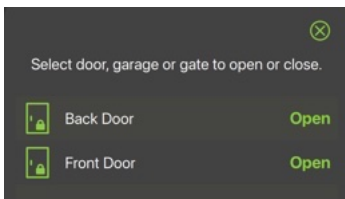
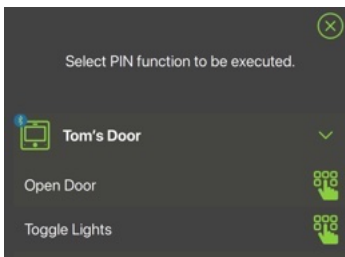
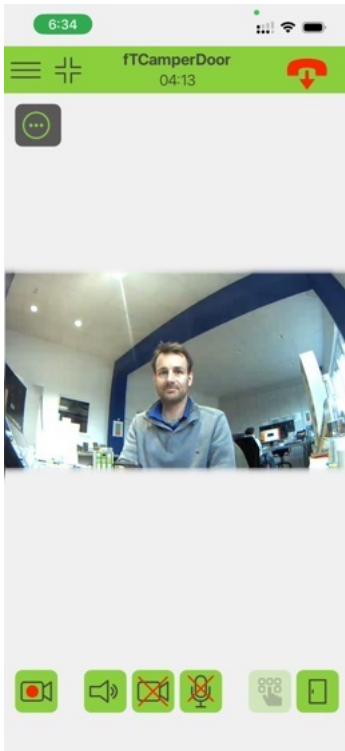
Damit das frogTerminal automatisch Anrufe von autorisierten Benutzern annimmt, stellen Sie sicher, dass das automatische Annehmen für Benutzer unter Web → **Einstellungen** → **Allgemein** auf **Automatische Anrufannahme** eingestellt ist. Zusätzlich können Benutzer auf reine Audio- oder volle Audio-/Video-Zugriffe über Web → **Anrufziele** → **Klingelsignale** eingeschränkt werden.







### 5.7.3. Anrufe initiieren



- Tippen Sie auf das **Telefonbuch** oder wählen Sie einen Eintrag aus Ihren **Favoriten**, um einen Anruf mit Ihrem frogTerminal zu initiieren.


Sobald ein Anruf verbunden ist, erscheint die Symbolleiste. Um den Video-Stream vor dem Verbindungsaufbau zu aktivieren, gehen Sie zu Burger-Menü → **Einstellungen** → **Video** und schalten Sie **Allow early video** ein. Diese Einstellung ermöglicht es Ihnen, Ihren Video-Stream vor dem Anruf zu aktivieren.



-  Blendet die Werkzeugleiste aus, um mehr Platz für den Videoanruf zu schaffen.
-  Startet eine manuelle Aufzeichnung während des Anrufs.
-  Beendet den Anruf.
-  Öffnet das Schnellmenü, um ein Bild aufzunehmen oder eine Aufzeichnung während des Anrufs zu starten.
-  Öffnet das Funktions-PINs-Schnellmenü.
-  Öffnet die Tür - wenn mehrere Türen, Tore oder Garagen konfiguriert sind, erscheint ein Auswahl-Dialog.

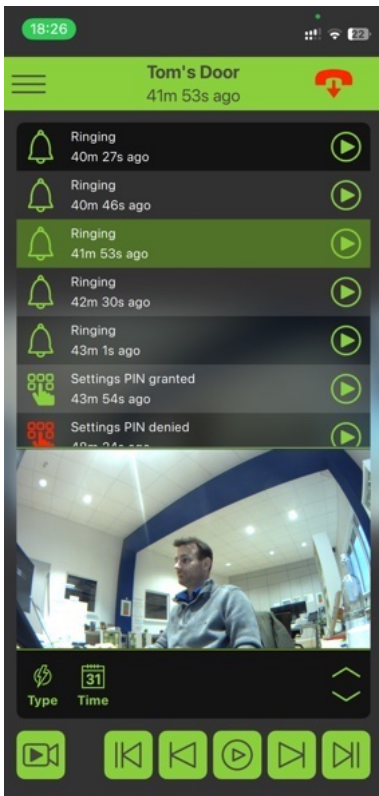
Die verfügbaren Funktions-PINs werden zur Ausführung aufgelistet. Wenn der Benutzer über die erforderlichen Berechtigungen verfügt und das Administratorkennwort festgelegt wurde, können diese Funktionen sofort und ohne Eingabe der entsprechenden PIN ausgelöst werden.

Wenn mehrere Türen, Tore oder Garagen konfiguriert sind, wird dieser Auswahl-Dialog angezeigt. Er zeigt die verfügbaren Einträge und deren aktuellen Status. Wählen Sie den gewünschten Eintrag aus, um ihn zu öffnen oder zu schließen.

Um ein Bild aufzunehmen oder eine Aufnahme während eines Anrufs auszulösen, tippen Sie  um die folgenden Optionen zu sehen.

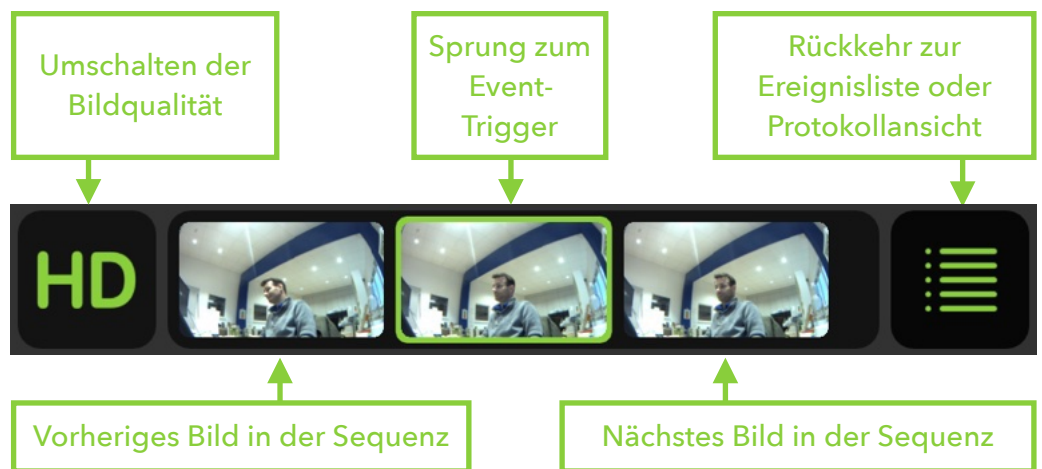
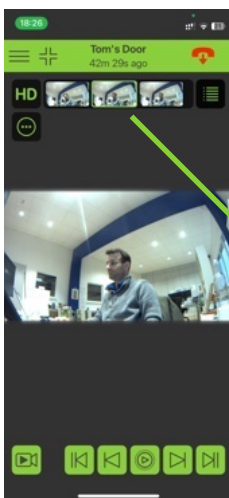
- **Trigger recording:** Löst eine Aufnahme über das Benutzerklick-Ereignis im frogTerminal aus. Startet manuell die Aufnahme eines Ereignisses. Gehen Sie zu **Settings** → **Recording**, um die Aufnahmeeinstellungen zu prüfen und zu ändern.
- **Share snapshot:** Nehmen Sie ein aktuelles Standbild vom Terminal auf und teilen Sie es über die Freigabeoptionen Ihres Smartphones.

## 5.7.4. Zutritts- & Ereignisprotokolle und Wiedergabe eines frogSIP-Anrufs



Tippen Sie auf den Button **Logs und Wiedergabe** (unten links).

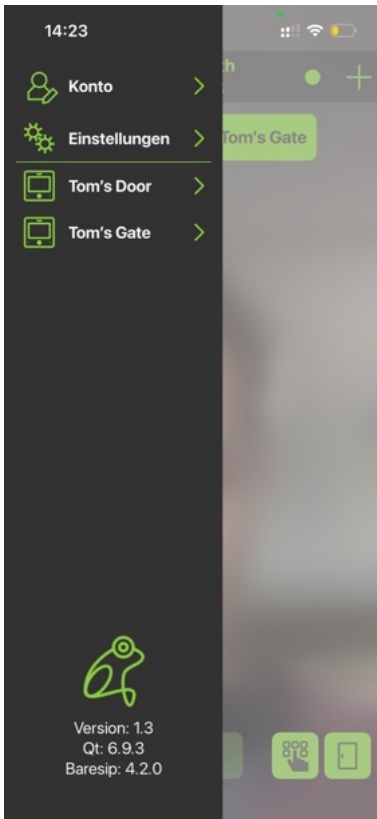
- Filtern Sie Ereignisse nach Typ oder Datumsbereich über die untere Symbolleiste.
- Tippen Sie auf ein Ereignis, um die zugehörige Videoaufnahme in derselben Ansicht abzuspielen, und verwenden Sie die Steuerungselemente der Player-Symbolleiste zur Verwaltung der Wiedergabe.
- Tippen Sie auf das Player-Symbol, um den Vollbild-Player zu öffnen, der eine größere Videoanzeige und zusätzliche Optionen in der oberen Symbolleiste bietet.



## 5.8. Terminal-Geräteeinstellungen

Die Seite **Geräteeinstellungen** in frogSIP wird verwendet, um zu verwalten, wie die App eine Verbindung zu einem frogTerminal herstellt. Diese Einstellungen umfassen den Terminalnamen, die SIP-Adresse, das Admin-Passwort, das Mieterpasswort, den Favoritenstatus sowie die Möglichkeit, das Gerät aus der App zu entfernen.

Diese Einstellungen unterscheiden sich von den Terminal-Nutzerfunktionen, die in **Abschnitt 5.9, „Terminal-Nutzereinstellungen“** beschrieben werden. Die Geräteeinstellungen steuern die Verbindung und die Zugangsdaten, die von der frogSIP App verwendet werden, während die Terminal-Nutzereinstellungen Zugriff auf alltägliche Funktionen bieten, wie Klingeltasteneinstellungen, Zugriffs-PINs, Zeitpläne und Türöffnerfunktionen.



So öffnen Sie die Seite **Geräteeinstellungen**:

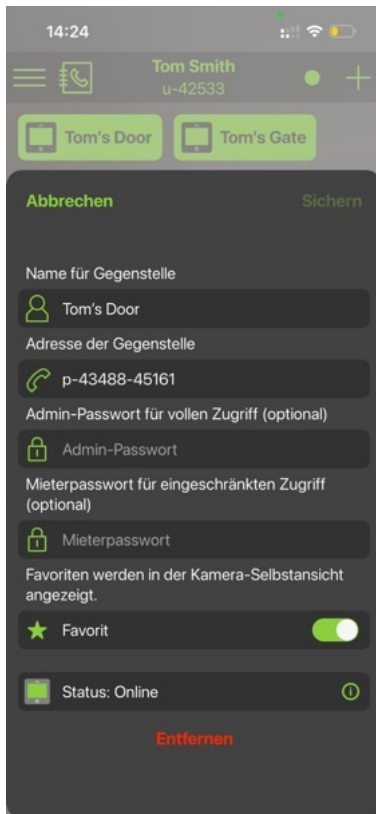
- Öffnen Sie die Seitenleiste / tippen Sie auf das Burger-Menü.
- Öffnen Sie **Einstellungen**.
- Wählen Sie **Geräte**.
- Wählen Sie **frogTerminals**.
- Wählen Sie Ihr frogTerminal aus.

Die Seite **Geräteeinstellungen** für das ausgewählte frogTerminal wird geöffnet.

## Geräteeinstellungen



- **Name:** Das Feld **Name** legt fest, wie das frogTerminal in der frogSIP App angezeigt wird. Dieser Name wird nur lokal in der App verwendet. Änderungen bleiben lokal in der App und helfen Nutzern dabei, das richtige Terminal zu erkennen, zum Beispiel wenn mehrere frogTerminals gekoppelt oder verfügbar sind.
- **Adresse:** Die SIP-Adresse definiert das SIP-Ziel, das von der frogSIP App verwendet wird, um das frogTerminal anzurufen oder mit ihm zu kommunizieren. Diese Einstellung wird normalerweise automatisch während der Kopplung konfiguriert. Ändern Sie diese Einstellung nur, wenn Sie von Ihrem Administrator, Installateur oder Support-Kontakt dazu aufgefordert werden.
- **Admin-Passwort:** Das Admin-Passwort kann von der frogSIP App verwendet werden, um den SIP-Message-Kanal freizuschalten und auf die erforderlichen Bluetooth-Informationen des Terminals zuzugreifen.  
**Das Admin-Passwort bietet Zugriff auf Administratorebene und sollte nur an autorisierte Nutzer weitergegeben werden.**
- **Mieterpasswort:** Das Mieterpasswort wird verwendet, um dem zugewiesenen App-Nutzer Zugriff auf die Bluetooth-bezogenen Funktionen dieses frogTerminals zu geben, ohne das Admin-Passwort bereitzustellen. Dieses Passwort wird in der Weboberfläche des frogTerminals für das entsprechende Klingelschild konfiguriert. Siehe **Abschnitt 8.1 „Klingelschilder“**.
- **Favorit:** Legt fest, ob das frogTerminal als Favorit in der Hauptanrufliste angezeigt wird. Verwenden Sie diese Option, um häufig verwendete Terminals einfacher zugänglich zu machen.
- **Entfernen:** Die Option **Entfernen** entfernt das ausgewählte frogTerminal aus der frogSIP App. Das Entfernen des Geräts aus der App löscht nicht die Konfiguration des frogTerminals selbst.



Die Schnelleinstellungen bieten schnellen Zugriff auf die wichtigsten Einstellungen eines frogTerminals.

Um die Schnelleinstellungen zu öffnen, halten Sie die Favoritentaste oder den Terminalnamen des entsprechenden frogTerminals in der Anrufliste gedrückt.

Es öffnet sich ein unterer Dialog mit schnellem Zugriff auf die Einstellungen und Statusinformationen des Terminals.

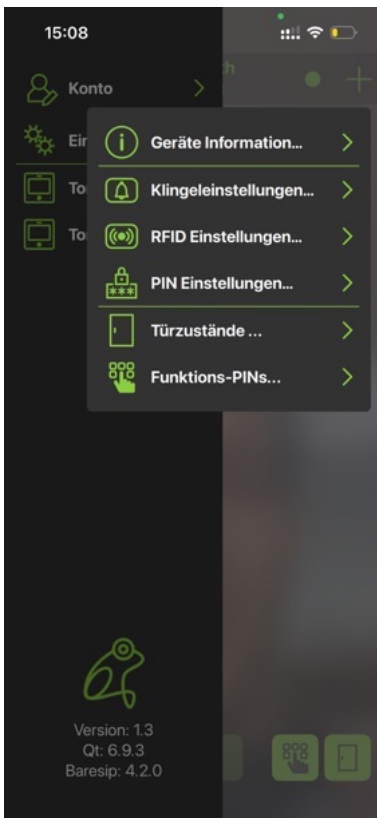
Die Schnelleinstellungen bieten Zugriff auf dieselben Geräteeinstellungen, einschliesslich Name, SIP-Adresse, Admin-Passwort, Mieterpasswort, Favoriteneinstellung und eine Option zum Entfernen des Geräts.

Zusätzlich wird der aktuelle Online-Status des frogTerminals angezeigt.

## 5.9. Terminal-Nutzereinstellungen

Die Terminal-Nutzereinstellungen bieten Zugriff auf alltägliche Nutzerfunktionen des ausgewählten frogTerminals. Dazu gehören das Ändern der Klingeltastennamen, das Verwalten von Zugriffs-PINs, das Konfigurieren von Zeitplänen sowie das Bedienen des Türöffners und der Funktions-PINs.

Diese Funktionen unterscheiden sich von den Geräteeinstellungen, die in **Abschnitt 5.8 „Terminal-Geräteeinstellungen“** beschrieben werden. Die Geräteeinstellungen steuern, wie die frogSIP App eine Verbindung zum frogTerminal herstellt und welche Passwörter für den Zugriff verwendet werden. Die Terminal-Nutzereinstellungen sind für die Bedienung des Terminals auf Nutzer- bzw. Mieter-Ebene vorgesehen.

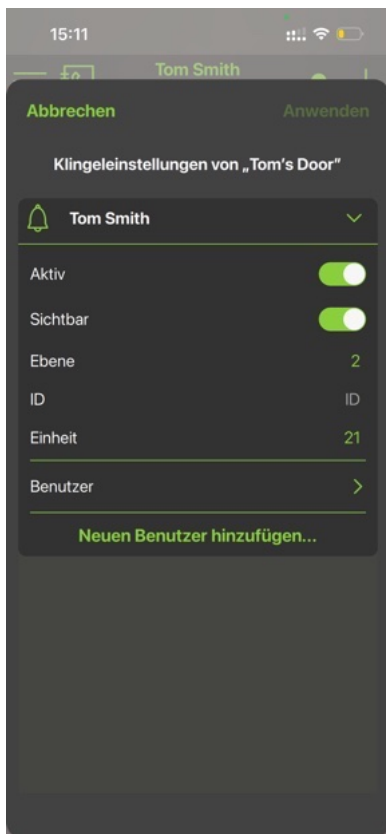


Wählen Sie in der linken Seitenleiste Ihr frogTerminal aus, in diesem Beispiel: **Tom's Door**. Dadurch öffnet sich ein Slide-out-Menü mit den verfügbaren Optionen für das ausgewählte Gerät.

Das Auswahlmenü ist in drei Bereiche unterteilt:

- **Geräteinfo:** Zeigt allgemeine Informationen zum frogTerminal an.
- **Einstellungen:** Konfigurieren Sie Klingeleinstellungen sowie den Zugriff per RFID und PINs. Diese Einstellungen entsprechen den Einstellungen, die in der Weboberfläche des Terminals definiert wurden.
- **Schnellzugriff:** Bietet direkten Zugriff auf die Türsteuerung, den Türstatusdialog und das Ausführen von Funktions-PINs.

### 5.9.1. Einstellungen für Klingelschilder



Nachdem Sie auf **Klingeleinstellungen** getippt haben, öffnet sich ein Dialog, in dem Sie folgende Einstellungen vornehmen können:

- Tippen Sie auf den Namen des Klingelschilds, um ihn zu ändern, zum Beispiel "Tom Smith".
- **Aktiv**: Aktivieren oder deaktivieren Sie das Klingelschild.
- **Sichtbar**: Legen Sie fest, ob das Klingelschild sichtbar oder ausgeblendet sein soll. Ausgeblendete Klingelschilder können weiterhin durch Ereignisse ausgelöst werden, zum Beispiel für einen automatischen Sicherheitsruf.
- **Ebene**, **ID** und **Einheit** sind optional. Weitere Informationen finden Sie in **Abschnitt 8.1 „Klingelschilder“**.
- Durch Tippen auf **Benutzer** öffnet sich die Ansicht, die im nächsten Bild gezeigt wird.

Schliessen Sie die Einstellungen ab, indem Sie auf **Anwenden** tippen, um die Änderungen zu speichern, auf **Abbrechen**, um sie zu verwerfen, oder auf **Neuen Benutzer hinzufügen...**, um einen weiteren Nutzer anzulegen.

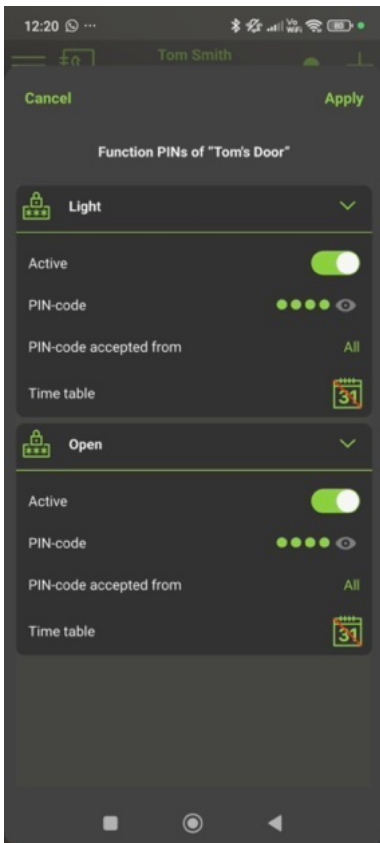


Durch Tippen auf **Benutzer** öffnet sich der Dialog zur Bearbeitung des ausgewählten Nutzers:

- **Name**: Zeigt den Namen des Benutzers an, zum Beispiel „Tom Smith“. Über den Papierkorb kann der Nutzer gelöscht werden.
- **Aktiv**: Aktiviert oder deaktiviert den Nutzer für Ruffunktionen.
- **SIP-Adresse**: Zeigt die SIP-Adresse des Nutzers an.
- **SIP-Domäne**: Zeigt die SIP-Domäne an, über die der Nutzer erreichbar ist.
- **Automatische Anrufbeantwortung**: Legt fest, ob und wie Anrufe von diesem Nutzer automatisch angenommen werden dürfen, zum Beispiel mit Audio und Video.
- **Verzögerung**: Legt eine Verzögerung für den Ruf fest. Mit + und – kann der Wert angepasst werden.
- **Zeitplan für Anrufe**: Über das Kalendersymbol kann ein Zeitplan für diesen Nutzer festgelegt werden. Damit kann definiert werden, wann der Nutzer angerufen werden darf.
- **Benutzer erneut einladen**: Sendet die Einladung erneut, zum Beispiel wenn die ursprüngliche Einladung nicht mehr verfügbar ist oder erneut versendet werden soll.

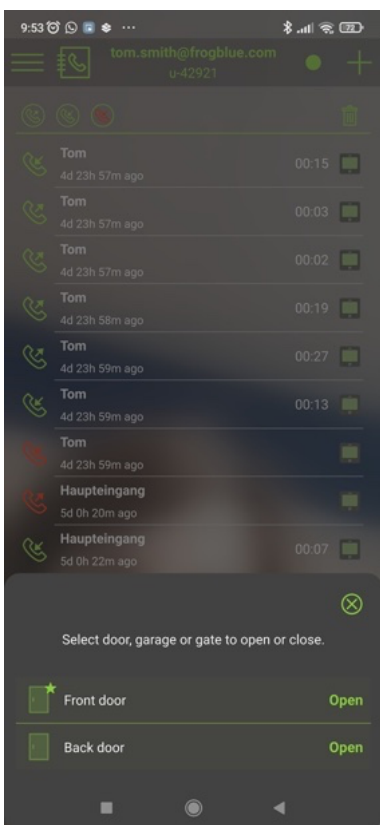
Schliessen Sie die Bearbeitung mit **Sichern** ab, oder verwerfen Sie die Änderungen mit **Abbrechen**.

## 5.9.2. Einstellungen für die Zugangskontrolle per PIN



- Wählen Sie im Ausgangsmenü **PIN settings**, um Ihre bereits angelegten Funktions-PINs zu verwalten.
- Im Beispiel rechts wurde eine PIN angelegt, um das Licht zu schalten (**Light**) und eine, um die Tür zu öffnen (**Open**).
- Mit dem Schieber lassen sich die PINs deaktivieren bzw. aktivieren.
- Unter **PIN-code** lässt sich die PIN ändern.
- Durch einen Klick auf das Kalender-Symbol erstellen Sie einen Zeitplan, um festzulegen, wann die PIN gültig ist.
- Beenden Sie die Einstellungen mit einem Klick auf **Apply**, um die Änderungen zu speichern oder mit einem Klick auf **Cancel**, um den Vorgang abubrechen.

## 5.9.3. Türöffner



- Nach einem Klick auf das Türsymbol unten rechts öffnet sich eine Liste, in der alle Türen und HomeObjects angezeigt werden, die in Ihrem Projekt enthalten sind. Das Symbol ändert sich je nach Zustand des Ausgangs.
- Drücken Sie **Open**, um die jeweilige Tür zu öffnen.

## 6. Zeitprofile

Über den Webbrowser im Menü: **Einstellungen** → **Zeitprofile**

Mit Zeitprofilen definieren Sie zeitabhängiges Verhalten, das in Anrufen, Ereignissen, Zugriffsregeln usw. verwendet wird. Zeitprofile ermöglichen

- Einfache Ein-/Aus-Zeitpläne, die mit früheren Versionen und somit mit bestehenden Konfigurationen kompatibel sind.
- Feinabstimmbare, regelbasierte Ein-/Aus-Zeitpläne mit wochen- oder tagesbasierten Programmen sowie optionalen Sonderprogrammen für bestimmte(s) Datum/Daten oder Datumsbereiche (z. B. Feiertage, Sonderveranstaltungen, Betriebsferien oder Abschaltzeiten)

Die Zeitprofile gliedern sich in drei Blöcke: Zeitpläne, Sonderprogramme und Zeitprofile.

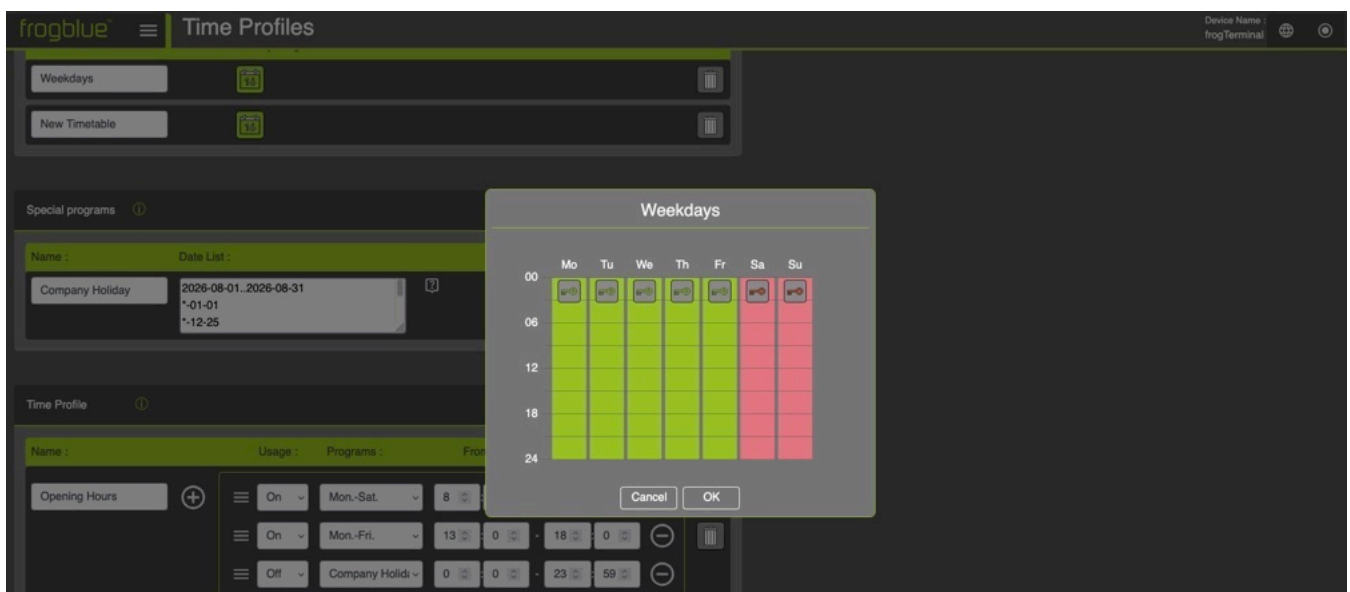
- Wenn Sie weiterhin die alten Zeitpläne nutzen wollen, fügen Sie diese bei **Zeitpläne** ein.
- Legen Sie **Sonderprogramme** für Betriebsferien und Feiertage an (optional).
- Richten Sie **Zeitprofile** ein: Benennen Sie Ihr Profil und fügen Sie eine oder mehrere Regeln hinzu. Sie können Ihre Zeitprofile überall dort nutzen, wo Zeitbedingungen verfügbar sind, beispielsweise bei Anrufzielen oder im Eventmanagement.

### 6.1. Zeitpläne


Klicken Sie auf das Kalender-Symbol unter **Wöchentliches Programm**, um klassische Wochenpläne zu erstellen, die kompatibel mit dem Bestandssystem sind.

Hier können Sie:

- **Name:** Beispielsweise „Wochentage“.
- **Wöchentliches Programm:** Klicken Sie auf das Kalender-Symbol, um den Wochenplan zu bearbeiten oder auszuwählen.
- Klicken Sie auf das Papierkorb-Symbol um Zeitpläne zu löschen.
- Fügen Sie neue Zeitpläne mit einem Klick auf das **+**-Symbol rechts oben im Zeitplan-Block hinzu.





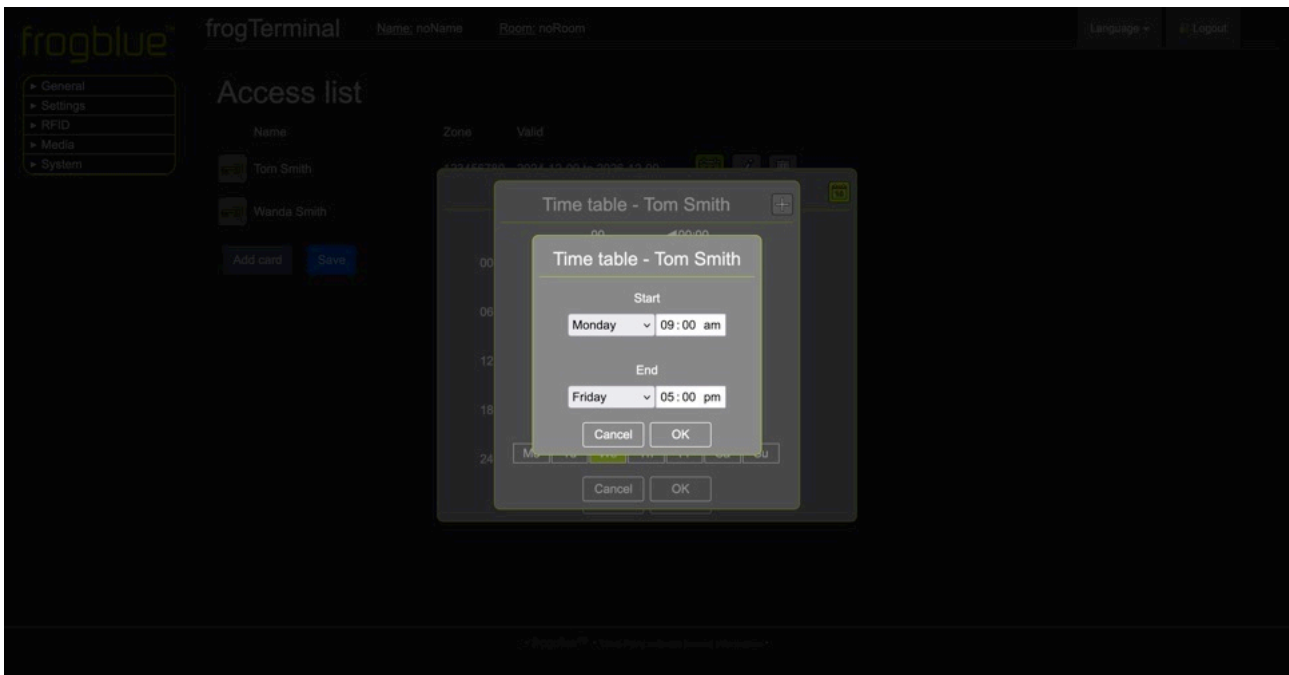
## Timetable Einstellungen

- Der  Button ermöglicht es Ihnen, den Zutritt für bestimmte Abschnitte des Zeitplans zu aktivieren oder zu deaktivieren. Beispielsweise werden bei Anklicken der Tasten für **Sa** und **Su** die Abschnitte für Samstag und Sonntag rot, was anzeigt, dass der Zutritt an Wochenenden verweigert wird.
- Das Anklicken eines grünen oder roten Tagesabschnitts des Zeitplans öffnet den Dialog **New Timetable** für den ausgewählten Tag.
- Tagesteile können auch per Drag & Drop verschoben werden, um Zeiteinstellungen von einem Tag auf andere zu kopieren.



## New Timetable Dialog

- Der  Button schaltet den Zutritt für den entsprechenden Zeitraum um. Ein grünes Symbol zeigt an, dass der Zutritt erlaubt ist, Rot zeigt an, dass er verweigert wird.
- Der  Button öffnet den **Dropdown-Dialog Time Table Day**, der es Ihnen ermöglicht, zusätzliche Zeiträume für eine feinere Steuerung hinzuzufügen. Beispielsweise können Sie konfigurieren, dass der Zutritt außerhalb der Geschäftszeiten verweigert und während der Geschäftszeiten von 9 bis 17 Uhr erlaubt ist.




## Time Table Day Dropdown Dialog

- In diesem Dialog können Sie benutzerdefinierte Zeiträume für Ihren Zeitplan konfigurieren, z. B. 9 bis 12 Uhr.
- Zeitabschnitte können auch mehrere Tage umfassen, wie z. B. Montag bis Freitag, 8 bis 18 Uhr, was Flexibilität für wiederkehrende Zeitpläne bietet.

## 6.2. Sonderprogramme




Sonderprogramme definieren bestimmte Daten (wie z.B. Feiertage) oder Zeitspannen (wie z.B. Betriebsferien), auf die innerhalb der Zeitprofile Bezug genommen werden kann.

- **Name:** Beispielsweise „Betriebsferien“.
- **Datumsliste:** Geben Sie einen Eintrag pro Zeile ein:
  - Format für einen einzelnen Tag: JJJJ-MM-TT
  - Format für einen Datumsbereich: JJJJ-MM-TT..JJJJ-MM-TT
- Klicken Sie auf das Papierkorb-Symbol um Sonderprogramme zu löschen.
- Fügen Sie neue Sonderprogramme mit einem Klick auf  rechts oben im Sonderprogramm-Block hinzu.

Tipp: Nutzen Sie Sonderprogramme für Feiertage, Betriebsferien, besondere Veranstaltungen usw.

### 6.3. Zeitprofile

Zeitprofile sind der neue Mechanismus (seit frogOS 1.7) zur Definition zeitbasierter Logik mit mehreren Regeln, die das Verhalten abhängig vom ausgewählten Programm und Zeitfenster ein- oder ausschalten können. Sie bieten die Möglichkeit das zeitbasierte Verhalten individuell anzupassen.

- **Name:** Beispielsweise „Öffnungszeiten“.
- Regelliste bestehend aus mehrere Zeilen. Jede Zeile enthält:
  - **Benutzung:** *Ein* oder *Aus*.
  - **Programme:** Zum Beispiel *Mo.-Fr.*, *Sa.-So.*, oder Sonderprogramme wie *Betriebsferien*.
  - **Von / Bis:** Zeitfenster. Format: Stunden, Minuten.
- Entfernen Sie Regeln mit einem Klick auf das „-“-Symbol am rechten Zeilenrand.
- Ändern Sie die Reihenfolge der Regeln, indem Sie  gedrückt halten und die Regel an die gewünschte Position schieben. Regeln werden von oben nach unten ausgeführt.
- Löschen Sie Ihr Zeitprofil mit einem Klick auf das Papierkorb-Symbol rechts neben den Regeln.
- Fügen Sie neue Profile und Regeln hinzu:
  - Ein Klick auf das -Symbol in der rechten oberen Ecke des Zeitprofil-Blocks erzeugt ein neues Zeitprofil.
  - Klicken Sie auf das -Symbol neben dem Profilnamen um eine zusätzliche Regelzeile einzufügen.



Im Beispiel in der obigen Abbildung wird eine klare „Öffnungszeiten“-Logik erstellt, bei der Wochentage während der Geschäftszeiten aktiv sind und Wochenenden und Betriebsferien explizit inaktiv bleiben.

## 7. Zutrittskontrollkonfiguration

### 7.1. Einführung in die Zutrittskontrolle von frogTerminal

Das frogTerminal bietet eine effiziente und flexible, zeitbasierte Zutrittskontrolle mittels PINs, RFID-Karten und sogar Telefonanrufen, ohne dass eine dauerhafte Cloud- oder Netzwerkverbindung erforderlich ist. Das System wurde entwickelt, um das Zutrittsmanagement zu vereinfachen und gleichzeitig robuste Sicherheit zu gewährleisten.

Für RFID-Karten verwendet das frogTerminal den internationalen Standard DESFire EV2, was Zuverlässigkeit und Sicherheit garantiert. Karten oder Transponder können an jedem frogTerminal beschrieben und dann über alle Terminals innerhalb desselben Projekts verwendet werden – zusätzliche Konfiguration ist nicht erforderlich. Obwohl eine Netzwerkverbindung optional ist, verbessert sie den Komfort, da sie eine Fernverwaltung über das Netzwerk oder Internet ermöglicht.

### 7.2. PINs, Zutrittscodes

Es gibt eine Reihe numerischer Codes zur Bedienung des frogTerminals.

- **Admin-PIN:** Eine sechsstellige numerische PIN, die zur Administration der Terminalkonfiguration über den Touchscreen des Geräts verwendet wird.
- **Funktions-PIN:** Eine numerische PIN, die zwischen eins und sechs Stellen lang ist und einer beliebigen Funktion auf dem frogTerminal zugeordnet werden kann. Beispielsweise könnte „111“ dafür vorgesehen sein, die Security zu rufen.
- **Zutritts-PIN:** Eine sechsstellige numerische PIN, die mit den Benutzerzutrittsregeln verknüpft ist und den Zutritt zu Türen oder Eingängen im Rahmen eines Zwei-Faktor-Authentifizierungssystems ermöglicht, das RFID-Karten oder -Transponder ergänzt.

**Hinweis:** Falsche PIN-Eingaben lösen eine Verzögerung aus, bevor die nächste PIN eingegeben werden kann. Diese Verzögerungen erhöhen sich schrittweise (z. B. 5 s, 10 s, 20 s, 30 s, bis zu 60 Sekunden).

### 7.3. Grafisches Feedback für Zutrittsereignisse



- Ein erfolgreiches Zutrittsereignis.

**Card locked**



- Ein verweigertes Zutrittsereignis.

**Wrong zone**



- Ein verweigertes Zutrittsereignis.
- Grund: Karte ist in dieser Zone nicht zum Zutritt berechtigt.

**Access denied,  
wrong time**



- Ein verweigertes Zutrittsereignis.
- Grund: Zeitplan-Ausnahme. Karte ist zu diesem Zeitpunkt nicht erlaubt.

**Wrong PIN**



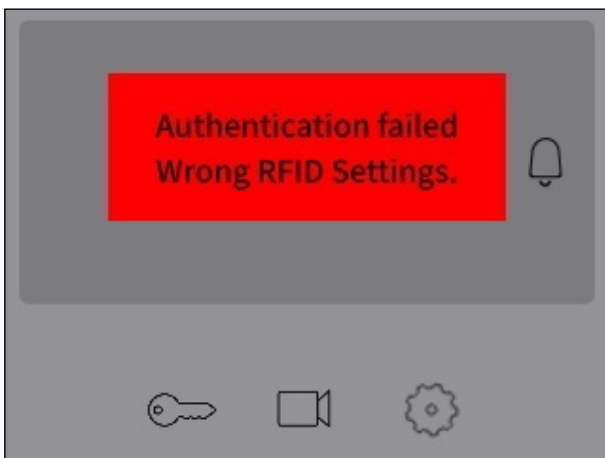
- Ein verweigertes Zutrittsereignis.
- Grund: Eingegebene PIN ist ungültig.



- Ein verweigertes Zutrittsereignis.
- Grund: die Karte ist nicht mehr gültig - sie muss neu beschrieben/aktualisiert werden.



- Mehrfaktor-PIN erforderlich für den Zutritt.
- Grund: Karte oder Zone erfordert eine zusätzliche Zutritts-PIN. Je nach Quelleneinstellung geben Sie die Benutzer-PIN oder die Terminal-Zonen-PINs ein.



- Die Karte ist falsch formatiert.



- Projekt nicht auf Karte geschrieben oder falsche Projektnummer.

## 7.4. Dezentrale Zutrittskontrolle

Bei frogblue werden Benutzerdaten direkt auf den Karten oder Transponder gespeichert, wodurch das System nahezu unabhängig von Netzwerken oder Clouds ist. Jedes frogTerminal liest die vollständigen Benutzerdaten von der Karte, sobald diese präsentiert wird, und gewährleistet so einen nahtlosen Betrieb ohne externe Abhängigkeiten.

Um einen sicheren Zutritt über alle Terminals eines Projekts zu ermöglichen, müssen die Verschlüsselungseinstellungen konsistent sein. Dies erfordert, dass an jedem Terminal dieselbe zehnstellige PIN und dasselbe Projektdatum eingegeben werden. Aktualisierungen der Benutzerdaten, wie z. B. PIN-Änderungen oder geänderte Zutrittsberechtigungen, können an einem einzigen Terminal (z. B. am Haupteingang) vorgenommen werden. Die aktualisierten Daten werden dann automatisch beim nächsten Einsatz der Karte auf diese geschrieben. Das Sperren von Karten erfolgt auf die gleiche Weise.

Zukünftige Erweiterungen: Anstehende Updates werden die Möglichkeit einführen, Benutzerdaten über das Netzwerk oder lokal via Bluetooth zu verwalten. Zusätzlich ist ein cloudbasiertes Zutrittsmanagementsystem mit Zeiterfassung geplant.

## 7.5. Karteninformationen

Jede Karte speichert sicher wesentliche Benutzerdaten für den Zutritt, einschließlich:

- Name, Vorname und Personalnummer
- Erstellungsdatum der Karte
- Gültigkeitszeitraum (Start- und Enddatum/-uhrzeit)
- Persönliche PIN
- Wöchentliche Zutrittspläne
- Zutrittsbefugnisse für bis zu neun Zonen

frogTerminals lesen und interpretieren die Kartendaten direkt. Änderungen, wie neue PINs oder Zutrittspläne, werden erkannt und nahtlos während der Kartennutzung integriert. Das Terminal archiviert den Inhalt der Karte und den Nutzungszeitstempel, sodass Administratoren Benutzerdetails und Zutrittsprotokolle direkt auf dem Terminaldisplay einsehen können. Falls eine Netzwerkverbindung besteht, können diese Daten auch remote über einen Webbrowser abgerufen werden.

The screenshot shows the 'frogTerminal' web interface. At the top, there's a header with 'frogblue™ frogTerminal' and fields for 'Name: noName' and 'Room: noRoom'. On the right, there are 'Language' and 'Logout' options. A sidebar on the left contains a menu with 'General', 'Settings', 'RFID', 'Terminal settings' (highlighted), 'Access list', 'Media', and 'System'. The main content area is titled 'Terminal settings' and contains several configuration fields: 'RFID Code' (text input), 'Project Date' (calendar icon, value: 08/12/2024), 'Projekt Number' (spinners, value: 1), 'Zone' (spinners, value: 1), 'PIN Code Source' (dropdown, value: None), 'Time Table Source' (dropdown, value: None), 'Authentication Call' (dropdown, value: Never), 'Url Source' (dropdown, value: None), 'Terminal Url.' (text input), and 'Card issued at' (calendar icon, value: 01/01/2024). A blue 'Save' button is located at the bottom left of the settings area. At the very bottom, there is a small footer: '© frogblue™ • Third Party software license information'.

## 7.6. Zutritts-Funktionen

Die Karte oder der Transponder definiert die Zutrittsregeln des Benutzers, wie PINs, Pläne und autorisierte Zonen. Das System ermöglicht zudem Flexibilität für spezielle Situationen:

- **Keine PIN-Anforderung:** Für Innentüren kann das Terminal so eingestellt werden, dass die persönliche PIN-Prüfung umgangen wird (**None**).
- **Geteilte PIN:** Für vorübergehende Sicherheitsbedürfnisse kann eine terminalspezifische PIN (**Terminal**) eingestellt werden, die die persönlichen PINs aller Benutzer überschreibt.
- **Zeitliche Zutrittsberechtigungen:** Terminals können entweder die auf der Karte gespeicherten Zutrittszeiten (**Card**) verwenden, lokale Pläne für alle Benutzer (**Terminal**) einstellen oder Zeitbeschränkungen vollständig deaktivieren (**None**).

## 7.7. Spezialfunktionen

frogTerminals unterstützen zusätzliche Funktionalitäten, um speziellen Anforderungen gerecht zu werden:

- **Integration von Telefonen:** Karten können eine Telefonnummer speichern, sodass das Terminal nach dem Auslesen und der Authentifizierung der Karte einen Anruf initiieren kann.
- **IP-Links:** Ein IP-Link kann auf der Karte gespeichert werden, der automatisierte Aktionen auslösen kann, wie z. B. das Auslösen spezieller Funktionen oder die Integration in Drittsysteme wie Zeiterfassungssysteme nach der Authentifizierung.
- **Erweiterte APIs:** Die frogTerminal API (Application Programming Interface) ermöglicht kundenspezifische Integrationen und macht das Terminal zu einem leistungsstarken, intelligenten Zutrittspunkt und Systeminterface für Anbieter von Drittlösungen.
- Diese Funktionen machen frogTerminal zu einer vielseitigen Lösung für fortschrittliche Zutrittskontrolle und Systemintegration.

## 7.8. RFID-Verschlüsselung und Zonen

Richten Sie Zutrittskontrollparameter wie RFID-Verschlüsselung, Zonen und Projekteinstellungen ein.

### Schrittübersicht:

- RFID-Verschlüsselung konfigurieren (zehnstelliger Code, Projektdatum und Projektnummer).
- Das Terminal den Zonen zuordnen.
- Benutzerspezifische oder Terminal-weite PINs und Pläne einstellen.

## 7.8.1. RFID-Verschlüsselung und Zonen über den Webbrowser (Terminal-Einstellungen)

Über den Webbrowser im Menü: **Zutrittskontrolle** → **Terminal-Einstellungen**

Hauptschlüssel	*****
Projekt Datum:	01 / 03 / 2026
Projektnummer:	1
Zone:	1
PIN Code Quelle:	Kein
Zeitplan Quelle:	Kein
Authentifizierungsanruf:	Nie
Url Quelle:	Kein
Mindest-Ausgabedatum	01 / 01 / 2024

- **Hauptschlüssel:** Zehnstelliger numerischer Code, der zusammen mit dem Projektdatum und der Projektnummer als Grundlage (oder „Seed“) für die Verschlüsselung Ihrer Zutrittskontrolle dient. Frogblue-Geräte, die mit demselben Hauptschlüssel, Datum und derselben Projektnummer in Betrieb genommen wurden, arbeiten als ein einheitliches System.
- **Projektdatum:** Der Zeitstempel, der als Sicherheits-Seed dient, typischerweise eingestellt auf das letzte Datum, an dem dieses Projekt in Betrieb genommen wurde.
- **Projektnummer:** Eine Zahl zwischen 1 und 32.767 zur Identifikation des Projekts, nützlich bei der Verwaltung mehrerer Projekte oder komplexer Setups.
- **Zone:** Eine Zahl von 1 bis 9, die die Zutrittszone definiert. Das System unterstützt bis zu neun Zonen, die jeweils einen bestimmten Zutrittsbereich darstellen (z. B. Parkplatz, Gebäude A, Serverraum, Sicherheit usw.).
- **PIN Code Quelle:** Bestimmt die Quelle der gespeicherten PIN-Codes für die Zwei-Faktor-Authentifizierung, drei Optionen:
  - **Keine:** Deaktiviert die PIN-Eingabe an diesem Terminal.
  - **Karte:** Die gängigste Einstellung, die die Zwei-Faktor-Authentifizierung mit spezifischen PIN-Codes ermöglicht, die einzelnen Benutzern zugeordnet und auf der Zutrittskarte gespeichert werden.
  - **Terminal:** Sichert die Tür oder den Zutrittspunkt mit einem terminal-spezifischen PIN-Code. Diese PIN gilt für alle Benutzer an diesem Standort und überschreibt persönliche PINs.  
Beim Auswählen der Terminal-Option erscheint ein zusätzliches Eingabefeld, in dem Sie eine sechsstellige PIN für den Zutritt an diesem Terminal festlegen können.
- **Zeitplan Quelle:** Gibt an, aus welcher Quelle zeitbasierte Zutrittsregeln stammen, mit 3 Optionen:
  - **Keine:** Deaktiviert zeitbasierte Zutrittsregeln an diesem Terminal.
  - **Karte:** Zeitregeln werden auf der Zutrittskarte gespeichert, wodurch individuelle Zeitpläne möglich sind (z. B. Allgemeines Personal: 9-17 Uhr, Reinigungskräfte: Fr-Sa 15-19 Uhr, Security: 24h).

- **Terminal:** Mit dieser Einstellung kann eine Tür oder ein Zutrittspunkt auch mit einem terminal-spezifischen Zeitplan gesichert werden. Die Zutrittszeiten an diesem Standort entsprechen exakt den lokal am Terminal festgelegten Zeiten.

Beim Auswählen der Terminal-Option erscheint ein zusätzlicher Button zur Konfiguration der terminal-spezifischen Zeitpläne. Siehe **Abschnitt 7.10 „Hinzufügen und Sperren von Karten“** zur Konfiguration von Zeitplänen.

- **Authentifizierungsanruf:**

Diese Einstellung bestimmt, ob das Terminal einen Authentifizierungsanruf initiieren soll, um den Zutritt zu bestätigen, beispielsweise zur Verifizierung von Lieferzugängen mit der Versandabteilung, zur Koordination der Eingänge von Gewerbeobjekten mit dem Standortmanagement oder zur Durchsetzung des Vier-Augen-Prinzips in der Sicherheit.

Es gibt vier Konfigurationsoptionen:

1. **Nie:** Deaktiviert Authentifizierungsanrufe für alle Zutrittsereignisse an diesem Terminal.
2. **Karteneintrag:** Die Anrufeinstellungen (ob und wer angerufen wird) werden auf der Zutrittskarte definiert und gespeichert, was individualisierte Konfigurationen für Benutzer ermöglicht.
3. **Nur bei Ausnahme:** Anrufe werden nur in Ausnahmefällen getätigt, beispielsweise bei Zugriffsversuchen außerhalb der festgelegten Zeitpläne oder nach falschen PIN-Eingaben.
4. **Immer:** Bei jedem Zutrittsereignis wird ein Authentifizierungsanruf getätigt, unabhängig von Zeitplänen oder PIN-Korrektheit, um maximale Überwachung zu gewährleisten.

- **URL-Quelle:** Diese Einstellung bestimmt, ob das Terminal einen IP-Anruf auslösen oder eine Drittanbieter-API während eines Zutrittsereignisses aufrufen soll. Dies ermöglicht die Integration mit externen Systemen, z. B. das Auslösen spezieller Funktionen, das Protokollieren von Zutrittsereignissen oder die Interaktion mit Drittanbieterapplikationen.

**Beispiele:**

**Logistik:** Automatische Benachrichtigung von Lagerautomationssystemen, um eine Bestellung vorzubereiten oder zu versenden, sobald der Zutritt erfolgt. Automatisches Ausleuchten eines Wegs zur Liefertür für eine effiziente Navigation.

**Gesundheitswesen:** Auslösen eines Rufsystems für Krankenschwestern oder Managementsystemen, um Besucherinformationen zu protokollieren oder die Zustellung kritischer Medikamente zu bestätigen.

**Gebäudeautomation:** Aktivieren der Beleuchtung und Anpassen der HLK-Einstellungen entlang einer definierten Route für den Benutzer oder automatisches Herbeirufen eines Aufzugs zur richtigen Etage.

**Arbeitskraftmanagement:** Protokollieren der Check-in/Check-out-Zeiten der Mitarbeiter zur Anwesenheitsverfolgung oder Einleiten eines Workflows, wenn ein Techniker einen bestimmten Bereich betritt.

**Sicherheit und Überwachung:** Benachrichtigen eines Sicherheitsteams oder -systems, wenn ein eingeschränkter Bereich betreten wird, oder Protokollierung von Einträgen zu Audit-Zwecken.

Es gibt drei Konfigurationsoptionen:

1. **Keine:** Deaktiviert das URL-Auslösen für Zutrittsereignisse an diesem Terminal.
2. **Karte:** Die auszulösende URL wird auf der Zutrittskarte definiert und gespeichert, wodurch benutzerdefinierte Aktionen für einzelne Benutzer ermöglicht werden.
3. **Terminal:** Eine spezifische URL wird lokal am Terminal festgelegt und universell für alle Zutrittsereignisse an diesem Standort ausgelöst. Diese Einstellung eignet sich ideal für standardisierte Integrationen über mehrere Benutzer hinweg.

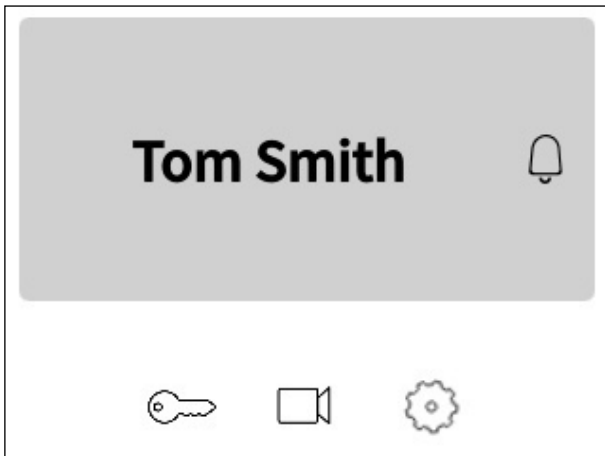
Beim Auswählen dieser Funktion erscheint ein zusätzliches Feld für die **Terminal-URL**. Diese URL wird ausgelöst, wenn die URL-Quelle als **Terminal** konfiguriert ist. Dadurch kann das Terminal standardisierte API-Aufrufe oder IP-Aktionen für alle Zutrittsereignisse initiieren.


- **Mindest-Ausgabedatum:** Gibt das früheste Erstellungsdatum an, ab dem Karten für den Zutritt an diesem Terminal zugelassen sind. Karten, die vor diesem Datum ausgegeben wurden, werden automatisch abgelehnt.

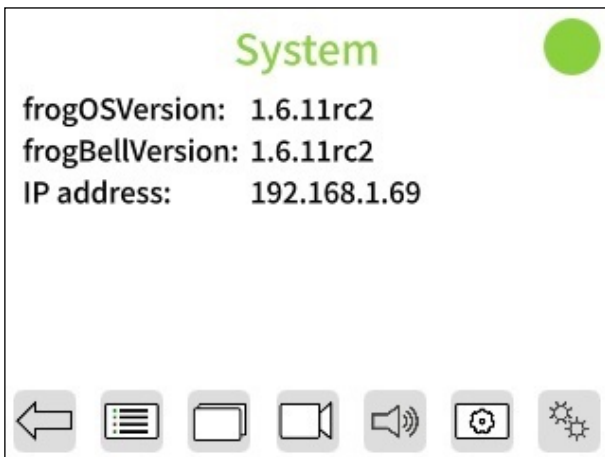
Diese Einstellung stellt eine einfache Sicherheitsmaßnahme dar, falls es zu einem möglichen Sicherheitsverstoß (z. B. verlorene Zutrittsschlüssel) kommt - setzen Sie dieses Datum einfach auf den aktuellen Tag, alle älteren Karten werden sofort gesperrt, alle Personen müssen nun ihre Schlüssel zur Neuschreibung mit aktualisierten Zutrittsdaten vorzeigen.


- Der  Button speichert die aktualisierten Zutrittseinstellungen am Terminal.

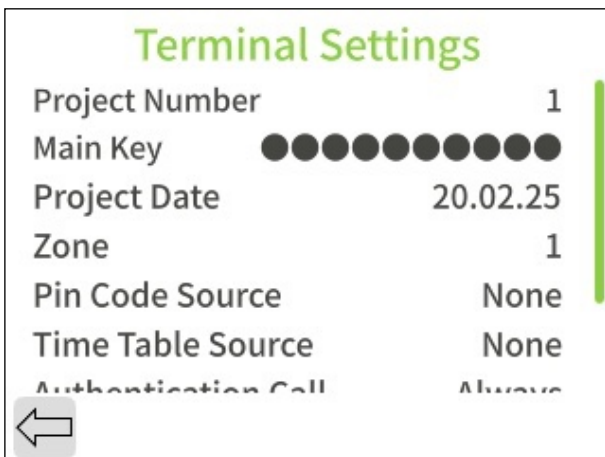
## 7.8.2. RFID-Verschlüsselung und Zonen über den On-Device-Touchscreen



- Tippen Sie auf  und geben Sie Ihre sechsstelligen Admin-PIN ein, um in den Konfigurationsmodus zu gelangen.



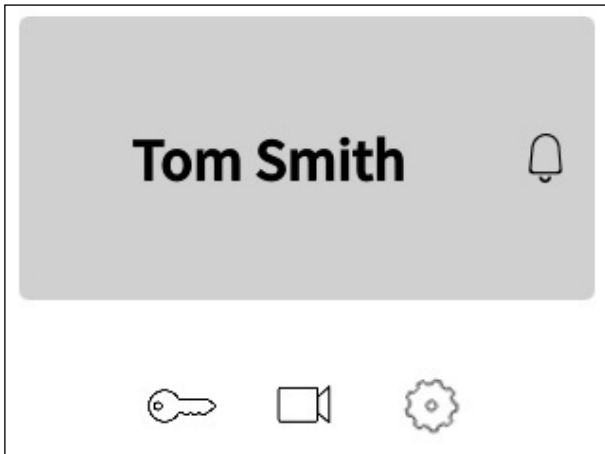
- Tippen Sie auf , um die Seite mit den RFID-Terminaleinstellungen aufzurufen.




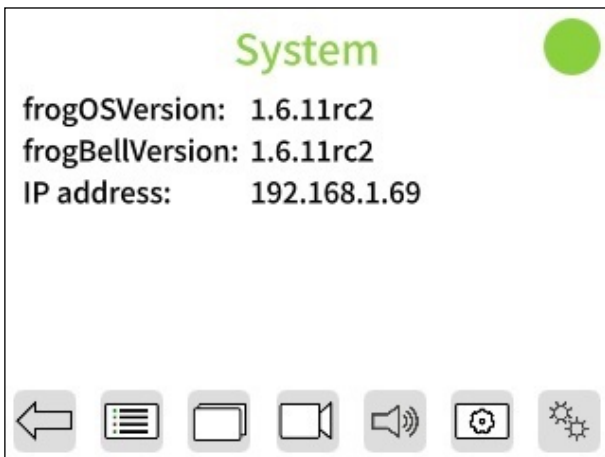
Die Einstellungen auf dieser Seite sind identisch mit den Einstellungen im Browser, die in dem *Abschnitt 7.8.1 „RFID-Verschlüsselung und Zonen über den Webbrowser (Terminal-Einstellungen)“* beschrieben werden.


## 7.9. Formatieren von Schlüsseln/Karten über den On-Device-Touchscreen

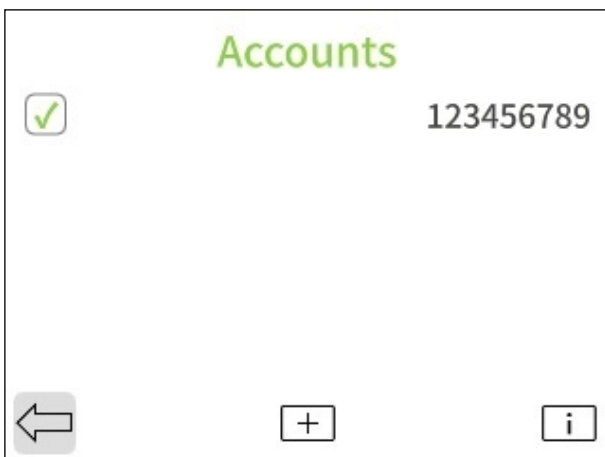
Um ein reibungsloses Beschreiben zu garantieren, muss die Karte formatiert werden, bevor sie neu beschrieben wird.




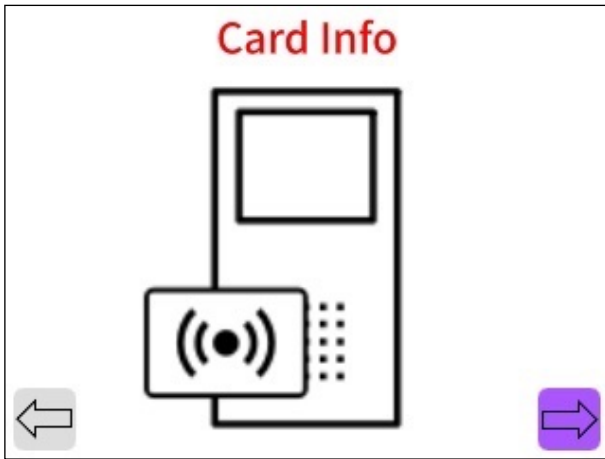
- Tippen Sie  und geben Sie Ihre sechstellige Admin-PIN ein, um den Konfigurationsmodus zu betreten.



- Tippen Sie , um auf die RFID-Schlüsseinstellungen zuzugreifen.



- Tippen Sie , um den Dialog *RFID Card Info* zu öffnen.

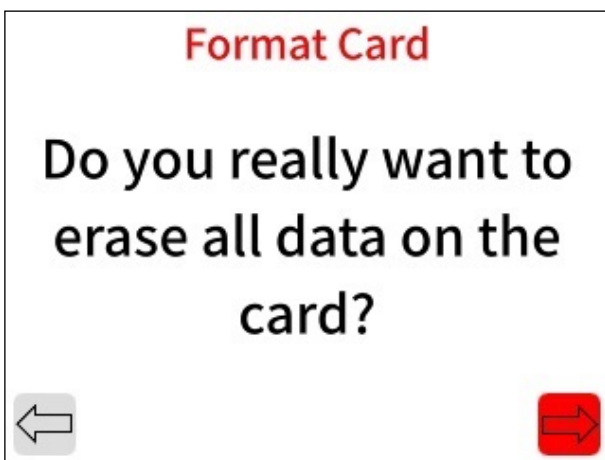


- Halten Sie Ihre RFID-Karte oder Ihren Transponder vor den RFID-Sensor des Terminals - direkt etwas links neben dem Lautsprecher.

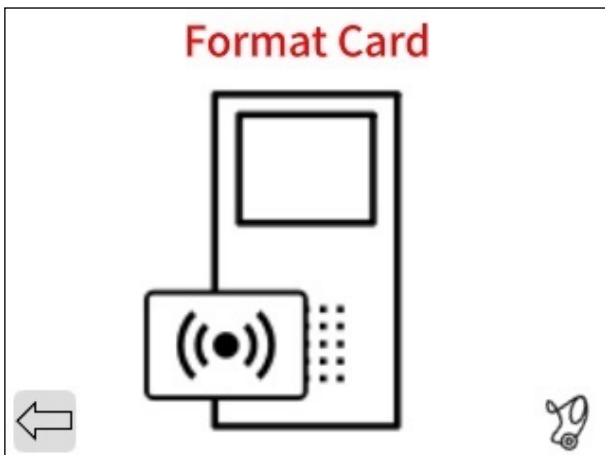


Dieser Bildschirm zeigt die Projekte oder Anwendungen, die auf der Karte oder dem Schlüssel gespeichert sind.

- Wählen Sie ein Projekt aus und tippen Sie auf **Delete**, dann bestätigen Sie und halten Sie den Schlüssel/die Karte vor das Terminal, um das Projekt zu löschen.
- Um eine Karte auf die Werkseinstellungen zurückzusetzen, tippen Sie auf **Format**.



- Bestätigen Sie, dass Sie alle Daten auf der Karte vollständig löschen möchten.



- Halten Sie den Key/die Karte vor das Terminal, warten Sie auf das Bestätigungssignal (Piepton) und Ihre Karte wird auf die Werkseinstellungen zurückgesetzt.

## 7.10. Hinzufügen und Sperren von Karten

Dieser Abschnitt zeigt, wie Sie RFID-Karten oder Schlüsselanhänger für den Benutzerzutritt hinzufügen und bei Bedarf sperren.

### Schrittübersicht:





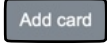

- Eine Karte über den Touchscreen oder das Webinterface hinzufügen.
- Zutrittszonen und Pläne zuweisen.
- Eine Karte sperren.

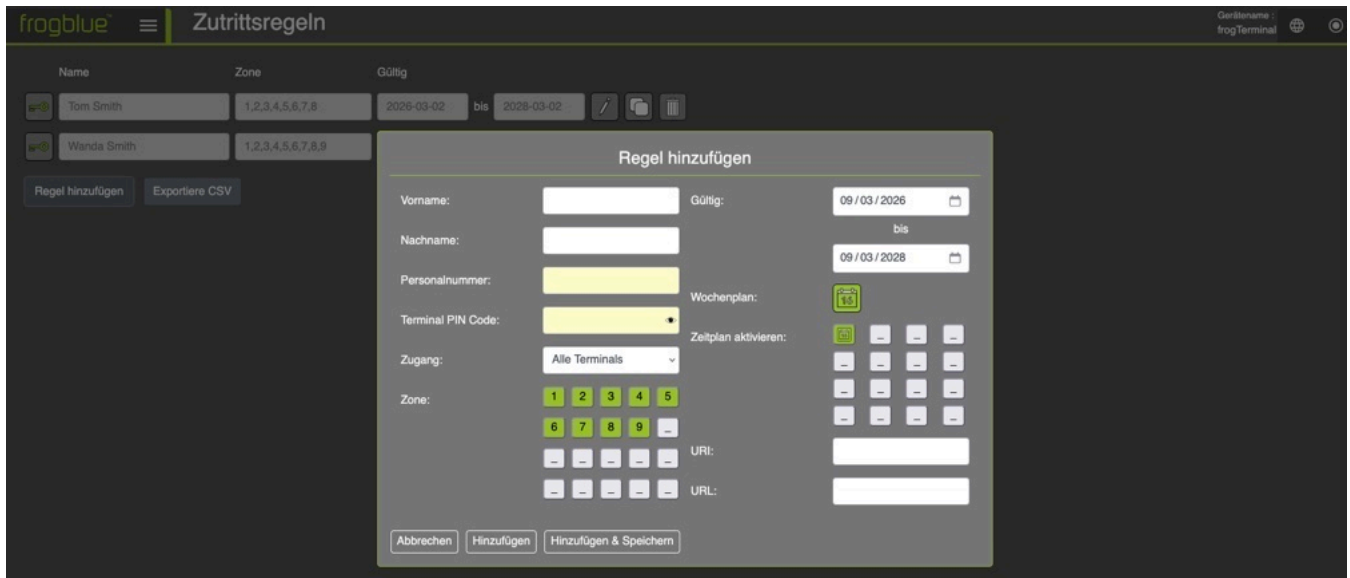
### 7.10.1. Hinzufügen und Sperren von Karten über den Webbrowser

Über den Webbrowser im Menü: **Zutrittskontrolle** → **Zutrittsregeln**



### Zutrittsliste

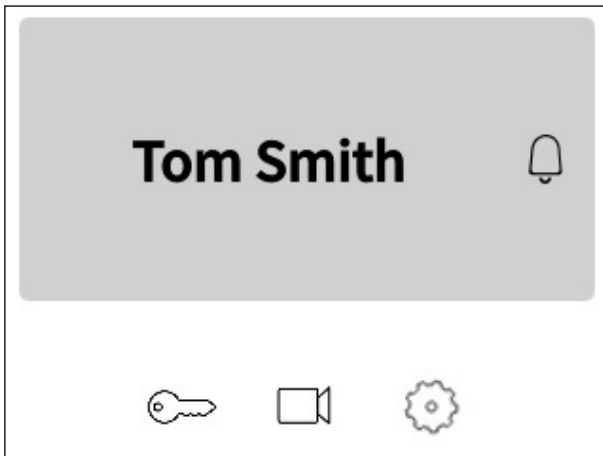
- Dieser Abschnitt zeigt die Zutrittsliste an, in der die Personalien aufgeführt sind, deren Zutrittsdaten auf diesem Terminal gespeichert sind.
- Der  Button schaltet den Masterzutritt für diesen Benutzer an/aus. Ein grünes Symbol zeigt, dass der Zutritt erlaubt ist, während ein rotes Symbol zeigt, dass er verweigert wird.
- Der  Button öffnet die Zeitplankonfiguration für den Benutzer. Weitere Details zur Konfiguration finden Sie im **Abschnitt 6 „Zeitprofile“**.  
**Hinweis:** Um die Zeitplankonfiguration nutzen zu können, muss bei den **Terminal-Einstellungen** die **Zeitplan-Quelle** auf **Karte** oder **Terminal** gesetzt werden (siehe **Abschnitt 7.8.1 „RFID-Verschlüsselung und Zonen über den Webbrowser (Terminal-Einstellungen)“**).
- Der  Button öffnet den **Edit Card** Dialog. Die Einstellungen entsprechen denen des **Add Card** Dialogs, dienen jedoch dazu, den bereits bestehenden Eintrag zu verändern. Details zum **Add Card** Dialog finden Sie im nächsten Abschnitt.
- Der  Button löscht den Zutrittskonfigurationseintrag des Benutzers von diesem Terminal.  
**Hinweis:** Dadurch wird die Karte nicht vom Zugriff auf das System gesperrt. Es werden lediglich die zwischengespeicherten Personalkartendaten auf diesem Terminal gelöscht. Eine mit dem korrekten Verschlüsselungsschlüssel beschriebene Karte kann sich weiterhin authentifizieren und Zutritt erhalten, sofern die Quelleneinstellungen dies erlauben. In solchen Fällen „überträgt“ die Karte die Daten zum Terminal, wodurch ein Eintrag in der Zutrittsliste mit den Kartendetails erstellt oder aktualisiert wird.
- Der  Button ermöglicht es Ihnen, einen neuen Personalkarten-Eintrag manuell zum System hinzuzufügen.
- Der  Button speichert die aktualisierten Zutrittseinstellungen am Terminal.  
**Hinweis:** Bei Systemen mit mehreren Terminals werden neue oder aktualisierte Zutrittsinformationen entweder dezentral über die Karte verteilt, wenn diese beim nächsten Zutrittsereignis an einem Terminal vorgezeigt wird, oder in Echtzeit über frogCast (Unified Bluetooth/IP Mesh) im IP-Netzwerk.




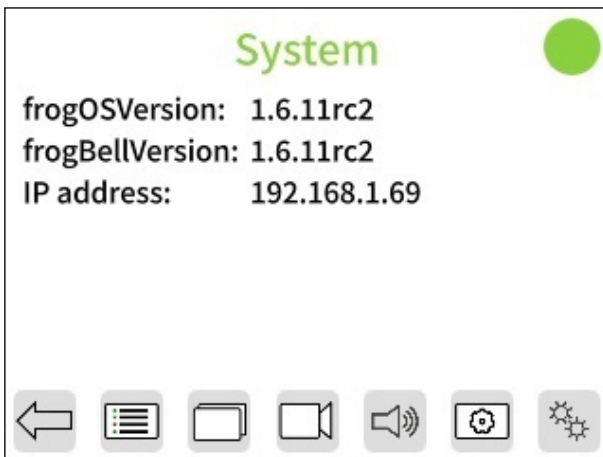
### Regel hinzufügen Dialog


- **Vorname:** Der Vorname der Person, die mit dieser Karte verknüpft ist.
- **Nachname:** Der Nachname der Person, die mit dieser Karte verknüpft ist.
- **Personalnummer:** Eine eindeutige Nummer oder Kennung für die Person, die mit dieser Karte verknüpft ist.
- **Terminal PIN Code:** Der eindeutige Zutritts-PIN-Code für die Person, die mit dieser Karte verknüpft ist. Dieser Code ist erforderlich, wenn bei den Terminaleinstellungen → **PIN-Code-Source** → **Card** eingestellt ist.
- **Zugang:** Gibt an, ob dieser Eintrag nur für dieses Terminal oder für alle Terminals im Projekt gilt.
- **Zone:** Gibt die Zonen an, zu denen diese Karte Zutritt gewährt. Durch Anklicken der Zahlen **1** bis **9** wird umgeschaltet, ob der Zutritt für jede Zone erlaubt oder verweigert wird. Beispielsweise gewährt die Auswahl von **3**, **6** und **9** Zutritt nur zu den Zonen 3, 6 und 9.
- **Gültig:** Der Datumsbereich, in dem dieser Zutrittseintrag gültig ist.
- **Wochenplan:** Es öffnet sich ein Zeitplan wie in **Abschnitt 6.1 „Zeitpläne“** beschrieben, der entsprechend angepasst werden kann.
- **Zeitplan aktivieren:** Aktivieren bzw. deaktivieren Sie den unter **Wochenplan** erstellten Zeitplan und fügen Sie bis zu 15 Zeitprofile hinzu. Details finden Sie in **Abschnitt 6.3 „Zeitprofile“**. Wie bei **Zone** wird durch Anklicken der Zahlen umgeschaltet, ob das Zeitprofil aktiviert werden soll.
- **URI:** Die URL, die im Ausnahmefall, wie z. B. bei einem Zutrittsverweigerungsereignis, ausgelöst wird.
- **URL:** Die URL, die bei erfolgreichem Zutritt ausgelöst wird.

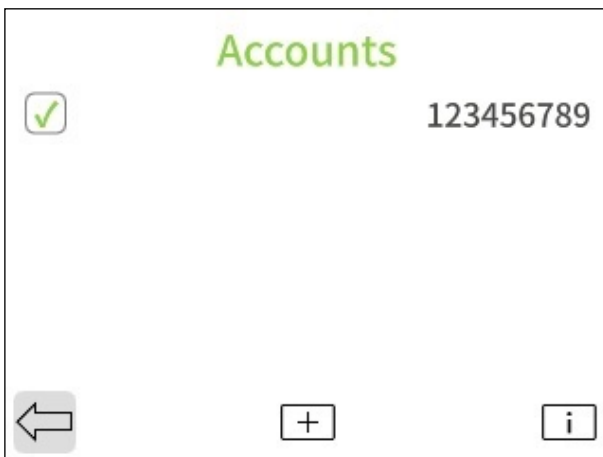
## 7.10.2. Hinzufügen und Sperren von Schlüsseln/Karten über den On-Device-Touchscreen




- Tippen Sie  und geben Sie Ihre sechstellige Admin-PIN ein, um den Konfigurationsmodus zu betreten.



- Tippen Sie , um auf die Zutrittsregel-Einstellungen zuzugreifen.



- Tippen Sie , um einen Zutrittseintrag hinzuzufügen.

Hinweis: Der **Add Card** Dialog ist identisch mit dem **Edit Card** Dialog.

### Edit Rule

Active

RFID card necessary

Name Tom Smith

Personnel No. 007

PIN Code ●●●●●●●●

Rule Scope All Stations

← [List] [16] [Trash] →

- **Active:** Aktivieren oder deaktivieren Sie diese Karte für den Zutritt im gesamten Projekt. Bei Deaktivierung wird diese Karte automatisch gesperrt, wenn sie an einem Terminal vorgezeigt wird.
- **RFID-card necessary:** Bestimmt, ob eine RFID-Karte oder ein RFID-Schlüssel für den Zutritt mit dieser Benutzerregel erforderlich ist.
- **Name:** Der Vorname (erstes Feld) und Nachname (zweites Feld) der Person, die mit dieser Karte verknüpft ist.
- **Personnel No.:** Eine eindeutige Nummer oder Kennung für den Benutzer, der mit dieser Karte verknüpft ist.
- **PIN Code:** Der eindeutige Zutritts-PIN-Code für die Person, die mit dieser Karte verknüpft ist. Dieser Code ist erforderlich, wenn bei den Terminaleinstellungen → **PIN Code Source** → **Card** eingestellt ist.
- **Rule Scope:** Gibt an, ob dieser Eintrag nur für dieses Terminal oder für alle Terminals im Projekt gilt.

### Edit Rule

Personnel No. UU /

PIN Code ●●●●●●●●

Rule Scope All Stations

Zone 1 2 3 4 5 6 7 8 9

Validity 20.02.25 to 20.02.27

SIP URI

URL http://

← [List] [16] [Trash] →

- **Zone:** Gibt die Zonen an, zu denen diese Karte Zutritt gewährt. Durch Anklicken der Zahlen 1 bis 9 wird umgeschaltet, ob der Zutritt für jede Zone erlaubt oder verweigert wird.
- **Validity:** Der Datumsbereich, in dem dieser Zutrittseintrag gültig ist.
- **SIP URI:** Die SIP-URI, die im Ausnahmefall, wie z. B. bei einem Zutrittsverweigerungs-ereignis, ausgelöst wird, z. B. sip://sipuser@sipregistrar.net
- **URL:** Die URL, die bei einem Zutrittsereignis ausgelöst wird.
- Drücken Sie auf das Symbol mit Karte und Pfeil in der rechten unteren Ecke.



- Halten Sie die Karte an den RFID-Sensor des Terminals, bis das Bestätigungssignal ertönt.

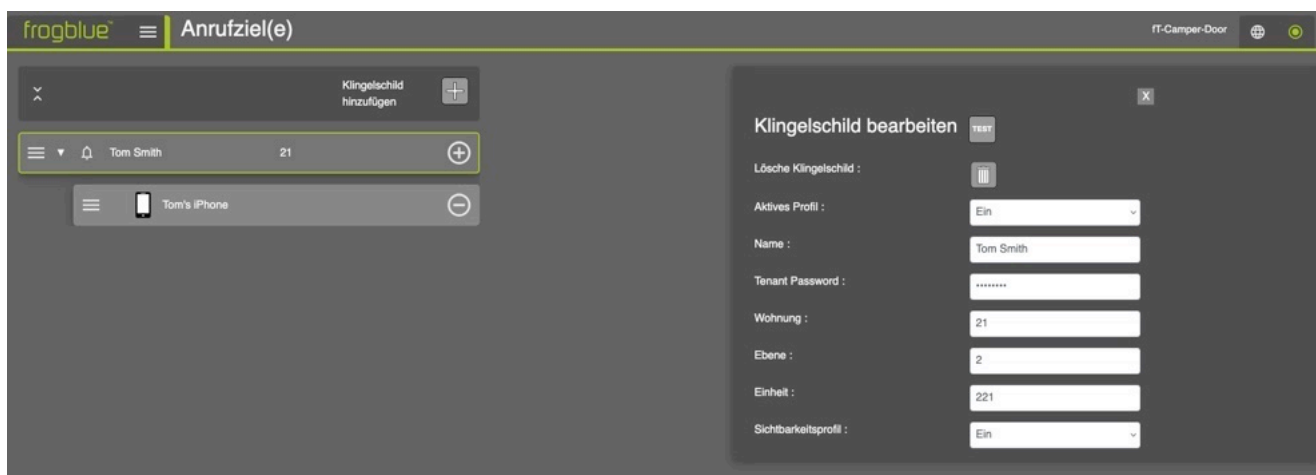
## 8. Anrufziele einrichten



### 8.1. Klingelschilder

Über den Webbrowser im Menü: **Kommunikation** → **Anrufziel(e)**

Hier richten wir die Klingelschilder ein, die auf dem Touchscreen des Terminals erscheinen, wenn dieses einen Input wahrnimmt, z. B. durch Berührung oder den Näherungssensor.


Ein Klingelschild steht für eine sichtbare Ruftaste auf dem Terminal-Display, zum Beispiel für einen Bewohner, Mieter, ein Büro, eine Abteilung oder eine Wohnung. Jedes Klingelschild kann einen eigenen Namen, Angaben zur Partei, Sichtbarkeitseinstellungen, Anrufaktionen und ein Mieterpasswort besitzen.



- Klicken Sie auf **Klingelschild hinzufügen**, um ein neues Klingelschild zu erstellen. Ein neuer Eintrag erscheint in der Liste der Klingelschilder.
-  Passen Sie die Position des Eintrags in der Liste an und legen Sie die Standardreihenfolge fest, in der die Tasten auf dem Touchscreen des Terminals erscheinen.
-  Löscht den Klingelschild-Eintrag.
- **Aktives Profil:** Durch Aktivieren des Eintrags wird er auf dem Touchscreen sichtbar und steht als Anrufziel zur Verfügung. Durch Deaktivieren wird er vom Touchscreen entfernt und kann nicht als Anrufziel verwendet werden.
- **Name:** Der Anzeigename für den Eintrag auf der Touchscreen-Klingelschild (z. B. „Tom Schmidt“).
- **Mieterpasswort:** Das Mieterpasswort wird verwendet, um dem zugewiesenen App-Nutzer Zugriff auf die Bluetooth-bezogenen Funktionen dieses frogTerminals zu geben, ohne das Admin-Passwort bereitzustellen. Dieses Passwort kann vom Nutzer in der frogSIP App unter folgendem Menüpunkt eingetragen werden: **Einstellungen** → **Geräte** → **<Ihr frogTerminal>** → **Mieterpasswort**

Die frogSIP App kann entweder das Admin-Passwort oder das Mieterpasswort verwenden, um den SIP-Message-Kanal freizuschalten und auf die erforderlichen Bluetooth-Informationen des Terminals zuzugreifen.

Verwenden Sie diese Option, wenn ein Nutzer die frogSIP App im Bluetooth-Modus für Zugriffsfunktionen nutzen können soll, zum Beispiel um die Tür ohne Internet- oder WLAN-Verbindung zu öffnen, jedoch keinen vollständigen Administratorzugriff auf das frogTerminal erhalten soll.

- **Wohnung (Optional):** Gibt die Wohnungs- oder Einheitsnummer an (z. B. „21“).
- **Ebene (Optional):** Das Stockwerk, in dem sich der Eintrag befindet (z. B. „2“).
- **Einheit (Optional):** Eine Kennung für diesen Eintrag (z. B. könnte „221“ Stockwerk 2, Einheit 21 repräsentieren).
- **Sichtbarkeitsprofil:** Wählen Sie, ob dieser Eintrag auf dem Touchscreen des Terminals angezeigt oder ausgeblendet wird. Der Eintrag kann dauerhaft sichtbar, dauerhaft ausgeblendet oder über ein Zeitprofil zeitgesteuert angezeigt werden. Ausgeblendete Einträge können weiterhin programmgesteuert, zum Beispiel über APIs, oder für Authentifizierungsanrufe verwendet werden.
- **Aktionen und Benutzer:** Definiert die Aktionen, die ausgelöst werden, wenn eine Klingeltaste gedrückt oder aktiviert wird. Verwenden Sie den  Button rechts neben dem Klingelschild, um einen neuen Aktions-Eintrag hinzuzufügen. Die angezeigten Zahlen geben die aktuelle Auswahl und die Gesamtzahl der Aktionen für diesen Klingelsignal-Eintrag an (aktuell/gesamt).

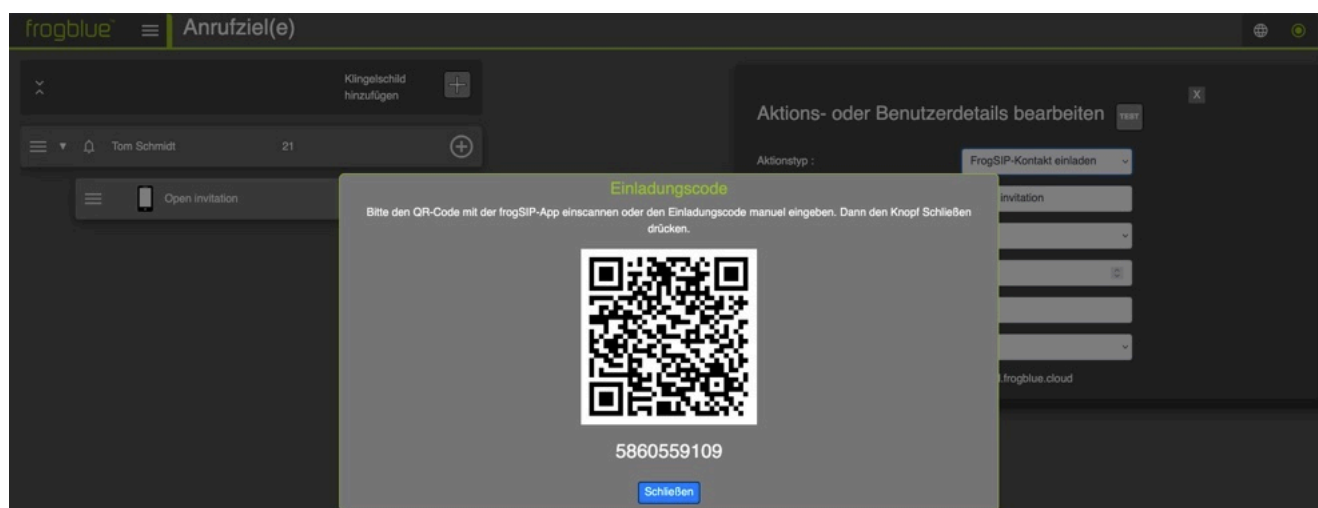
Klingelaktionen können gestapelt werden, indem verschiedene Parameter - wie Zeitpläne und Verzögerungen - verwendet werden, um unterschiedliche Aktionen zu festgelegten Zeiten oder in Folge auszuführen. Weitere Verbesserungen des Aktions- und Ereignissystems sind derzeit in Entwicklung.

Klicken Sie auf **TEST**, um die Klingeltaste direkt über die Weboberfläche zu testen. Die konfigurierten Zielgeräte werden angerufen und die zugewiesenen Aktionen in der festgelegten Reihenfolge ausgeführt. So können Sie prüfen, ob die Klingelziele und Aktionen korrekt eingerichtet sind.

Durch Drücken des  Buttons öffnet sich ein Dialog, in dem Sie aus einer Anzahl von Aktionstypen über das Dropdown-Menü wählen können:

### 8.1.1. Klingelaktionen: frogSIP-Kontakt einladen

Hier können Sie Ihr Terminal mit Smartphones koppeln, auf denen die frogSIP App läuft.

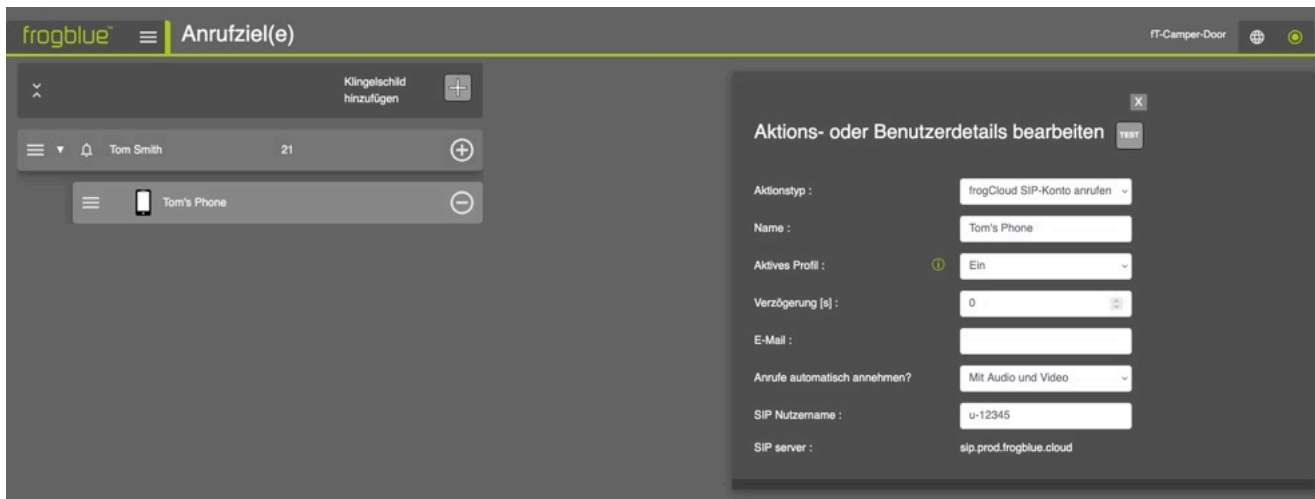


- Wählen Sie **FrogSIP-Kontakt einladen** aus dem Dropdown-Menü
- Scannen Sie den QR-Code oder geben Sie den Einladungscode in der **frogSIP App** ein. Siehe **Abschnitt 5.6 „Kopplung des Terminals mit der frogSIP App“**.

### 8.1.2. Klingelaktionen: frogCloud SIP-Konto anrufen

Verwenden Sie diese Aktion, um einen bestehenden frogCloud-Kontakt über seinen SIP-Benutzernamen anzurufen.

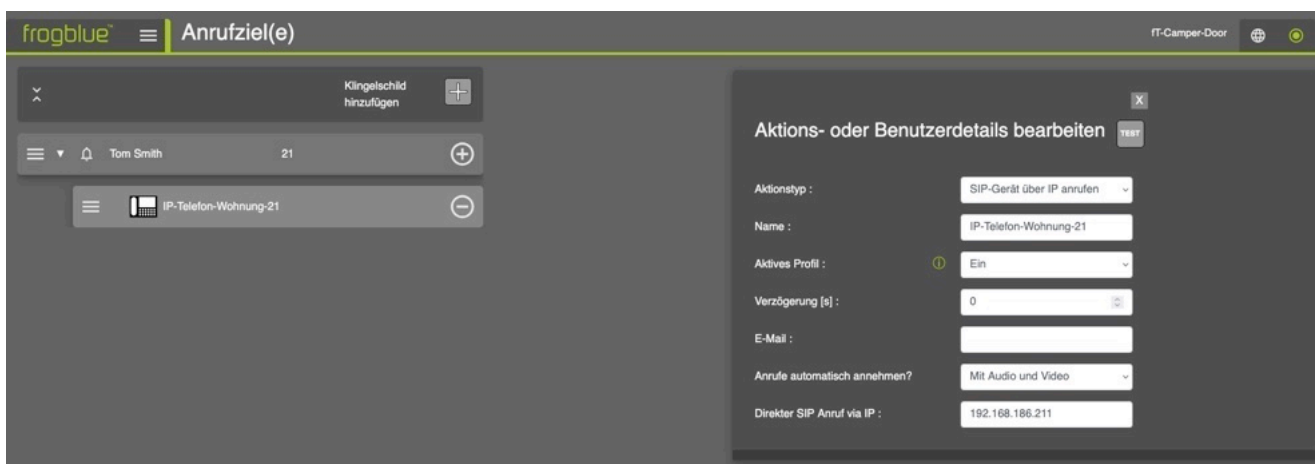
Damit diese Funktion verwendet werden kann, muss die SIP-Freigabe zwischen dem frogTerminal und dem SIP-Benutzer im frogCloud-Projekt unter **SIP Shares** aktiviert sein.



- **Aktionstyp:** Wählen Sie **SIP-Gerät über IP anrufen** aus dem Dropdown-Menü.
- **Name:** Geben Sie einen Namen für die Aktion ein, z. B. „Tom's Phone“.
- **Aktives Profil:** Wählen Sie ein Zeitprofil, in dem das Klingelzeichen aktiv ist.
- **Verzögerung [s]:** Zeit in Sekunden bis zur Ausführung der Anrufaktion.
- **Anrufe automatisch annehmen?:** Sie können den Anruf direkt ablehnen, den Anruf manuell annehmen, oder den Anruf mit Audio und/oder Video beantworten.
- **SIP Nutzername:** Die SIP-Adresse des anzurufenden Benutzers, zum Beispiel „u-12345“. Die SIP-Adresse finden Sie in der frogSIP App des Benutzers unter: **Einstellungen** → **Konnektivität** → **SIP-Konto**
- Klicken Sie auf **Speichern**, um eine neue Aktion für SIP-Anrufe per IP zu erstellen.
- Klicken Sie auf **TEST**, um einen Testanruf direkt aus der Weboberfläche auszulösen. Das konfigurierte Zielgerät wird angerufen, sodass Sie die Einstellungen prüfen können.

### 8.1.3. Klingelaktionen: SIP-Gerät per IP anrufen

Zum direkten Anrufen von SIP-Telefoniegeräten über die IP-Adresse.

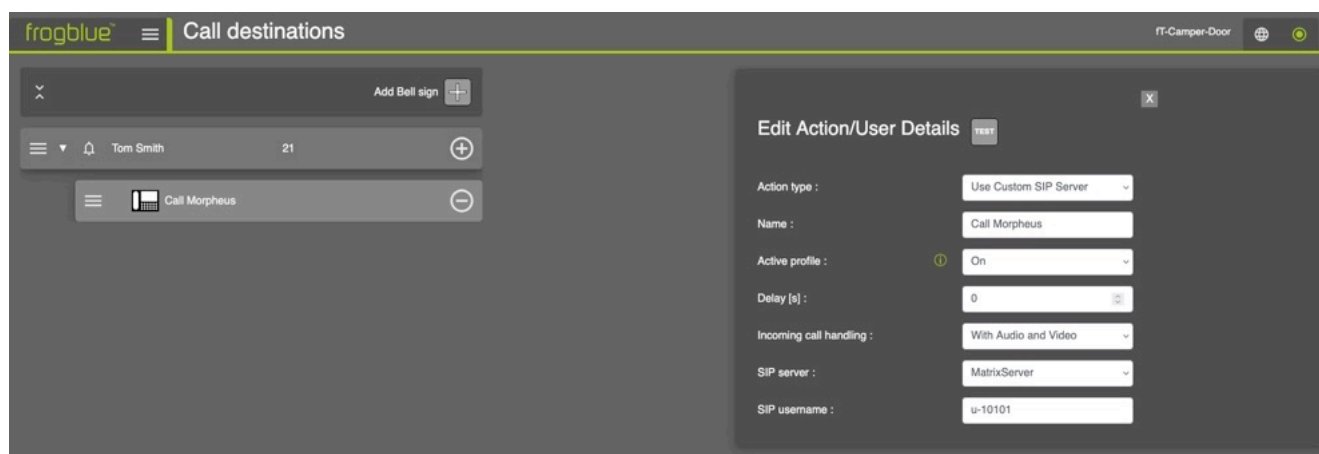


- **Aktionstyp:** Wählen Sie im Dropdown-Menü *SIP-Gerät per IP anrufen* aus.
- **Name:** Geben Sie einen Namen für die Aktion ein, z. B. „IP-Telefon-Wohnung-21“.
- **Aktives Profil:** Wählen Sie ein Zeitprofil aus, in dem das Klingelschild aktiv ist.
- **Verzögerung [s]:** Zeit in Sekunden, bis die Anrufaktion ausgeführt wird.
- **Behandlung eingehender Anrufe:** Legt fest, wie eingehende Anrufe von diesem Benutzer behandelt werden. Sie können den Anruf direkt ablehnen, manuell annehmen oder eine automatische Annahme mit Audio und/oder Video erlauben.
- **Direkte Anruf-IP-Adresse:** Die IP-Adresse des anzurufenden SIP-Telefongeräts.
- Klicken Sie auf **Speichern**, um eine neue SIP-Anrufaktion per IP zu erstellen.

Bei Installation mit einem SIP-Server können Anrufe an jedes Telefon im System getätigt werden. Der SIP-Server muss zuvor konfiguriert werden – siehe **Abschnitt 18.2 „SIP-Server-Registrierung“** für Details.

#### 8.1.4. Klingelaktionen: Benutzerdefinierten SIP-Server verwenden

Verwenden Sie diese Aktion, um SIP-Telefoniegeräte über einen benutzerdefinierten SIP-Server anzurufen.

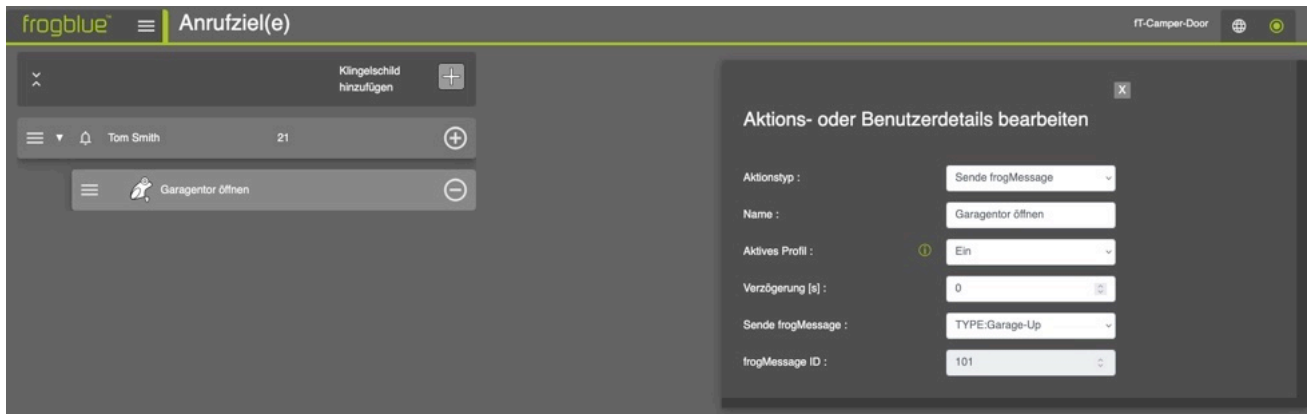


- **Aktionstyp:** Wählen Sie *Benutzerdefinierten SIP-Server verwenden* aus dem Dropdown-Menü aus.
- **Name:** Geben Sie einen Namen für die Aktion ein, z. B. „Morpheus anrufen“.
- **Aktives Profil:** Wählen Sie das Zeitprofil aus, in dem diese Anrufaktion aktiv ist.
- **Verzögerung [s]:** Legen Sie die Zeit in Sekunden fest, bevor die Anrufaktion ausgeführt wird.
- **Behandlung eingehender Anrufe:** Wählen Sie, ob eingehende Anrufe automatisch abgelehnt, manuell angenommen oder automatisch mit Audio und/oder Video beantwortet werden.
- **SIP-Server:** Wählen Sie den benutzerdefinierten SIP-Server aus dem Dropdown-Menü aus, z.B. „MatrixServer“. Siehe **Abschnitt 18.2.2 „SIP-Einrichtung über den Webbrowser“**, um benutzerdefinierte SIP-Server zu konfigurieren.
- **SIP Nutzername:** Geben Sie den SIP Nutzernamen des Kontakts ein, den Sie anrufen möchten, z. B. „u-10101“.
- Klicken Sie auf **Speichern**, um die neue Anrufaktion *Benutzerdefinierten SIP-Server verwenden* zu erstellen.

Wenn das frogTerminal mit einem SIP-Server verbunden ist, können Anrufe an jedes Telefon oder SIP-Gerät durchgeführt werden, das auf diesem System registriert ist. Der SIP-Server muss zuerst konfiguriert werden. Weitere Informationen finden Sie in **Abschnitt 18.2 „SIP-Server-Registrierung“**.

### 8.1.5. Klingelaktionen: frogMessage senden

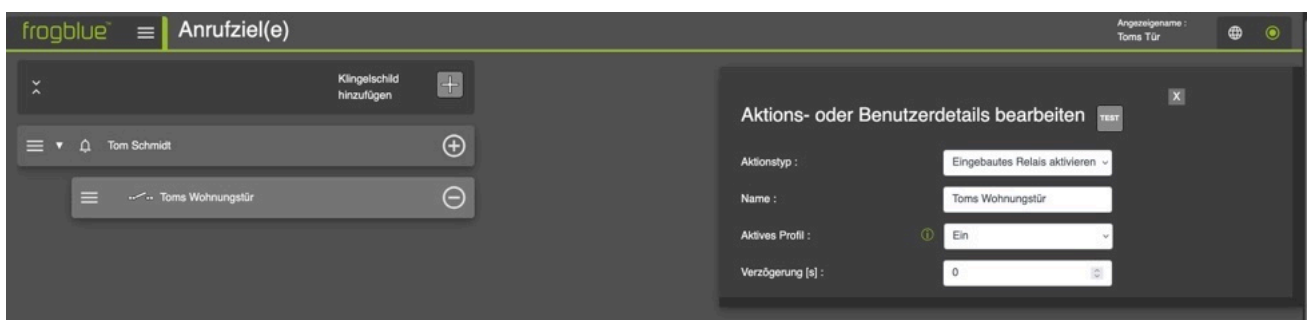
Diese Funktion ermöglicht die nahtlose Integration in das intelligente frogblue-Automatisierungs-Mesh und erlaubt die automatische Steuerung von Licht, Türen, Toren und Rollläden. Dafür muss Ihr frogTerminal für die frogMesh-Integration provisioniert sein – siehe **Abschnitt 17**.



- **Aktionstyp:** Wählen Sie *Sende frogMessage* aus dem Dropdown-Menü.
- **Name:** Geben Sie einen Namen für die Aktion ein, z. B. „Garagentor öffnen“.
- **Aktives Profil:** Wählen Sie ein Zeitprofil, in dem das Klingelzeichen aktiv ist.
- **Verzögerung [s]:** Zeit in Sekunden, bevor die frogMessage ausgeführt wird, z. B. um dem Fahrzeug Zeit zu geben, die Einfahrt zu verlassen, bevor das Garagentor geöffnet wird.
- **Sende frogMessage:** Wählen Sie die frogMessage, die gesendet werden soll, im Dropdown-Menü aus.
- **frogMessage ID:** Eindeutige Kennziffer der frogMessage, die jeder frogMessage beim Erstellen automatisch zugewiesen wird.

### 8.1.6. Klingelaktionen: Hardware-Relais auslösen

Diese Funktion ermöglicht es Ihnen, das integrierte Hardware-Relais des frogTerminals direkt auszulösen. Beispielsweise kann eine Klingeltaste so konfiguriert werden, dass sie ein externes Licht oder ein anderes System über das Relais aktiviert.

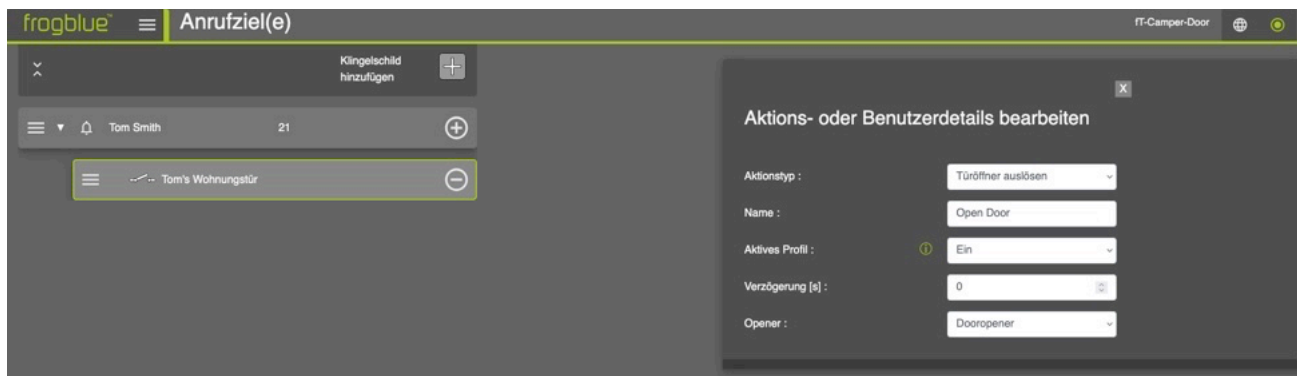


- **Aktionstyp:** Wählen Sie im Dropdown-Menü *Eingebautes Relais aktivieren* aus.
- **Name:** Geben Sie einen Namen für die Aktion ein, z. B. „Tom’s Unit Door“.
- **Aktives Profil:** Wählen Sie ein Zeitprofil, in dem das Klingelzeichen aktiv ist.
- **Verzögerung [s]:** Zeit in Sekunden, bis das Relais geschaltet wird.

### 8.1.7. Klingelaktionen: Türöffner auslösen

Diese Funktion ermöglicht das Auslösen vordefinierter Öffnersequenzen oder Home-Objekte, wie sie unter **Zutrittskontrolle** → **Türen** definiert wurden. Dadurch können mehrere Zutrittspunkte flexibel gesteuert werden.

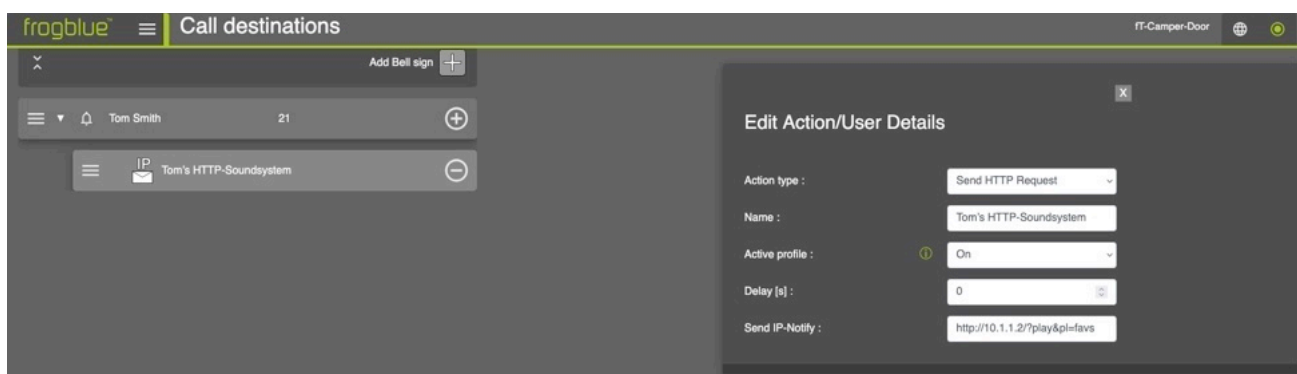
Zum Beispiel kann das System so konfiguriert werden, dass zuerst ein Tor geöffnet wird und nach einer festgelegten Verzögerung, z. B. 20 Sekunden, automatisch das Garagentor geöffnet wird – siehe **Abschnitt 15 „Türsteuerungseinstellungen“** für Details.



- **Aktionstyp:** Wählen Sie im Dropdown-Menü **Türöffner auslösen** aus.
- **Name:** Geben Sie einen Namen für die Aktion ein, z. B. „Tür öffnen“.
- **Aktives Profil:** Wählen Sie ein Zeitprofil aus, in dem das Klingelschild aktiv ist.
- **Verzögerung [s]:** Zeit in Sekunden, bis der Öffner ausgelöst wird.
- **Opener:** Der auszulösende Öffner oder das auszulösende Home-Objekt, z. B. „Türöffner“.

### 8.1.8. Klingelaktionen: HTTP-Anfrage senden

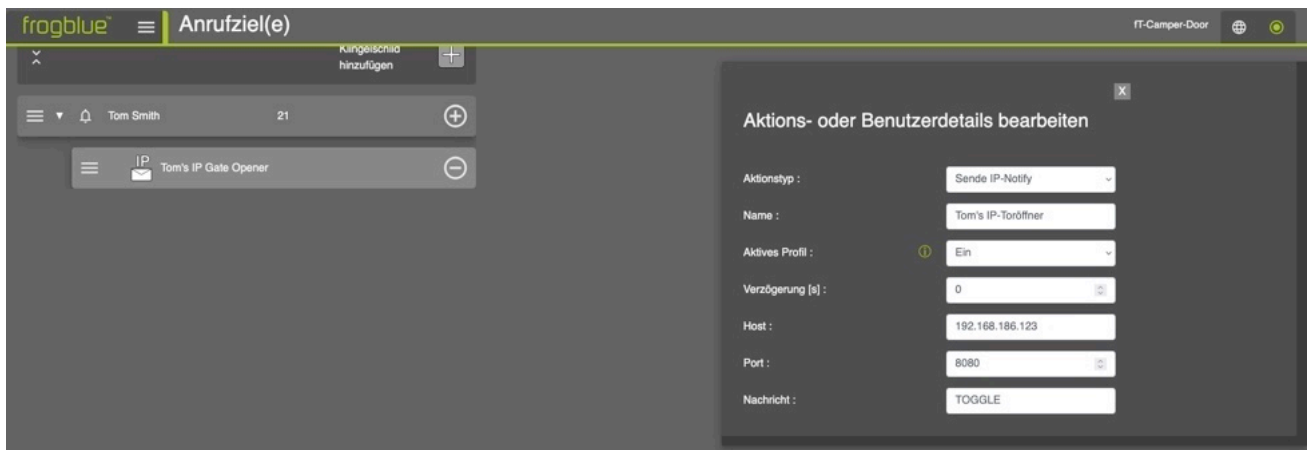
Dies ermöglicht die nahtlose Integration mit HTTP-Geräten von Drittanbietern, sodass eine Klingeltaste HTTP-Anfragen an externe Systeme senden kann, z. B. um ein Soundsystem anzuschalten.



- **Aktionstyp:** Wählen Sie im Dropdown-Menü **HTTP-Anfrage senden** aus.
- **Name:** Geben Sie einen Namen für die Aktion ein, z. B. „Toms HTTP-Soundsystem“.
- **Aktives Profil:** Wählen Sie ein Zeitprofil aus, in dem das Klingelschild aktiv ist.
- **Verzögerung [s]:** Zeit in Sekunden, bis die HTTP-Aktion ausgelöst wird.
- **URL:** Geben Sie die URL ein, die durch diese Aktion ausgelöst werden soll, z. B. „http://10.1.1.2/?play&pl=favs“.
- Klicken Sie auf **Speichern**, um die neue Klingelaktion **HTTP-Anfrage senden** zu erstellen.

### 8.1.9. Klingelaktionen: Sende IP-Notify

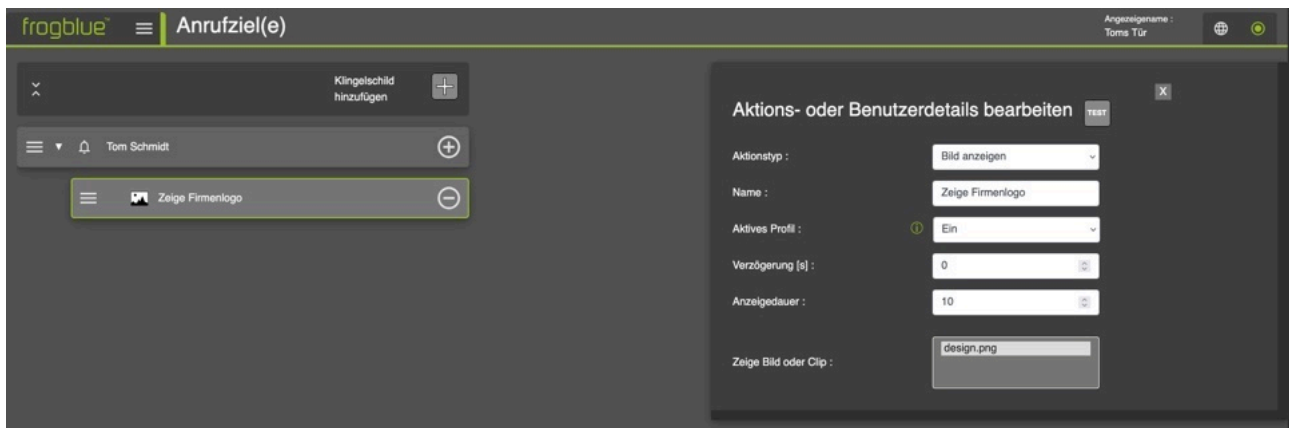
Dies ermöglicht die nahtlose Integration mit IP-Geräten von Drittanbietern, sodass eine Klingeltaste Netzwerkbenachrichtigungen an externe Systeme, z. B. einen IP-Toröffner, senden kann.



- **Aktionstyp:** Wählen Sie *Send IP-Notify* aus dem Dropdown-Menü.
- **Name:** Geben Sie einen Namen für die Aktion ein, z. B. „Tom's IP-Toröffner“.
- **Aktives Profil:** Wählen Sie ein Zeitprofil aus, in dem das Klingelschild aktiv ist.
- **Verzögerung [s]:** Zeit in Sekunden, bis der Öffner ausgelöst wird.
- **Host:** Geben Sie den Hostnamen oder die IP-Adresse des IP-Geräts ein, z. B. „192.168.186.123“.
- **Port:** Geben Sie den Port ein, über den das IP-Gerät Befehle empfängt, z. B. „8080“.
- **Nachricht:** Geben Sie den vom Gerät erwarteten Befehl ein, z. B. den Befehl zum Öffnen des Tores.
- Klicken Sie auf **Speichern**, um die neue Klingelaktion *IP-Notify senden* zu erstellen.

### 8.1.10. Klingelaktionen: Bild oder Clip anzeigen

Diese Funktion zeigt ein vorab geladenes Bild, beispielsweise ein Firmenlogo, auf dem Bildschirm des Terminals an, wenn die Klingeltaste gedrückt wird. Dies verbessert die Markenpräsenz oder liefert den Benutzern ein klares visuelles Signal.

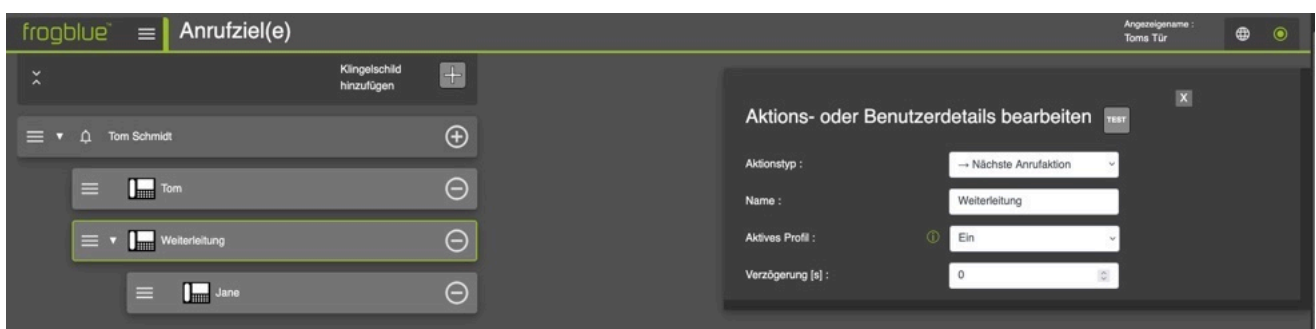


- **Aktionstyp:** Wählen Sie Bild anzeigen aus dem Dropdown-Menü.
- **Name:** Geben Sie einen Namen für die Aktion ein, z. B. „Show Company Logo“.
- **Aktives Profil:** Wählen Sie ein Zeitprofil, in dem das Klingelzeichen aktiv ist.
- **Verzögerung [s]:** Zeit in Sekunden, bis die ausgewählte Datei angezeigt wird.
- **Anzeigedauer:** Zeit in Sekunden, wie lange die ausgewählte Datei angezeigt wird.
- **Zeige Bild oder Clip:** Wählen Sie eine Datei aus, die zuvor auf der Weboberfläche des Terminals unter **Medien** auf das Terminal hochgeladen wurde. Weitere Details finden Sie im **Abschnitt 16 „Onboard-Medieneinstellungen“**.

### 8.1.11. Klingelaktionen: → Nächste Anrufaktion

Die Funktion **Nächste Anrufaktion** bietet eine einfache Möglichkeit, Rufumleitungen oder Anruflketten zu erstellen. Aktionen, die nach einer Nächsten Anrufaktion hinzugefügt werden, gehören zur nächsten Anrufgruppe und werden nur ausgeführt, wenn die vorherige Anrufgruppe nicht beantwortet oder abgelehnt wird.

Es können mehrere Nächste Anrufaktionen verwendet werden, um eine Abfolge von Anrufgruppen zu erstellen, z. B.: Vorverkauf anrufen → Vertrieb anrufen → Vertriebsleitung anrufen.

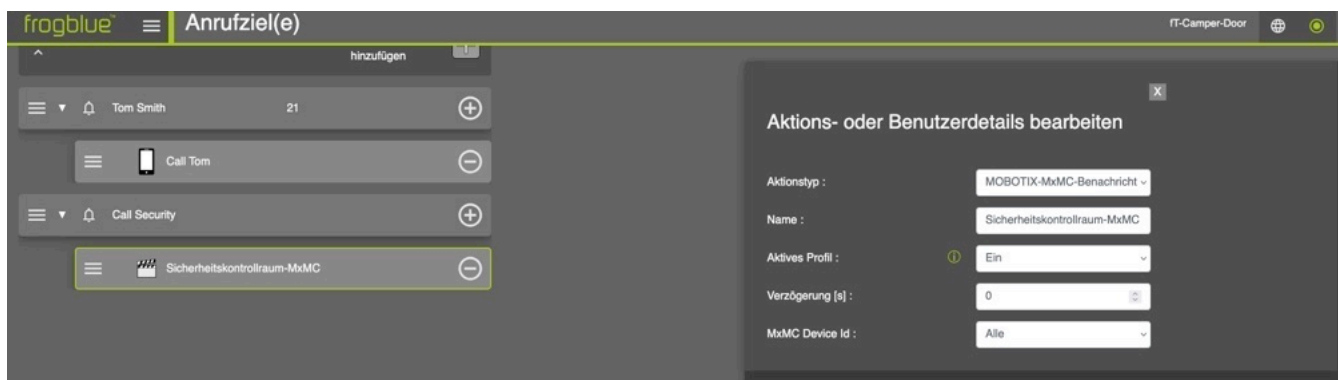


- **Aktionstyp:** Wählen Sie im Dropdown-Menü → **Nächste Anrufaktion** aus.
- **Name:** Geben Sie einen Namen für die Aktion ein, z. B. „Weiterleitung“.
- **Aktives Profil:** Wählen Sie ein Zeitprofil, in dem die Weiterleitung aktiv ist.
- **Verzögerung [s]:** Zeit in Sekunden, bis die Weiterleitung durchgeführt wird.

In diesem Beispiel wird zuerst Tom angerufen. Wenn er den Anruf nicht annimmt oder ablehnt, wird die Anruflkette fortgesetzt und Jane automatisch angerufen. Um die Klingelaktion für Jane hinzuzufügen, klicken Sie wie gewohnt auf das **+**-Symbol neben **Tom Smith**.

### 8.1.12. Klingelaktionen: MOBOTIX-MxMC-Benachrichtigung

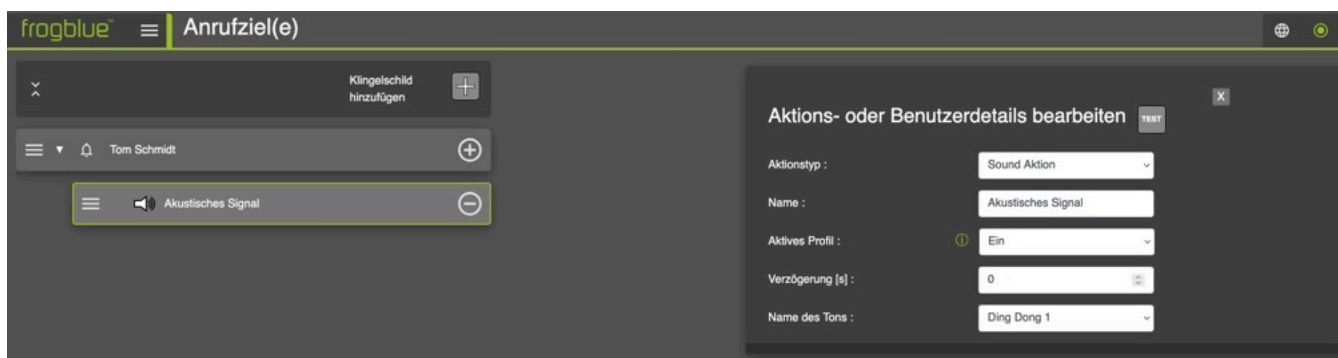
Verwenden Sie diese Aktion, um das MOBOTIX MxManagementCenter zu benachrichtigen, wenn der Klingeltaster gedrückt wird.



- Klicken Sie auf **Klingelschild hinzufügen** **+**, um eine Anrufaktion hinzuzufügen, und wählen Sie die neue Aktion aus, um sie zu bearbeiten.
- **Aktionstyp**: Wählen Sie im Dropdown-Menü **MxMC benachrichtigen** aus.
- **Name**: Geben Sie einen Namen für die Aktion ein, z. B. „Sicherheitskontrollraum-MxMC“.
- **Aktives Profil**: Wählen Sie ein Zeitprofil aus, in dem die Aktion aktiv ist.
- **Verzögerung [s]**: Zeit in Sekunden, bis die Benachrichtigung gesendet wird.
- **MxMC Device ID**: Wählen Sie **Alle**, um alle im Netzwerk laufenden MxMC-Instanzen zu benachrichtigen, oder wählen Sie eine bestimmte Instanz aus der Liste der eindeutigen IDs aus. Die Instanzen werden automatisch erkannt, sobald sich MxMC mit Ihrem frogTerminal verbindet.
- Klicken Sie auf **Speichern**, um die neue Klingelaktion **MxMC benachrichtigen** zu erstellen.

### 8.1.13. Klingelaktionen: Sound Aktion

Das Terminal spielt einen vordefinierten Ton ab, wenn der Klingeltaster gedrückt wird. Diese Funktion ist besonders für Testzwecke nützlich.

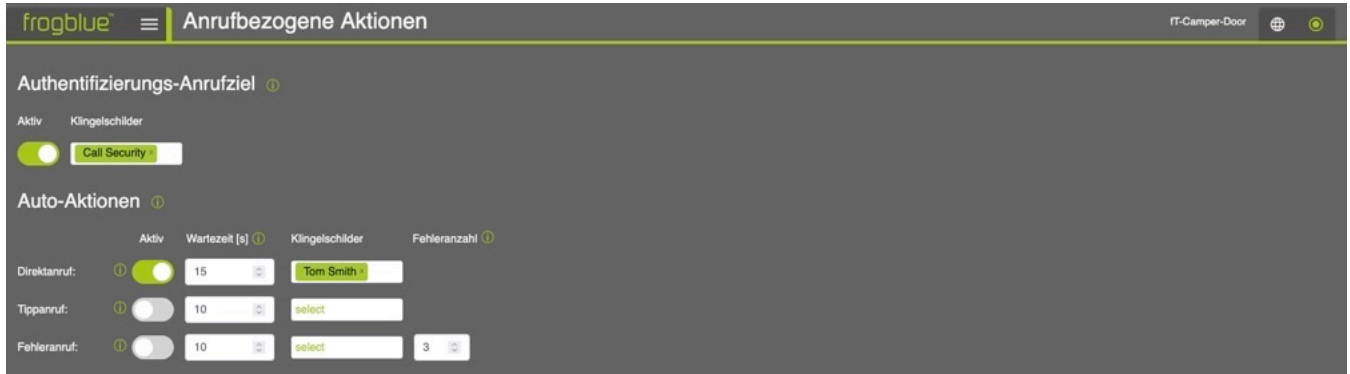


- **Aktionstyp**: Wählen Sie **Sound Aktion** aus dem Dropdown-Menü.
- **Name**: Vergeben Sie einen Namen für Ihre Aktion, z.B. „Akustisches Signal“.
- **Aktives Profil**: Wählen Sie ein Zeitprofil, in dem die Weiterleitung aktiv ist.
- **Verzögerung [s]**: Zeit in Sekunden, bis die Weiterleitung durchgeführt wird.
- **Name des Tons**: Wählen Sie einen Werkston aus dem Dropdown-Menü. Alternativ können Sie eigene Audiodateien verwenden. Diese müssen zuerst unter **Medien** → **Audiodateien** hochgeladen werden. Siehe **Abschnitt 16.1 „Audiodateien“**.

## 8.2. Authentifizierungs-Anrufziel

Über den Webbrowser im Menü: **Kommunikation** → **Anrufbezogene Aktionen**

Konfigurieren Sie das Ziel für Mehrfaktor-**Authentifizierungsanrufe**. Dieser Anruf wird während eines Zutrittsereignisses initiiert, wenn der Authentifizierungsanruf basierend auf der definierten Zutrittsregel ausgelöst wird.



- **Aktiv** einschalten, um Authentifizierungsanrufe zu aktivieren, und die gewünschten Klingelschilder auswählen, die angerufen werden sollen, z. B. „Call Security“.

## 8.3. Automatische Aktionen

Über den Webbrowser im Menü: **Kommunikation** → **Anrufbezogene Aktionen**

Definieren Sie die Anrufziele für Ereignisse oder Fehler am Terminal:

- **Vorschauanruf**: Wird initiiert, wenn die Annäherungs- oder Bewegungssensoren für den angegebenen Verzögerungszeitraum ausgelöst werden und keine Aktion erfolgt, z. B. wenn eine Person eine gewisse Zeit untätig vor dem Terminal steht.
- **Touch-Anruf**: Wird initiiert, wenn der Touchscreen für den angegebenen Verzögerungszeitraum aktiviert wird, ohne dass eine gültige Funktion ausgeführt wird, z. B. bei Verdacht auf Manipulation.
- **Ungültiger Anruf**: Wird initiiert, wenn die Anzahl der Fehler den konfigurierten Schwellenwert überschreitet, z. B. drei aufeinanderfolgende falsche PIN-Eingaben oder ein nicht erkannter Karten-/Schlüssel-Scan.

## 9. Ereignismanagement

Über den Webbrowser im Menü: **Ereignisse & Analysen** → **Ereignismanagement**

Der Bereich **Ereignismanagement** dient zur Konfiguration ereignisbasierter Abläufe im System. Hier legen Sie fest:

- **Ereignisse:** Was passiert
- **Bedingungen:** Unter welchen Umständen das Ereignis eintreten soll
- **Aktionen oder Aktionsketten:** Was das System ausführen soll

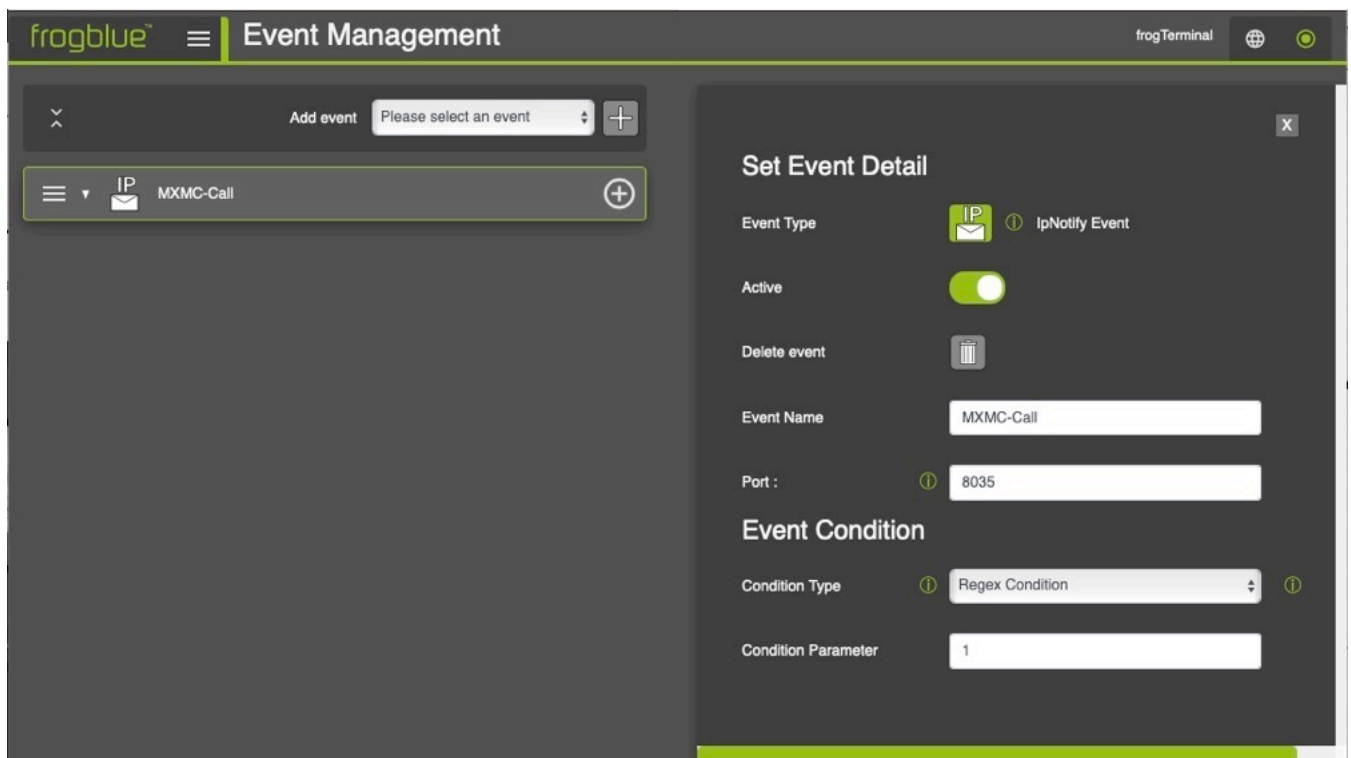
Dies ermöglicht die Umsetzung individuell angepasster Automatisierungslogik, zum Beispiel:

- Wenn eine bestimmte frogMessage empfangen wird (Ereignis) ab 10 Uhr morgens (Bedingung) → Ton abspielen und eine IP-Nachricht senden (Aktion)
- Wenn ein externes System eine IP-Nachricht mit „Tür öffnen“ sendet (Ereignis) → ein HomeObject oder ein lokales Ausgangsrelais auslösen (Aktion)
- Wenn ein SIP-Anruf eingeht (Ereignis) → ein Licht anschalten (Aktion)

### Um ein neues Ereignis hinzuzufügen

1. Wählen Sie den Ereignistyp aus dem **Ereignis hinzufügen** Dropdown-Menü und klicken Sie auf das **+**-Symbol.
2. Es öffnet sich ein Konfigurationsdialog, in dem Sie die Ereignisparameter einstellen können.
3. Speichern Sie das Ereignis.

Der Konfigurationsdialog weist für jeden Ereignistyp einen vergleichbaren Aufbau auf:




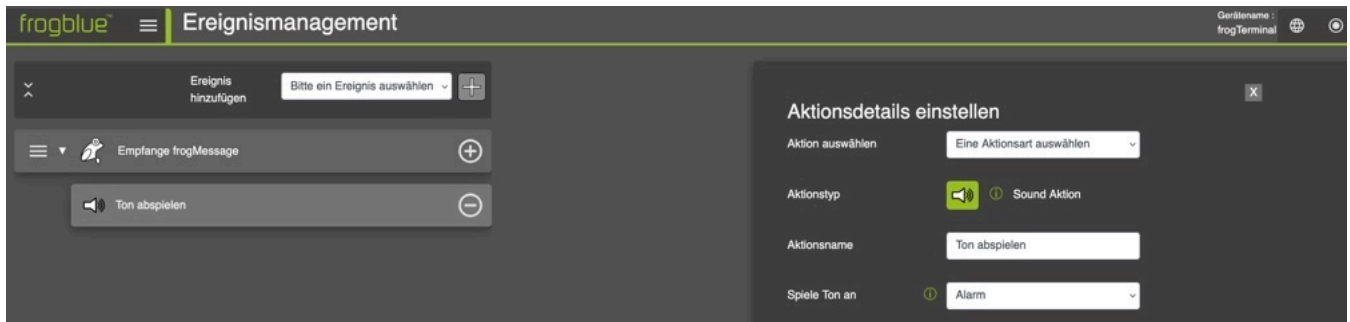
## Ereignisdetails einstellen

- **Aktiv:** Aktivieren or deaktivieren Sie das Ereignis.
- **Ereignis löschen:** Entfernen Sie die Ereigniskonfiguration und alle damit verbundenen Aktionen vollständig.
- **Ereignisname:** Vergeben Sie einen aussagekräftigen Namen für das Ereignis für eine einfache Identifikation.
- **Ereignisparameter:** Das Parameterfeld ändert sich je nach ausgewähltem Ereignistyp. Beispiele hierfür sind:
  - **Port:** <Port to Listen for IP Message Event>
  - **frogMessage Name**
  - **IP Notify String**
  - **Zeitintervall**
  - **Lokale Variable**

## Ereignisbedingung

- **Bedingungstyp:** Der Bedingungstyp legt fest, wann das Ereignis seine Aktionen ausführen soll.
  - **Keine Bedingung:** Die Aktionen werden immer ausgelöst, sobald das Ereignis eintritt.
  - **Regex Bedingung:** Löst nur aus, wenn der empfangene Wert einem Muster der regulären Ausdrücke entspricht.
  - **Wert gleich Bedingung:** Löst nur aus, wenn der empfangene Wert genau mit dem definierten Text übereinstimmt.
  - **Zeittabellen Bedingung:** Löst nur während eines bestimmten Zeitplans aus (kalenderbasierter Ablauf).
  - **Zeitprofil Bedingung:** Löst basierend auf einem zuvor definierten Zeitprofil aus.
  - **Variablen gleich Bedingung:** Löst aus, wenn eine definierte Variable einen bestimmten Wert erreicht. Variablen werden mit einem `\$` definiert, z. B. `\$myVar1`.
  - **Vergleichsbedingung:** Löst aus, wenn eine Vergleichsbedingung erfüllt ist (beispielsweise \$myVar1 ist größer als/kleiner als/gleich \$value)
- **Bedingungsparameter:** Der Bedingungsparameter legt fest, wann das Ereignis seine Aktionen ausführen soll.
  - **Keine:** Die Aktion löst immer aus.
  - **Ja:** Für jede Bedingungsart gilt Folgendes:
    - Wenn der Parameterwert die Bedingung erfüllt, wird die Aktion ausgeführt.

Beachten Sie, dass im oberen Beispiel lediglich ein Ereignis (die frogMessage „Tür“ wird empfangen) und eine Bedingung (Zeitprofil: Shop open) definiert wurden. Bisher wird keine Aktion ausgeführt. Die gewünschte Aktion lässt sich mit einem Klick auf  neben dem Ereignisnamen hinzufügen.



### Aktionsdetails einstellen

- **Aktion auswählen:** Wählen Sie zwischen verschiedenen Aktionen.
- **Aktionstyp:** Zeigt die ausgewählte Aktion.
- **Aktionsname:** Vergeben Sie einen aussagekräftigen Namen für Ihre Aktion. Je nach gewählter Aktion folgen auf den Aktionsnamen verschiedene Einstellungsmöglichkeiten für die jeweilige Aktion.

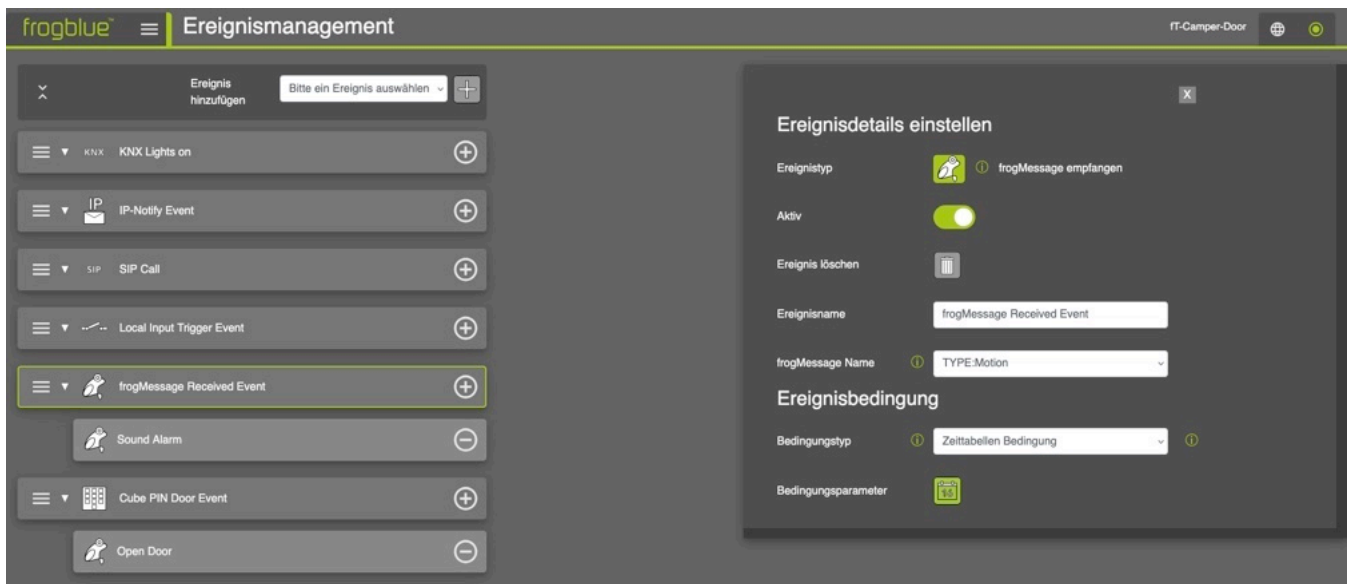
In diesem Beispiel wird ein Ton abgespielt (Aktion), wenn die frogMessage „Tür“ empfangen wird (Ereignis), während das Zeitprofil „Shop open“ aktiv ist (Bedingung).

## 9.1. Ereignisse

Es wird zwischen den folgenden Ereignissen unterschieden:

### 9.1.1. frogMessage empfangen

Dieses Ereignis wird ausgelöst, wenn eine frogMessage empfangen wird. Der Ereignisparameter ändert sich, sodass die entsprechende frogMessage nach Namen ausgewählt werden kann.

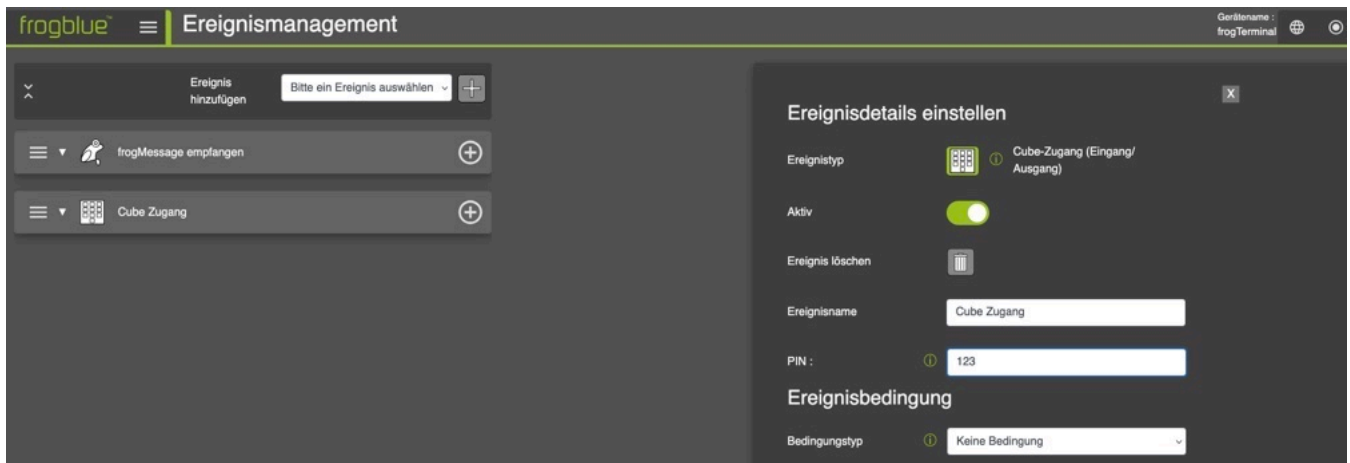


- **frogMessage Name:** Name der frogMessage.
- **Bedingungstyp:** Bedingung, z. B. Zeitprofil.

### 9.1.2. Cube Zugang

Dieses Ereignis wird mit frogblue Cube-Zutrittsgeräten verwendet, z. B. frogAccess1-1. Das Ereignis wird ausgelöst, wenn am Cube eine PIN eingegeben wird.

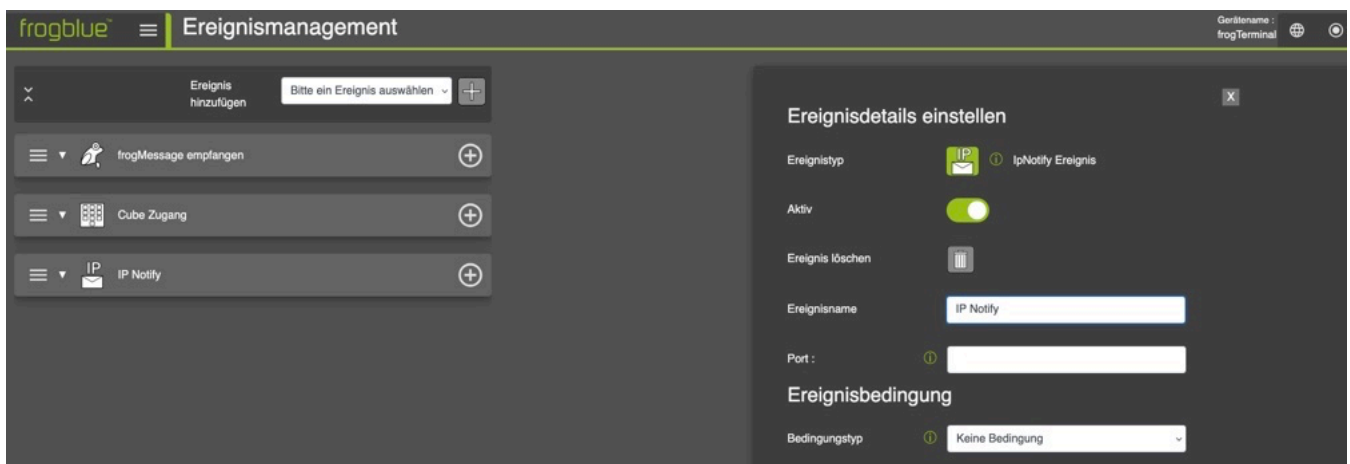
Bevor dieses Ereignis konfiguriert werden kann, muss der Cube mit der frogProject App in das Projekt integriert werden. Nehmen Sie keine Änderungen an der initialen CubeAccess-Konfiguration vor. Schreiben Sie die Konfiguration sowohl auf den Cube als auch auf das frogTerminal.



- **PIN:** Geben Sie eine Funktions-PIN ein, die CubeAccess als PIN-Quelle verwendet.
- **Bedingungstyp:** Bedingung, z. B. Zeitprofil.

### 9.1.3. IP Notify Ereignis

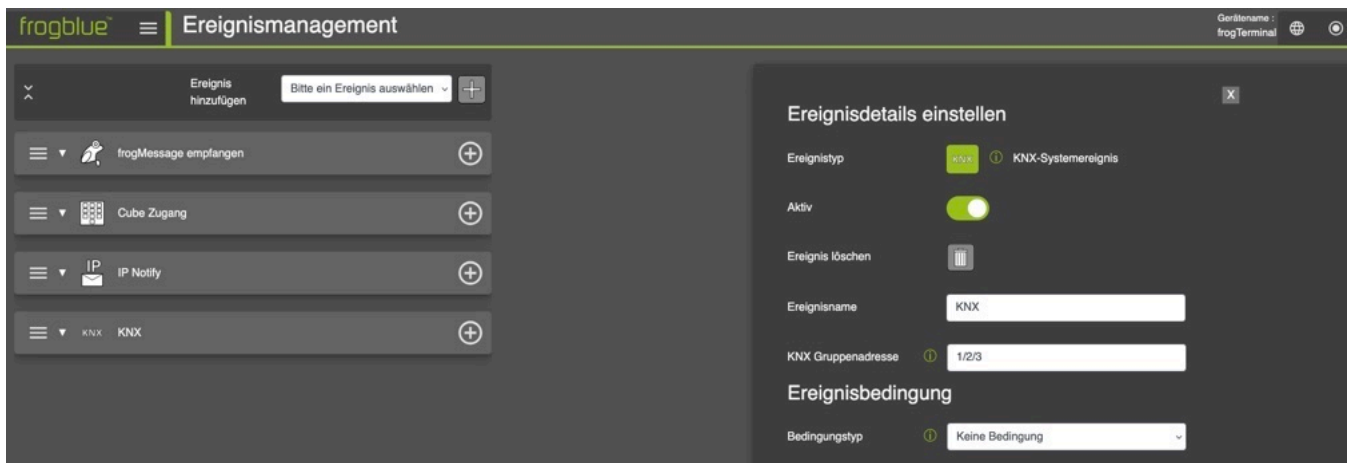
Dieses Ereignis wartet auf eingehende IP-Notify-Nachrichten (TCP/IP).



- **Port:** Standardmäßig wird der unter **System** → **Netzwerk** konfigurierte Port verwendet. Der System-Standardport ist 4806. Alternativ können Sie für dieses Ereignis einen individuellen Port festlegen.
- **Bedingungstyp:** Bedingung, z. B. Wert-gleich-Bedingung. Diese löst nur aus, wenn die eingehende Nachricht mit der definierten Zeichenfolge übereinstimmt, z. B. „IP-MSG-123“.

### 9.1.4. KNX-Systemereignis

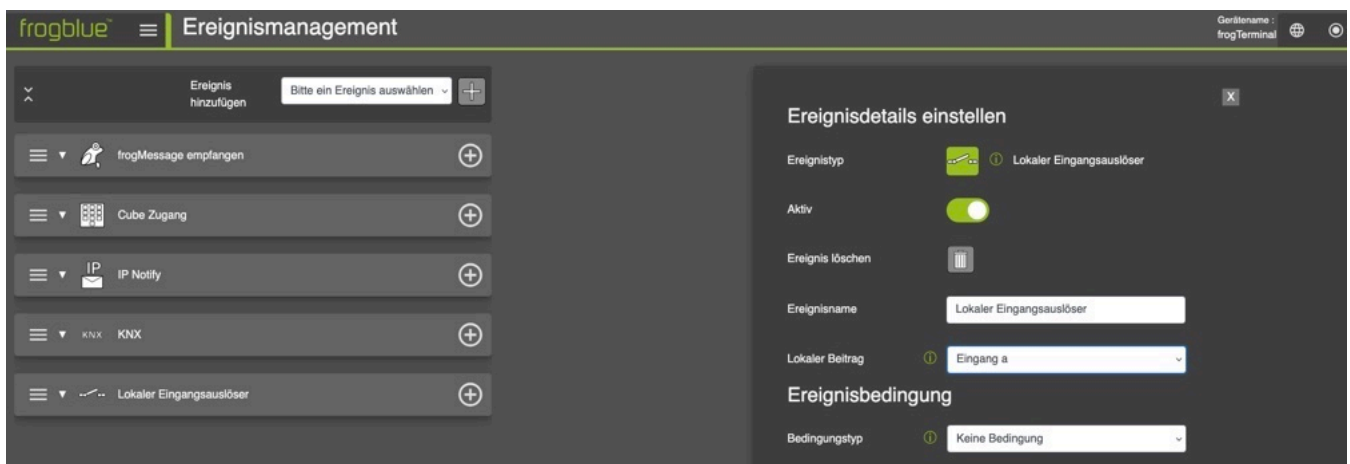
Dieses Ereignis wartet im Netzwerk auf eingehende KNX-Gruppenadressnachrichten.



- **KNX Gruppenadresse:** Geben Sie eine KNX-Gruppenadresse ein. Beispiel: Main/Middle/Sub → „1/2/3“.
- **Bedingungstyp:** Bedingung, z. B. Zeitprofil.

### 9.1.5. Lokaler Eingangsauslöser

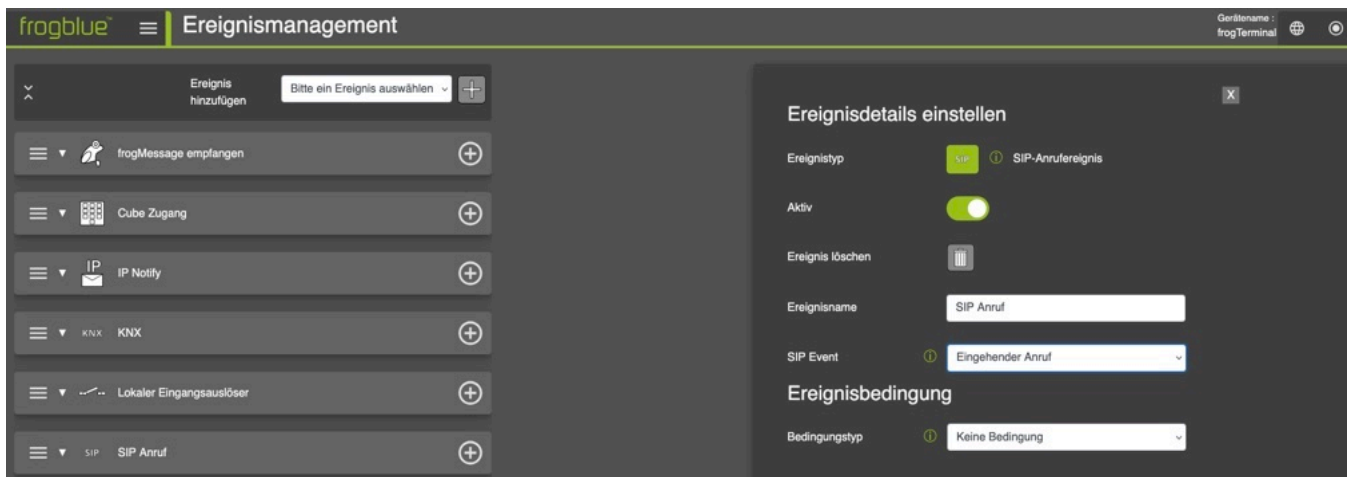
Dieses Ereignis tritt auf, wenn ein Eingangereignis am physischen Eingangsanschluss erkannt wird.



- **Lokaler Eingang:** Wählen Sie den lokalen Hardware-Eingang *a* oder *b*.
- **Bedingungstyp:** Bedingung, z. B. Zeitprofil.

## 9.1.6. SIP-Anrufereignis

Ein eingehendes SIP-Anrufereignis.

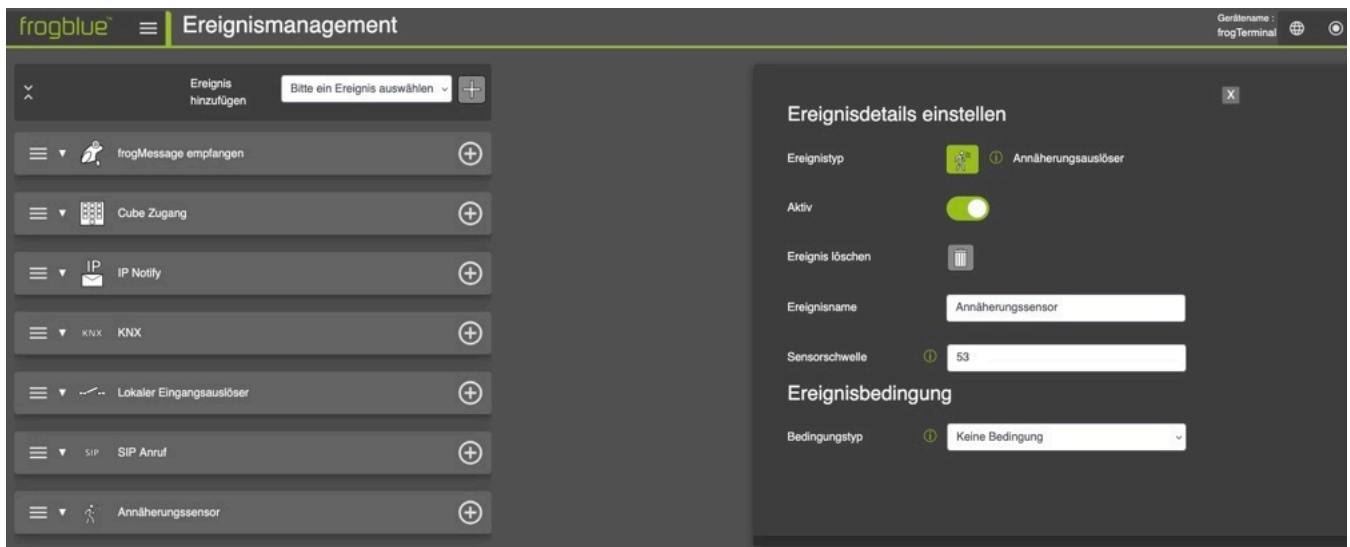


Für ein SIP-Anrufereignis können Sie zwischen verschiedenen **SIP Events** wählen: Das Ereignis tritt ein, sobald

- **Eingehender Anruf:** ein Anruf eingeht.
- **Ausgehender Anruf:** ein Anruf initiiert wird.
- **Anruf beendet:** ein Anruf beendet wird.
- **Starte DTMF Ton:** ein DTMF Ton empfangen wird, erkennt das System - wie bei Drücken einer Zahlentaste im Anruf - den eindeutigen Klang. Dieses Signal löst sofort ein DTMF Ereignis aus, das vom Terminal empfangen und ausgewertet wird.
- **Anruf abgelehnt:** ein Anruf abgelehnt wird.
- **Maximale Klingeldauer erreicht:** die maximale Klingeldauer, die unter **Einstellungen** → **Allgemein** festgelegt ist, erreicht ist.
- **Maximale Anrufdauer erreicht:** die maximale Anrufdauer, die unter **Einstellungen** → **Allgemein** festgelegt ist, erreicht ist.
- **Klingeln:** das Gerät klingelt.
- **Anruf beantwortet:** der Anruf beantwortet wird.
- **Anrufverbindung hergestellt:** eine Verbindung hergestellt ist.

### 9.1.7. Annäherungsauslöser

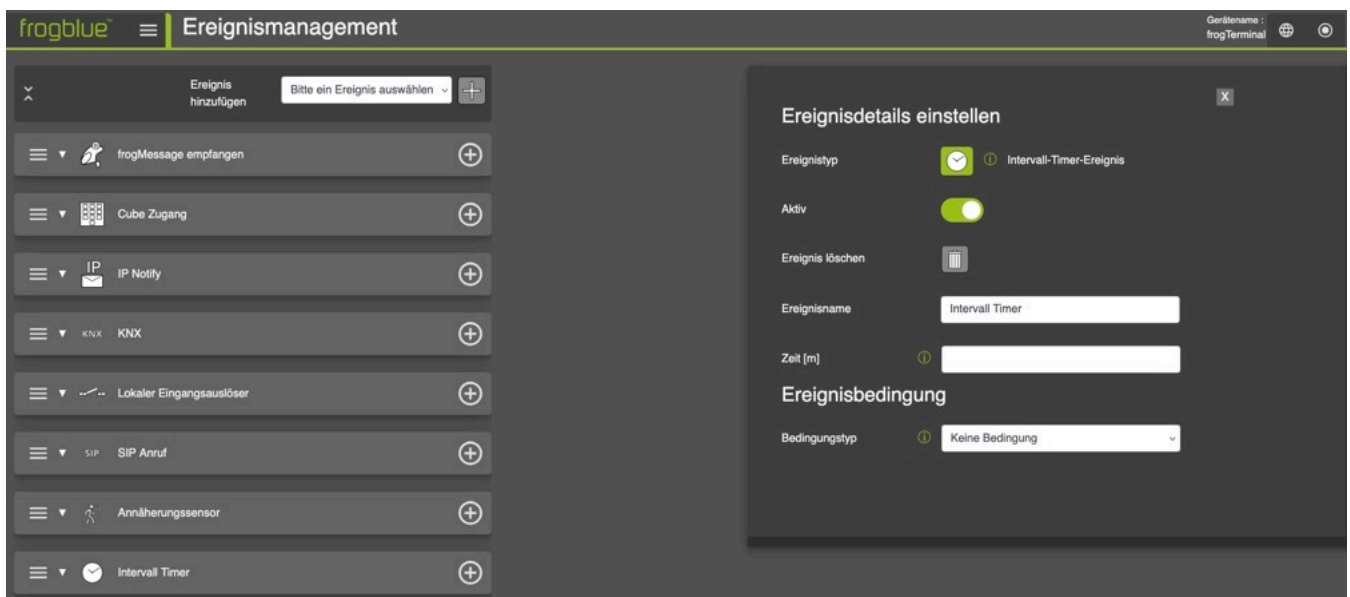
Ereignis, wenn der Näherungssensor die Präsenz eines Objekts erkennt.



- **Sensorschwelle:** Geben Sie den gewünschten Empfindlichkeitsschwellwert für den Näherungssensor ein. Ein höherer Wert führt zu einer kürzeren Erfassungsreichweite.

### 9.1.8. Intervall-Timer-Ereignis

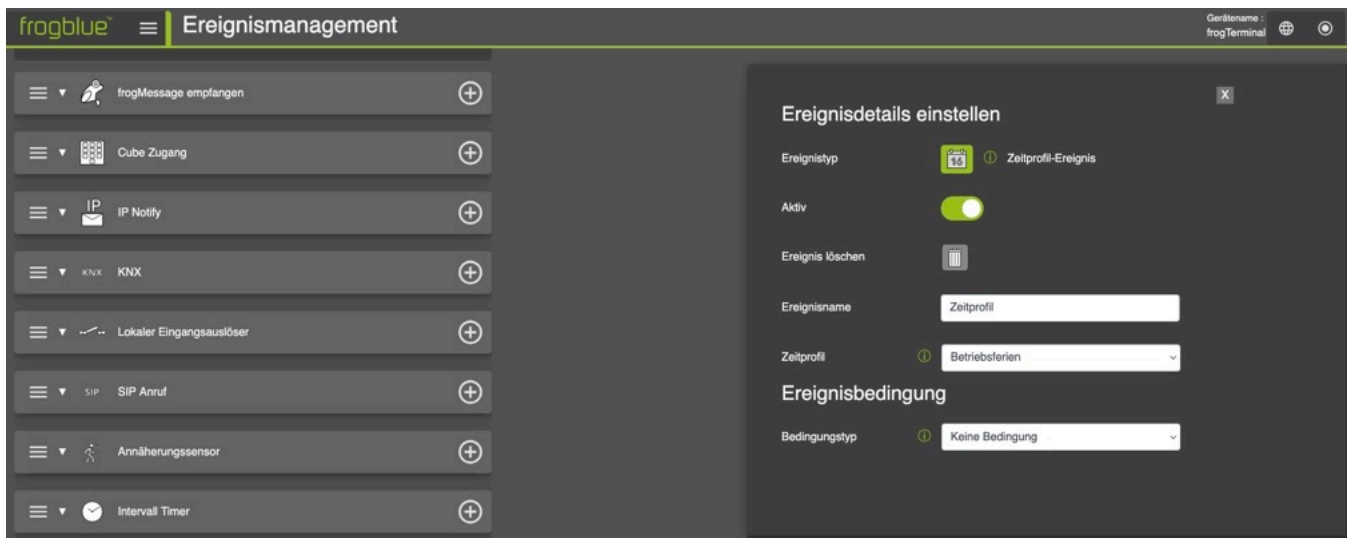
Dieses Ereignis wird nach einer festgelegten Zeit wiederholt ausgelöst.



- **Zeit [m]:** Geben Sie die Zeit in Minuten ein, nach der das Ereignis wiederholt ausgelöst werden soll.
- **Bedingungstyp:** Bedingung, z. B. Zeitprofil.

### 9.1.9. Zeitprofil-Ereignis

Ereignis tritt zu den im Zeitprofil festgelegten Zeitpunkten ein.



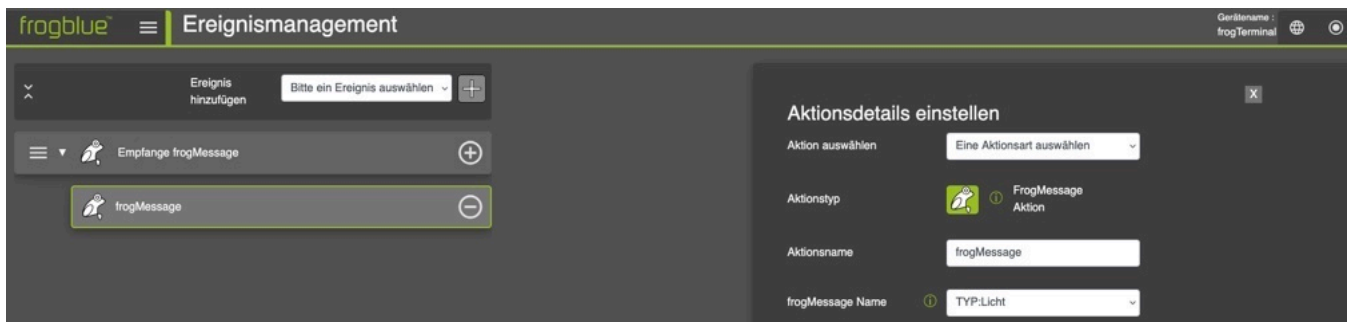
- **Zeitprofil:** Binden Sie ein Zeitprofil ein, das Sie zuvor unter *Einstellungen* → *Zeitprofile* angelegt haben.

## 9.2. Aktionen

Nachdem Sie ein Ereignis festgelegt haben, stehen Ihnen die folgenden Aktionen zur Verfügung:

### 9.2.1. FrogMessage Aktion

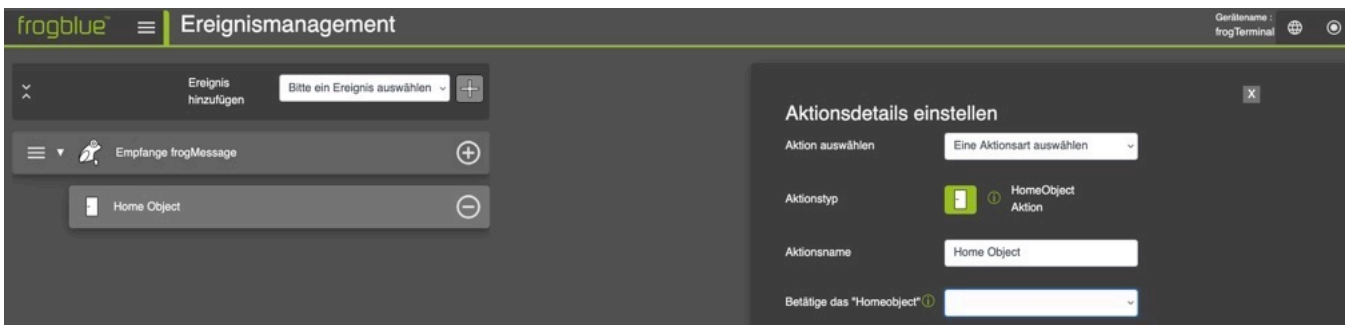
Löst eine frogMessage aus.



- **frogMessage Name:** Wählen Sie eine bestehende frogMessage aus dem Dropdown-Menü.

## 9.2.2. HomeObject Aktion

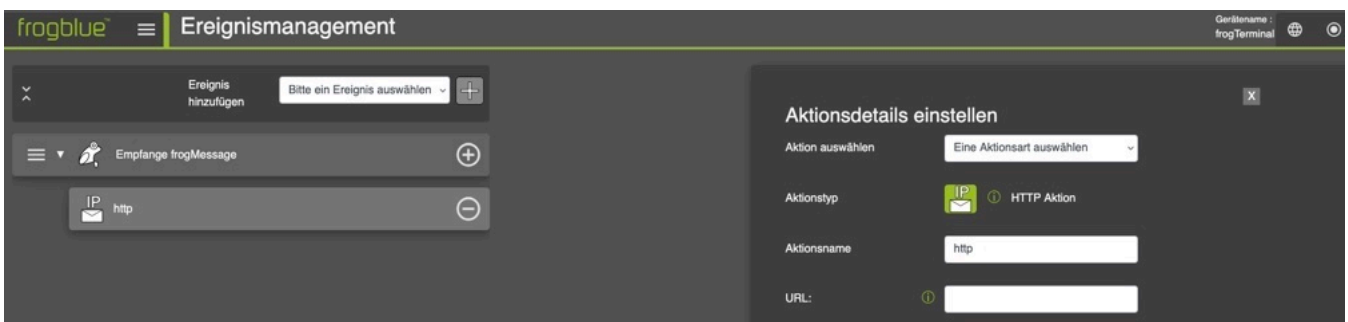
Löst ein HomeObject aus.



- **Betätige das HomeObject:** Wählen Sie ein bereits angelegtes HomeObject aus dem Dropdown-Menü.

## 9.2.3. HTTP Aktion

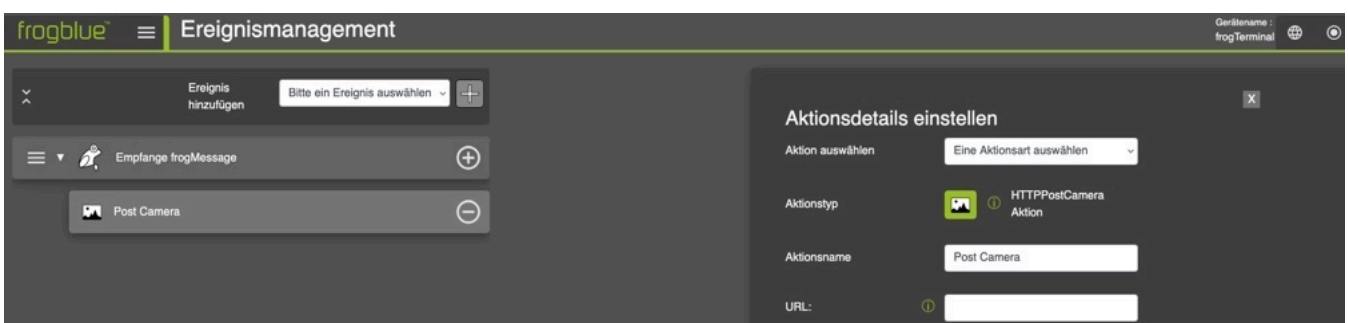
Ruft eine HTTP-Adresse auf.



- **URL:** Geben Sie die URL ein, die aufgerufen werden soll.

## 9.2.4. HTTP Post Camera Aktion

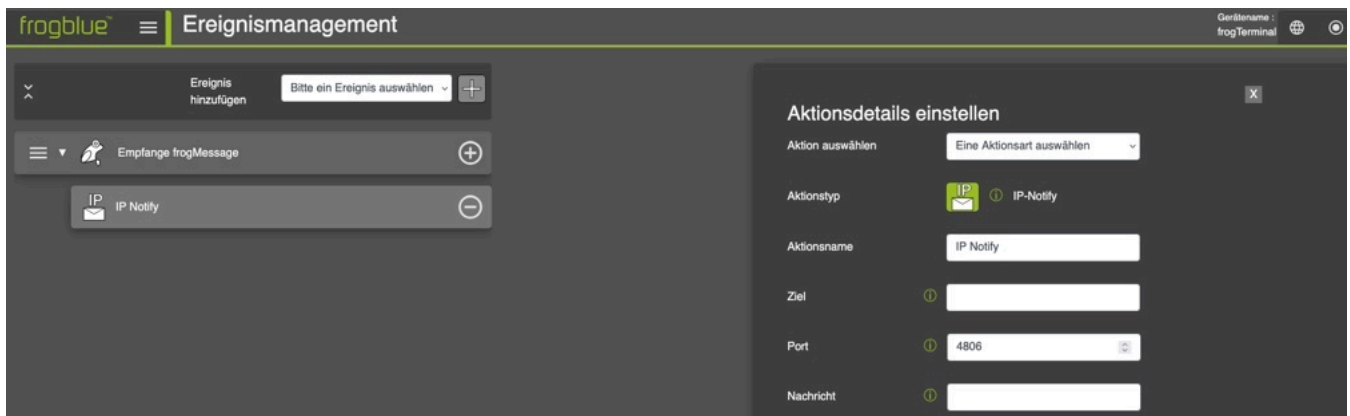
Es wird ein HTTP-Post ausgelöst, der im Body das jetzige Kamerabild enthält.



- **URL:** Wo der Post hingeschickt wird.

### 9.2.5. IP Notify Aktion

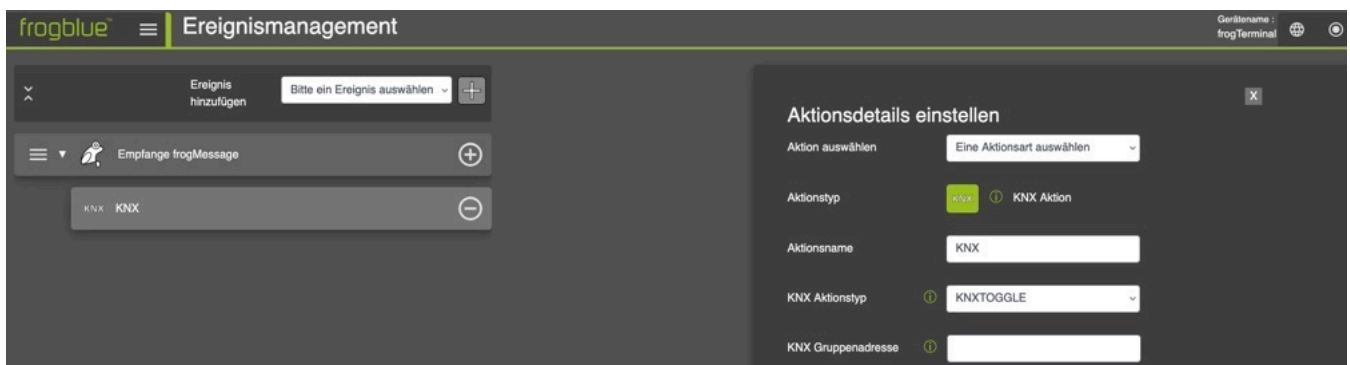
Löst ein IP Notify aus.



- **Ziel:** Geben Sie einen Ziel-Hostnamen oder eine Ziel-IP-Adresse ein.
- **Port:** Geben Sie den Zielport ein. Standardmäßig wird der Port aus **System** → **Netzwerk** genutzt.
- **Nachricht:** Geben Sie die Nachricht ein. „\$value“ wird durch den Wert des Ereignisses ersetzt.

### 9.2.6. KNX Aktion

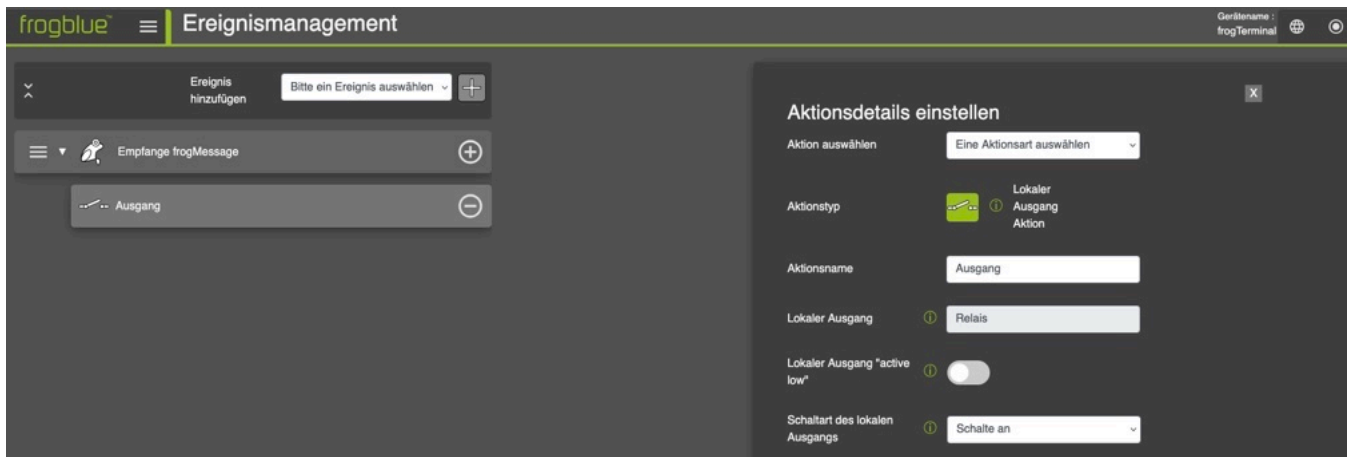
Eine KNX Aktion wird ausgelöst.



- **KNX Aktionstyp:** Wählen Sie zwischen **KNX Toggle** und **KNX SetValue**.
- **KNX Gruppenadresse:** Geben Sie eine KNX-Gruppenadresse ein. Beispiel: *Main/Middle/Sub* → „1/2/3“

## 9.2.7. Lokaler Ausgang Aktion

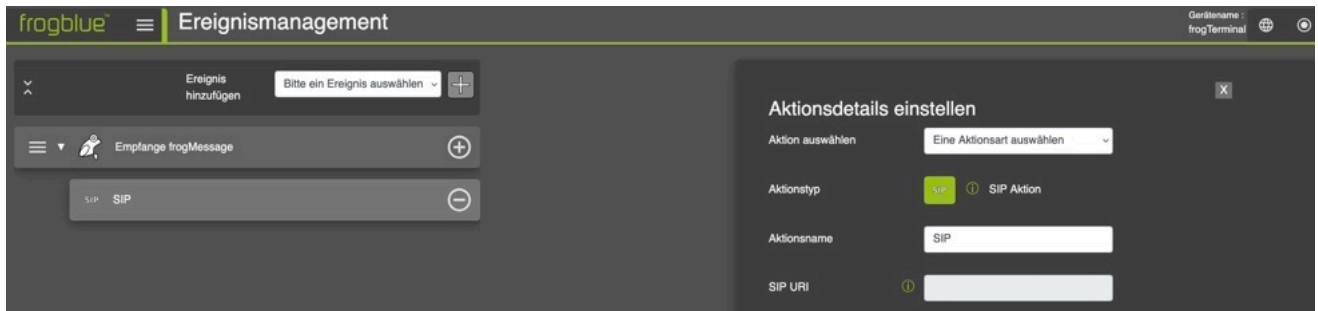
Die Lokale Ausgangsaktion schaltet den lokalen Relaisausgang des frogTerminals. Dies kann zum Beispiel verwendet werden, um einen angeschlossenen Türöffner, eine Torsteuerung, ein Signalgerät oder ein anderes System über den Relaisausgang anzusteuern.



- **Aktion auswählen:** Wählen Sie *Lokale Ausgangsaktion*.
- **Aktionsname:** Geben Sie einen Namen für die Relaisaktion ein. Dieser Name dient zur Identifizierung der Aktion in der Ereigniskonfiguration.
- **Lokaler Ausgang:** Das Aktionsziel wird vom System intern auf Relais gesetzt.
- **Lokaler Ausgang „active low“:** Legt fest, ob die Schaltlogik des Relaisausgangs invertiert wird. Standardmäßig ist diese Option deaktiviert. In diesem Zustand arbeitet der Ausgang mit Active-High-Schaltlogik. Aktivieren Sie den Schalter, wenn das angeschlossene System eine Active-Low-Schaltlogik bzw. eine invertierte Ansteuerung benötigt.
- **Schaltart des lokalen Ausgangs:** Legt fest, wie der Relaisausgang geschaltet wird.
  - **Schalte an:** Schaltet den Relaisausgang ein.
  - **Schalte aus:** Schaltet den Relaisausgang aus.
  - **Wechsel Zustand:** Ändert den aktuellen Relaiszustand. Ist das Relais ausgeschaltet, wird es eingeschaltet. Ist es eingeschaltet, wird es ausgeschaltet.
  - **Schalte an für Zeitdauer:** Schaltet den Relaisausgang für eine festgelegte Zeit ein und danach wieder aus.
  - **Schalte auf Eventwert:** Setzt den Relaisausgang entsprechend dem Wert des auslösenden Ereignisses.
- **Schaltdauer des lokalen Ausgangs in Millisekunden:** Diese Option wird angezeigt, wenn **Für Zeit einschalten** ausgewählt ist. Geben Sie die Dauer in Millisekunden ein, für die der lokale Ausgang aktiv bleiben soll. Zum Beispiel hält ein Wert von 1000 den Ausgang für 1 Sekunde aktiv.

## 9.2.8. SIP Aktion

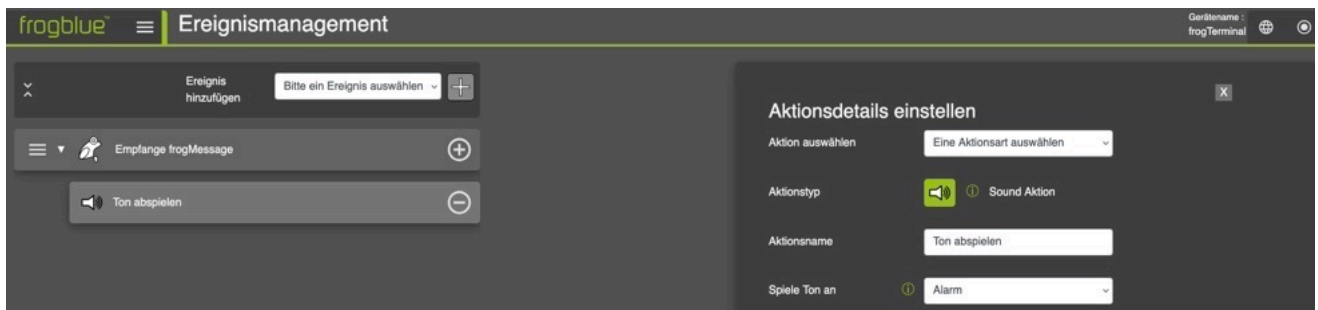
Startet einen SIP-Anruf.



- **SIP URI:** Geben Sie eine SIP-URI ein. Format: `sip:benutzer@host[:port]`.  
Beispiel: „sip:bob.smith@example.com“ oder „sip:1234@192.0.2.1:5060“

## 9.2.9. Sound Aktion

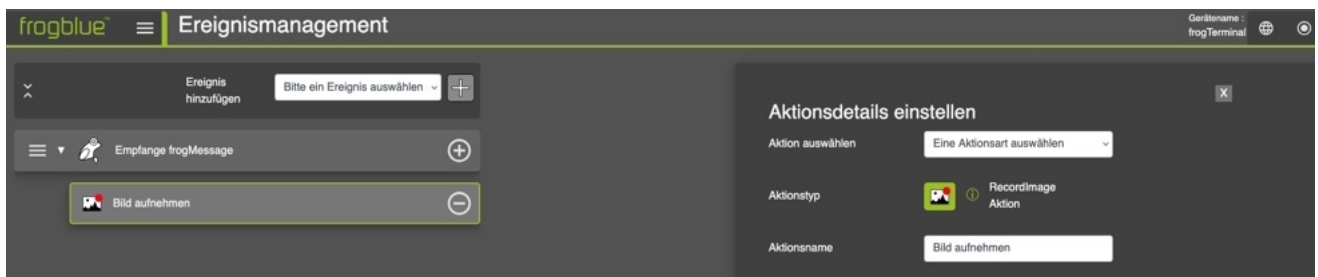
Spielt einen Signalton ab.



- **Spiele Ton an:** Wählen Sie den Signalton, der abgespielt werden soll.

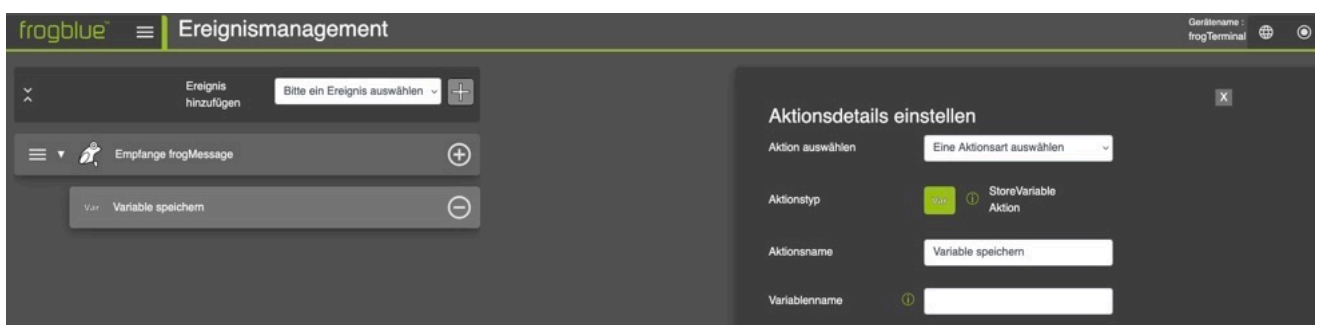
## 9.2.10. RecordImage Aktion

Startet die Bildaufnahme.



## 9.2.11. StoreVariable Aktion

Speichert einen Wert in einer Variablen für einen bestimmten Zeitraum.



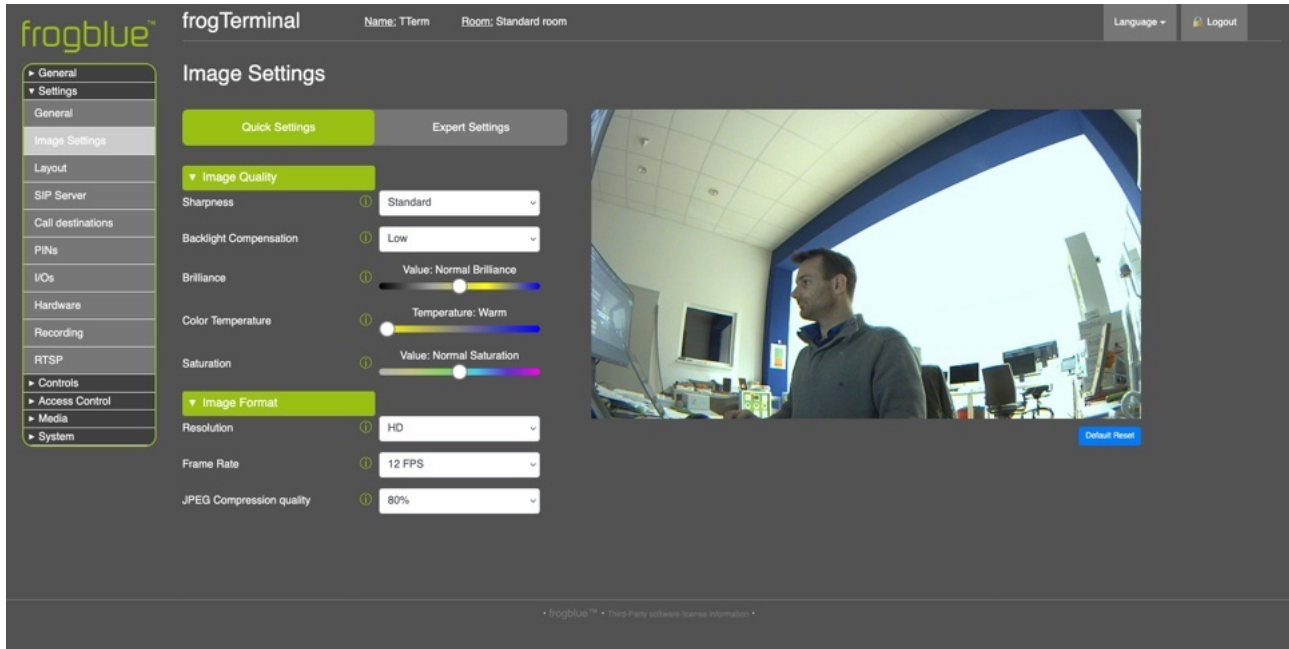
- **Variablenname:** Vergeben Sie einen Variablennamen.

## 10. Kameraeinstellungen und Aufnahmeverwaltung

### 10.1. Konfiguration der Kameraeinstellungen

Über den Webbrowser im Menü: *Einstellungen* → *Bild-Einstellungen*

Passen Sie die Kameraeinstellungen für optimale Videoqualität und Abdeckung an.



#### Bildqualität:

- **Sharpness:** Erhöht die Klarheit von Kanten und feinen Details, was dem Bild entweder ein definierteres, schärferes oder ein glatteres Aussehen verleiht.
- **Backlight Compensation:** Passt die Intensität des Gegenlichts an, um die Sichtbarkeit in dunklen Umgebungen zu verbessern oder Blendung in hellen Szenen zu reduzieren.
- **Brilliance:** Passt den Gesamtkontrast und die Lebendigkeit an, sodass Farben und Details stärker hervortreten.
- **Colour Temperature:** Passt die Wärme oder Kühle der Farben im Bild an und gleicht die Farbnuancen basierend auf der Umgebung (z. B. Sonnenlicht oder Leuchtstofflampen) aus.
- **Saturation:** Steuert die Intensität der Farben, sodass diese kräftiger oder dezenter erscheinen.

#### Bildformat:

- **Resolution:** Bestimmt das Detailniveau im Bild und legt die Klarheit und Pixeldichte des Video-Outputs fest.
- **Frame Rate:** Steuert bzw. begrenzt die Anzahl der Bilder pro Sekunde, was die Flüssigkeit und Glätte des Videos beeinflusst.
- **JPEG Compression quality:** Qualitätseinstellung für die zugrunde liegende JPEG-Kompression.

## 10.2. Optimale Einstellungen für geringe Latenz und hohe Bildrate

Um die beste Leistung mit niedriger Latenz und hoher Bildrate zu erreichen, stellen Sie sicher, dass:

- **Kein browserbasierter HTTPS- oder Web-Stream** aktiv ist (z. B. Kamera-Livestream im Browser).
- Die folgenden **Bildeinstellungen** angewendet werden:
  - **Image Enhancement**: Auf *Aus* gestellt.
  - **Image Resolution**: Auf *maximal HD* eingestellt.
  - **JPEG Compression Quality**: Auf *60%* eingestellt.
- Die **On-Board-Aufzeichnung** ist für optimale Leistung **deaktiviert**. Stattdessen verwenden Sie ein VMS-System zur Videoaufzeichnung.

## 10.3. Ereignis-Aufnahmeeinstellungen

Über den Webbrowser im Menü: **Einstellungen** → **Aufzeichnungen**

- Aktivieren und konfigurieren Sie ereignisbasierte Aufnahmen.
- Konfigurieren Sie die Einstellungen von Vor- und Nachaufnahmen.
- Aktivieren Sie Alarmbenachrichtigungen für fehlgeschlagene Zugriffsversuche.
- Sehen Sie sich aufgezeichnete Ereignisse an und verwalten Sie diese.



### Allgemeine Einstellungen

- **Aufzeichnung aktivieren**: Schaltet die Ereignisaufnahme für die integrierte SD-Karte ein/aus.
- **Auslöseverzögerung**: Legen Sie die Verzögerung zwischen dem Eintreten des Ereignisses und dem Beginn der Aufnahme fest. Dies stellt sicher, dass flüchtige Ereignisse, wie z. B. eine Klingelbetätigung, keine störende Hand abbilden, die einen Teil des Bildes verdeckt.
- **Voralarm Intervall**: Definieren Sie den Zeitraum, in dem die Aufnahme vor dem Auslösen des Ereignisses erfolgt. Dieses Intervall, das die Auslöseverzögerung einschließt, ermöglicht es, Aufnahmen vor dem Ereignis festzuhalten.
- **Vor-Bilder**: Geben Sie an, wie viele Bilder oder Frames vor dem Auslösen des Ereignisses aufgenommen werden sollen.
- **Nachalarm Intervall**: Legen Sie die Dauer der Aufnahme nach dem Auslösen des Ereignisses fest.
- **Nach-Bilder**: Definieren Sie die Anzahl der Bilder oder Frames, die nach dem Auslösen des Ereignisses aufgenommen werden sollen.

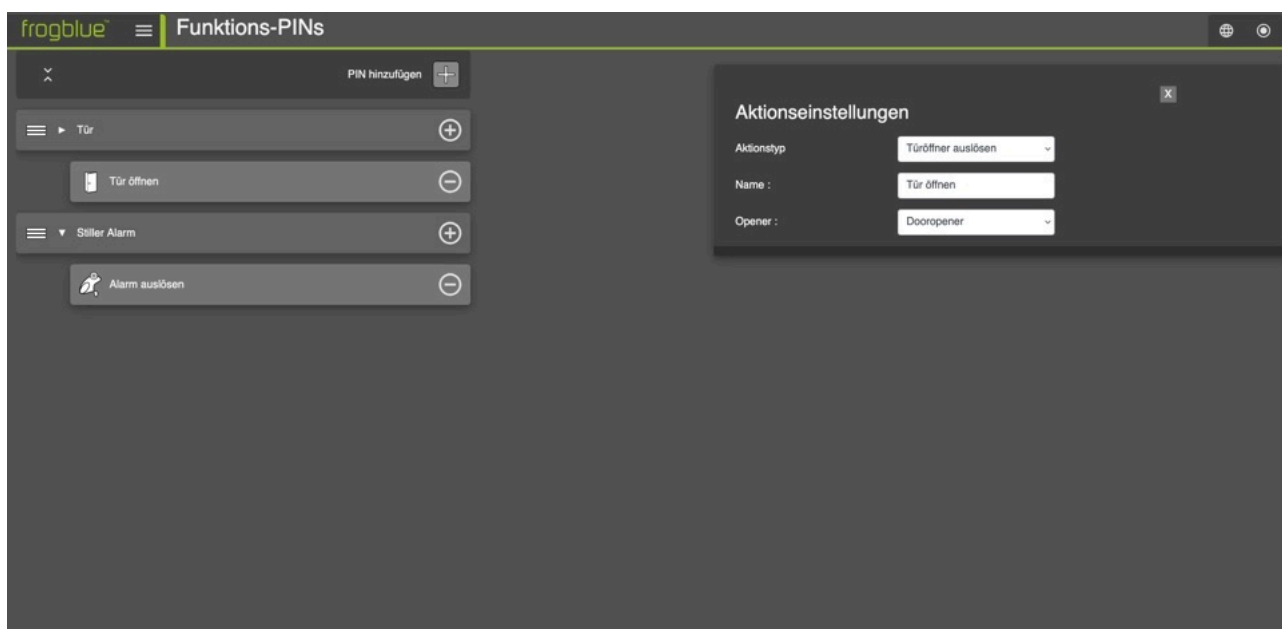
## Zeitraffer

- **Intervall:** Legen Sie das Intervall zwischen Zeitraffer-Aufnahmen fest, um periodische Schnappschüsse zu erfassen.
- **Zeitprofil:** Wählen Sie ein zuvor unter **Einstellungen** → **Zeitprofile** erstelltes Zeitprofil bzw. einen Zeitplan für die Zeitraffer-Aufnahme - beispielsweise Aufzeichnung nur während der Tageslichtstunden, um eine optimale Bildaufnahme sicherzustellen.

## 11. Funktions-PINs

Über den Webbrowser im Menü: **Aktoren** → **Funktions-PINs**

Funktions-PINs können spezifischen Funktionen zugeordnet werden, sodass beispielsweise eine Tür direkt geöffnet, alle Lichter in einem Bereich über frogMessage eingeschaltet oder ein stiller Alarm bzw. Sicherheitsalarm ausgelöst werden kann. Funktionen können ähnlich wie bei Anrufzielen gestapelt werden, sodass Sequenzen oder mehrere Aktionen möglich sind, z. B. Tür öffnen und gleichzeitig einen stillen Alarm auslösen.



**Funktions-PINs:** Eine Funktions-PIN besteht aus eins bis sechs Ziffern, die Länge der PIN ist frei wählbar. Funktion-PINs lösen hinterlegte Funktionen wie das lokale Relais aus oder versenden Nachrichten über IP & Bluetooth.

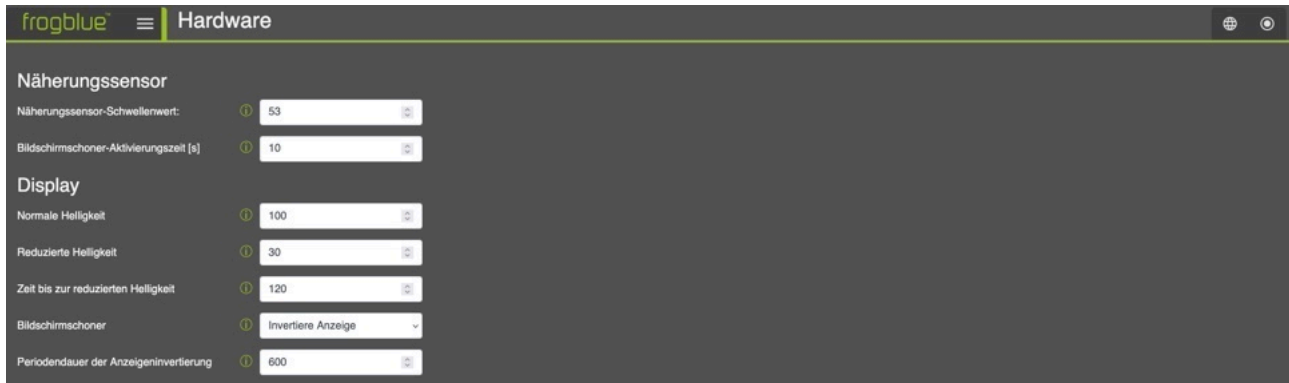
**Hinweis:** Funktions-PINs unterstützen derzeit das Senden von frogMessages, das Auslösen des integrierten Relais, das Starten einer Türöffner-Sequenz, das Senden von IP-Nachrichten oder das Auslösen von Drittanbietersystemen über HTTP-Nachrichten.

## 12. Hardware




### 12.1. Näherungssensor & Touchscreen-Display

Über den Webbrowser im Menü: **Einstellungen** → **Hardware**

Konfigurieren Sie die Aufwach- und Standby-Einstellungen des Terminals.



#### Näherungssensor

- **Näherungssensor-Schwellenwert:** Diese Einstellung bestimmt die Empfindlichkeit des Näherungssensors, niedrigere Werte bedeuten höhere Empfindlichkeit.
- Um den aktuellen Erkennungswert zu visualisieren, navigieren Sie über die Bildschirmenüs des Gerätes (  →  →  ) zu einer Live-Grafik der Näherungssensorwerte.
- **Bildschirmschoner-Aktivierungszeit [s]:** Zeit in Sekunden ohne Aktivität, nach der das Terminal automatisch in den Bildschirmschoner oder den Startbildschirm wechselt.

#### Display

- **Normale Helligkeit [%]:** Diese Einstellung bestimmt die Helligkeit des Terminaldisplays bei Aktivierung, z. B. durch Berührung oder Näherung.
- **Reduzierte Helligkeit [%]:** Diese Einstellung bestimmt die Helligkeit des Terminaldisplays im Standby-Modus.
- **Zeit bis zur reduzierten Helligkeit [s]:** Zeit in Sekunden, nach der die Helligkeit reduziert wird und das Terminal im Standby-Modus verbleibt, bis eine Berührung, Bewegung oder ein anderer Auslöser erfolgt.

### 12.2. Ein- / Ausgabe-Einstellungen

Über den Webbrowser im Menü: **Einstellungen** → **Hardware**

Richten Sie die Hardware-Eingänge und Relais-Ausgangseinstellungen für Ihr frogTerminal ein.



**Eingänge (Eingang A / Eingang B):** Konfigurieren Sie die physischen Eingänge A und B, um Aktionen basierend auf Zustandsänderungen auszulösen.

- **Steigende Flanke:** Wird aktiviert, wenn der Eingang von niedrig nach hoch wechselt.
- **Fallende Flanke:** Wird aktiviert, wenn der Eingang von hoch nach niedrig wechselt.
- **Wählen Sie die Aktion für den Eingang:**
  - **Klingelschild:** Wählen Sie den Klingel-Eintrag aus, der einen Anruf auslösen soll, wenn dieser Eingang aktiviert wird.
  - **BT-Nachricht:** Senden Sie eine Bluetooth-Nachricht über frogMesh.
  - **Relais:** Aktivieren Sie das Hardware-Relais.
  - **IP-Notify:** Senden Sie eine IP-Nachricht oder HTTP-Anfrage an eine bestimmte URL.
  - **Sound abspielen:** Wählen Sie eine Audiodatei (z. B. einen Klingelton) aus, die abgespielt wird, wenn der Eingang aktiviert wird.

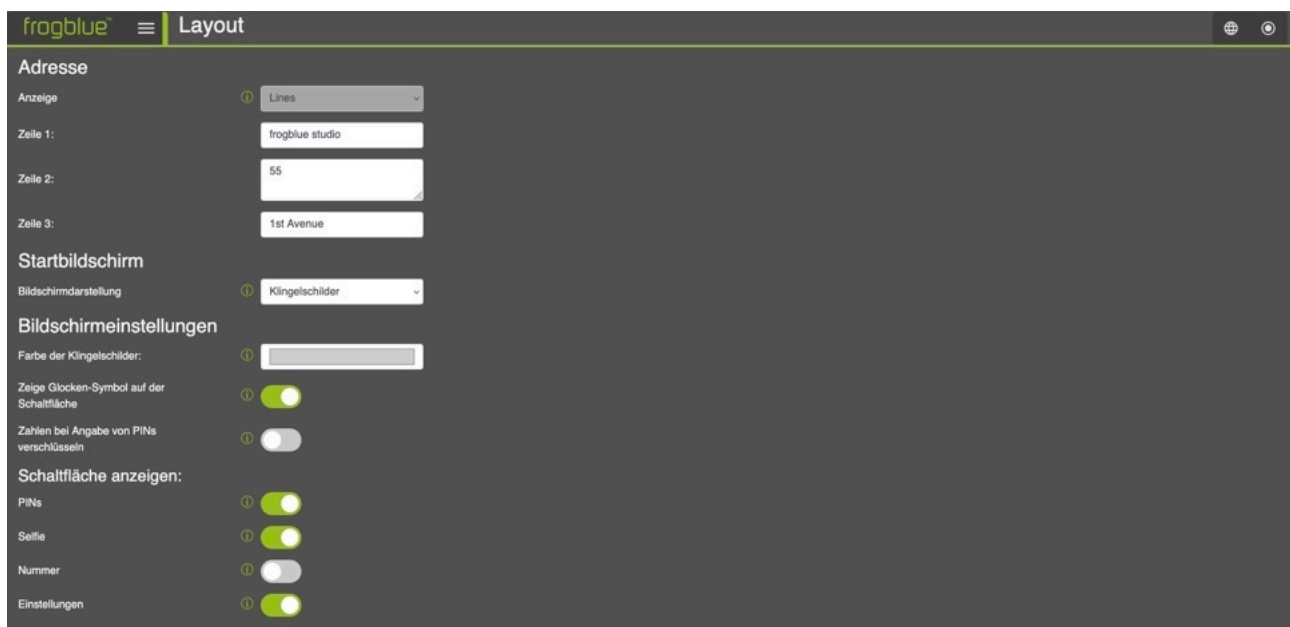
**Ausgang:** Legen Sie die physischen Relais-Ausgangseinstellungen fest:

- **Ausgang/Relais:** Wählen Sie zwischen einem positiven oder negativen Impuls.
- **Dauer [s]:** Definieren Sie die Dauer in Sekunden, in der das Relais ausgelöst wird.

## 13. Touchscreen-Display-Layout

Über den Webbrowser im Menü: **Einstellungen** → **Layout**

Konfigurieren Sie das Home Screen Layout, das auf dem Gerätetouchscreen Ihres Terminals erscheint.

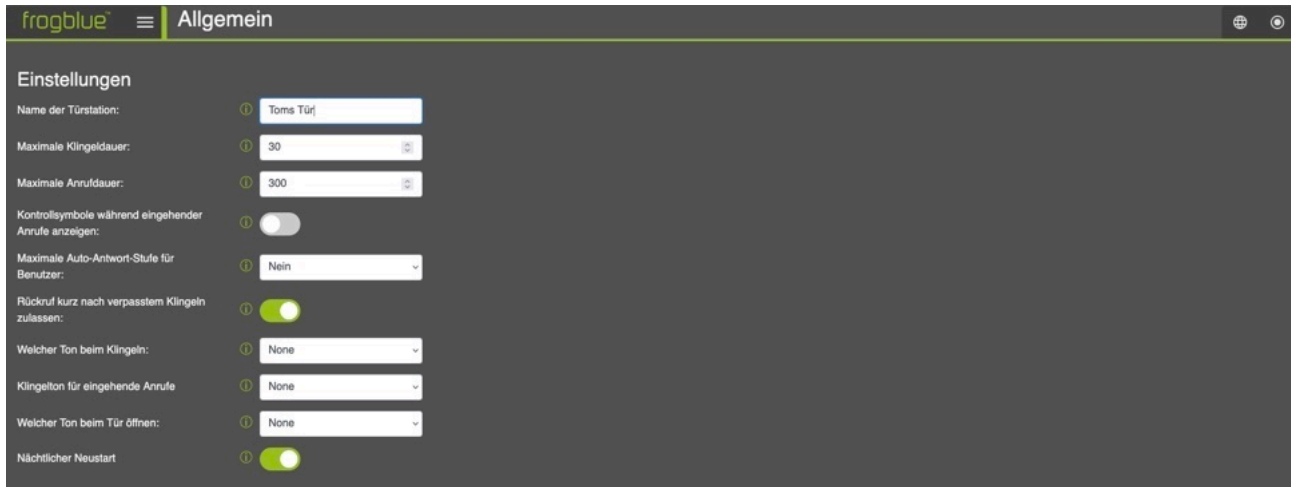


- **Adresse:** Die Einstellungen für das Layout des Standby-Bildschirms.
- **Startbildschirm/Bildschirmeinstellungen:** Die Einstellungen für den Startbildschirm.

## 14. Allgemeine Terminal-Einstellungen

Über den Webbrowser im Menü: *Einstellungen* → *Allgemein*

Konfigurieren Sie allgemeine Einstellungen wie den Namen und die Standard-Klingeleinstellungen.



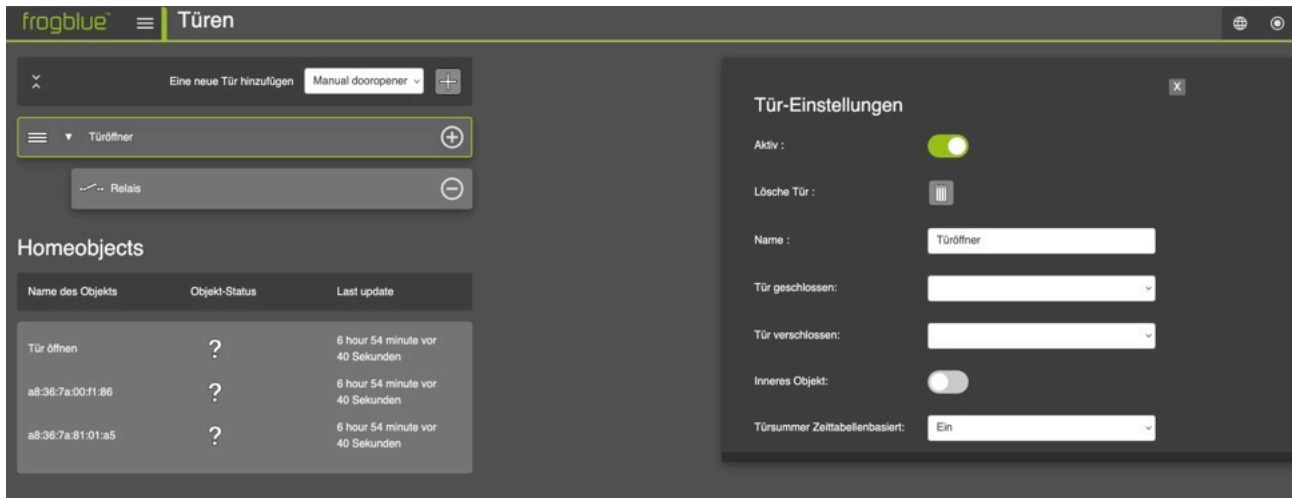
### Einstellungen

- **Name der Türstation:** Geben Sie den Namen für Ihr frogTerminal ein, z. B. „Toms Tür“, um das Gerät in Ihrem System zu identifizieren.
- **Maximale Klingeldauer:** Legen Sie die maximale Zeit fest, die das Terminal versucht, bei einem Angerufenen zu klingeln, bevor es aufgibt.
- **Maximale Anrufdauer:** Legen Sie die maximale Anrufdauer fest, nach der das Terminal automatisch auflegt.
- **Kontrollsymbole während eingehender Anrufe anzeigen:** Blendet die Symbolleiste automatisch ein, wenn ein Anruf eingeht (z. B. um Video ein- oder auszuschalten).
- **Maximale Auto-Antwort-Stufe für Benutzer:** Legen Sie das zulässige Level für die automatische Anrufbeantwortung fest:
  - **Ablehnen:** Alle eingehenden Anrufe automatisch ablehnen.
  - **Nein:** Eingehende Anrufe nicht zulassen; keine SIP-Verbindungen werden akzeptiert.
  - **Automatisch Annehmen:** Automatische Anrufbeantwortung aktivieren. Individuelle Benutzerberechtigungen müssen weiterhin im Menü der Anrufzielaktionen konfiguriert werden (klicken Sie auf den „i“-Button neben dem Aktionseintrag eines Benutzers, um die Anrufbeantwortung am Terminal für diesen Benutzer zuzulassen).
- **Rückruf kurz nach verpasstem Klingeln zulassen:** Nach einem verpassten Anruf ermöglicht diese Funktion dem Benutzer oder dem angerufenen Telefon, zurückzurufen und den Anruf automatisch beantworten zu lassen. Sie überschreibt andere Einstellungen zur automatischen Beantwortung und Berechtigungen.
- **Welcher Ton beim Klingeln:** Ton, der beim Drücken der Klingel am Terminal abgespielt wird.
- **Klingelton für eingehende Anrufe:** Ton für eingehende Anrufe am Terminal
- **Welcher Ton beim Tür öffnen:** Der Ton, der am Terminal abgespielt wird, wenn die Tür geöffnet wird - nützlich, um die Person darauf aufmerksam zu machen, dass die Tür jetzt offen ist, insbesondere bei geräuschlosen Türöffnern.
- **Nächtlicher Neustart:** Das Terminal wird automatisch zwischen 2 und 3 Uhr neu gestartet.

## 15. Türsteuerungseinstellungen

Über den Webbrowser im Menü: **Aktoren** → **Türen**

Konfigurieren sie den lokalen Türöffner, "HomeObjects" und die Steuerungsmöglichkeiten der frogSip App.



## 16. Onboard-Medieneinstellungen

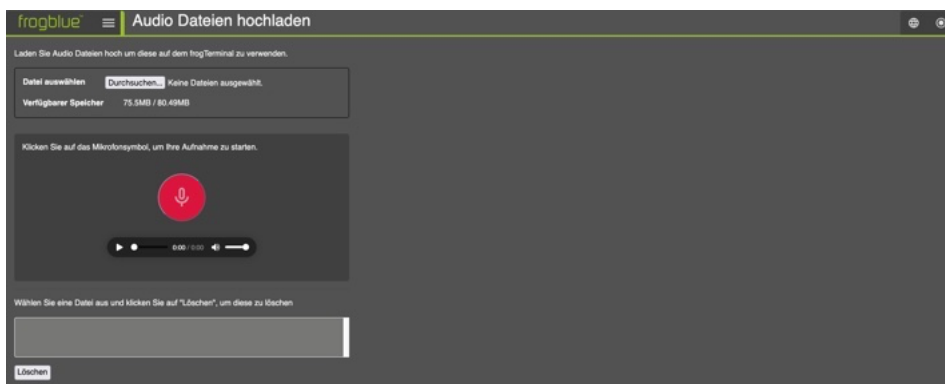
Über den Webbrowser im Menü: **Medien**

Laden Sie Audio-, Bild- und Videodateien hoch und verwalten Sie die Aufzeichnungen der lokalen Events.

### 16.1. Audio-Dateien

Über den Webbrowser im Menü: **Medien** → **Audiodateien**

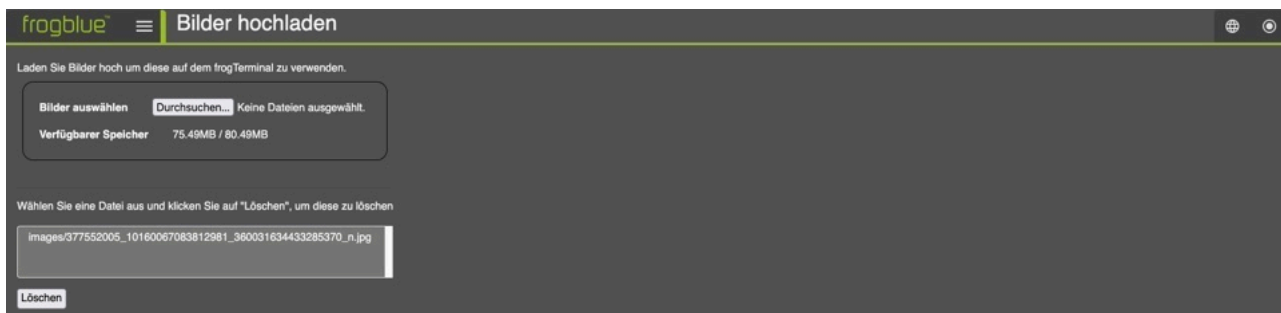
Ermöglicht die Verwaltung und das Hochladen benutzerdefinierter Audiodateien, die im frogTerminal verwendet werden können, z. B. für benutzerdefinierte Klingeltöne, Sprach- oder Soundbenachrichtigungen oder -alarme.



## 16.2. Bilddateien

Über den Webbrowser im Menü: **Medien** → **Bilder**

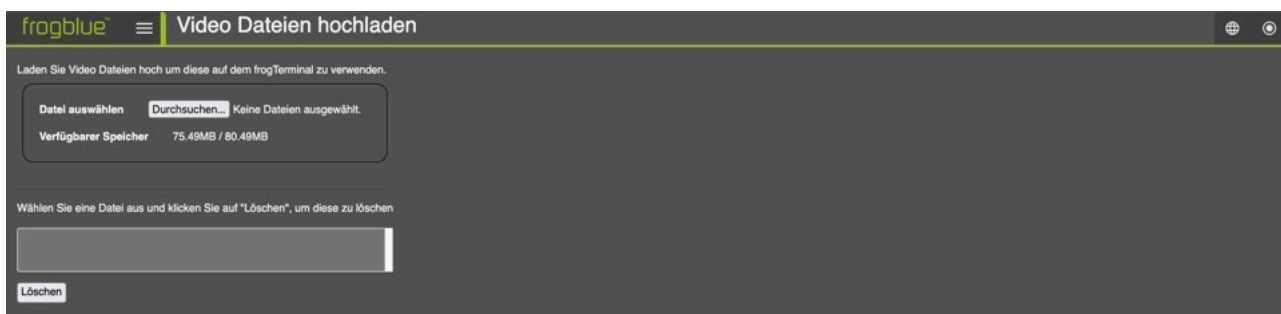
Ermöglicht die Verwaltung und das Hochladen benutzerdefinierter Bilddateien, die im frogTerminal verwendet werden können, z. B. für benutzerdefinierte Logos oder Benutzeroberflächen.



## 16.3. Video-Dateien

Über den Webbrowser im Menü: **Medien** → **Videos**

Ermöglicht die Verwaltung und das Hochladen benutzerdefinierter Videodateien, die im frogTerminal verwendet werden können, z. B. für Lieferhinweise oder automatisierte Standort-Einweisungen.

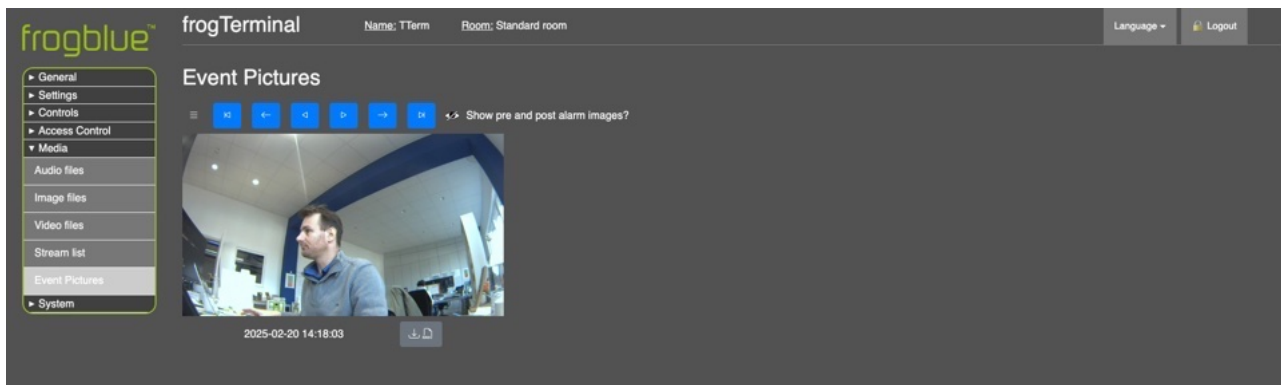



## 16.4. Streamliste

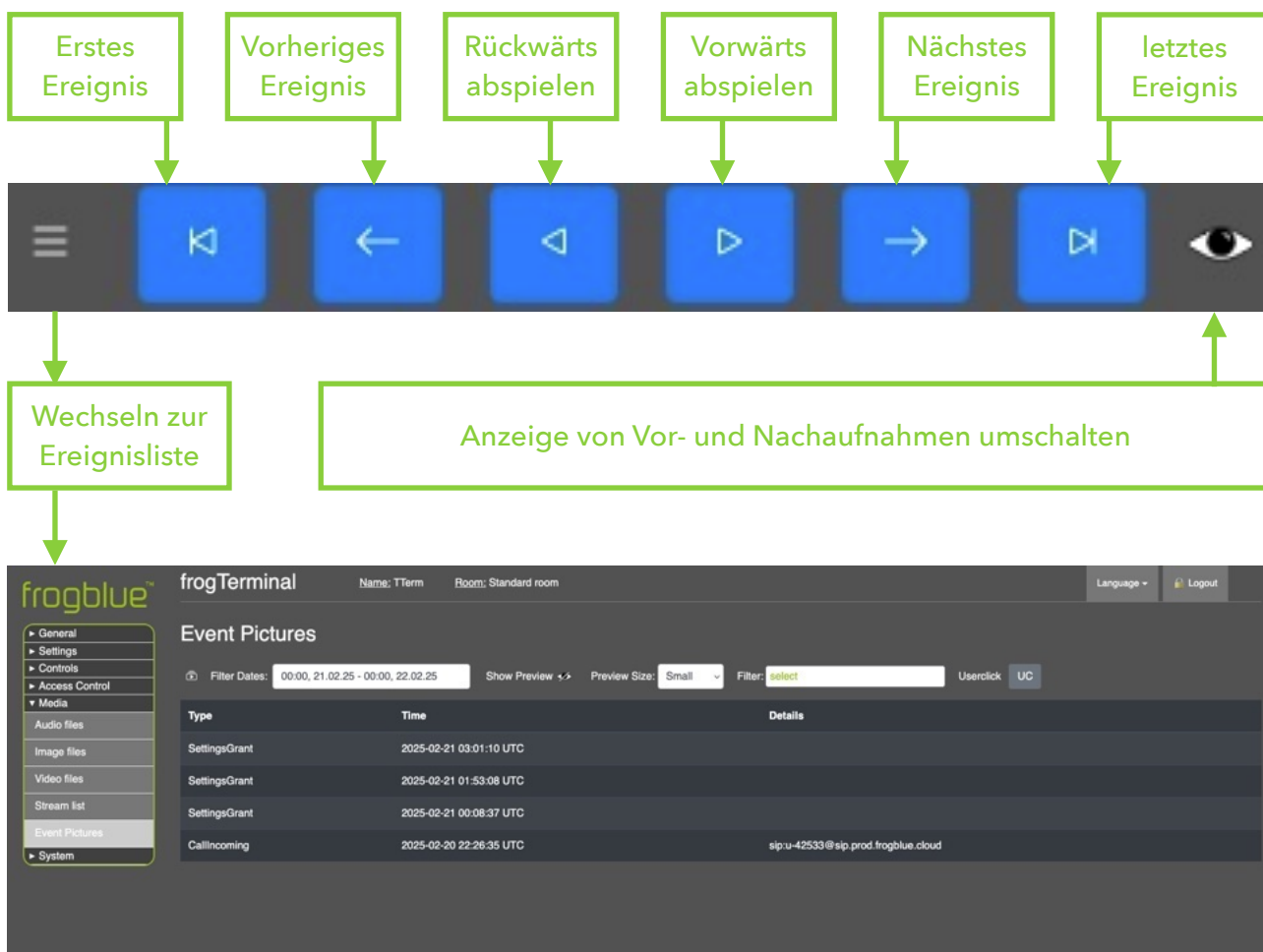
*Funktion noch nicht vollständig implementiert - Unterstützung für externe Streams folgt.*


## 16.5. Ereignisbilder

Ermöglicht das Suchen, Anzeigen und Herunterladen gespeicherter Ereignisbilder vom frogTerminal.



- Verwenden Sie die Wiedergabesteuerungen, um das gesuchte Ereignisbild zu finden.
- Verwenden Sie den Download-Button , um Bilder im hochwertigen RAW-Format auf Ihren Computer oder Ihr webbasiertes Gerät herunterzuladen.



- Verwenden Sie die Ereignisliste, um nach Ereignissen nach Zeit, Datum und Ereignistyp zu suchen und zu filtern.
-  Löst eine manuelle Aufnahme aus.

## 17. Konfiguration des frogTerminals für Automatisierung via frogCast/frogMesh

Die Bereitstellung des frogTerminals mit frogCast/frogMesh-Konfiguration ermöglicht eine nahtlose Integration in frogblues Smart-Automation-Mesh, wodurch die automatisierte Steuerung von Lichtern, Türen und Rollläden möglich wird.

Notieren Sie sich zunächst die **Bluetooth MAC-Adresse** Ihres frogTerminal aus dem **Webbrowser** unter **Allgemein** → **Übersicht**.

Öffnen Sie die **frogProject App** auf Ihrem iPad oder einem kompatiblen Gerät.

Erstellen Sie ein neues Projekt und legen Sie das Projektpasswort fest (für eine einfache Einrichtung können Sie dasselbe Passwort verwenden, das Sie im Schritt 4 des Installationsassistenten: frogblue Mesh Setup festgelegt haben, s. **Abschnitt 4.4**).

Wenn Sie die Benutzeroberfläche offen gelassen haben, fahren Sie fort. Falls Sie die Benutzeroberfläche gesperrt haben, siehe **Abschnitt 22 „Wartung und Fehlersuche“** zum Zurücksetzen Ihres frogTerminal.

Wählen Sie **+**, um ein Gerät zu frogProject hinzuzufügen, und suchen Sie Ihr frogTerminal über die Bluetooth MAC-Adresse.

Sobald das Gerät hinzugefügt wurde, wählen Sie Ihr Terminal aus der Geräteliste aus und tippen Sie auf das Konfigurationssymbol, um die Einstellungen zu speichern (wählen Sie keine Einstellungsteile aus, die ersetzt werden sollen - tippen Sie einfach auf **OK**).

Ihr frogTerminal ist provisioniert und bereit für die Automatisierung. Schritte, bei denen frogMessages verfügbar sind, z.B. in Funktions-PINs oder Anrufzielen, zeigen nun die verfügbaren frogMessages in ihren jeweiligen Dropdown-Menüs an.

## 18. Netzwerkkonfiguration

### 18.1. Ethernet- oder WLAN-Einrichtung

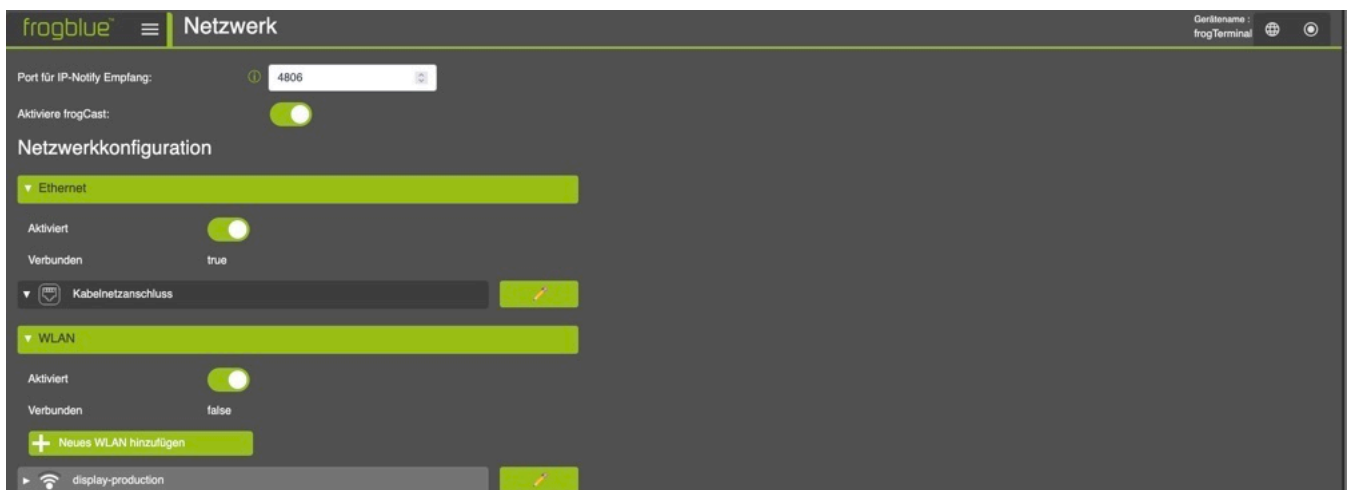
Konfigurieren Sie die Netzwerkeinstellungen, um das frogTerminal mit Ihrem lokalen Netzwerk zu verbinden.

#### Schrittübersicht:

- Verbindungstyp wählen (Ethernet oder WLAN).
- IP-Einstellungen konfigurieren (DHCP oder statisch).
- Netzwerkverbindung testen.

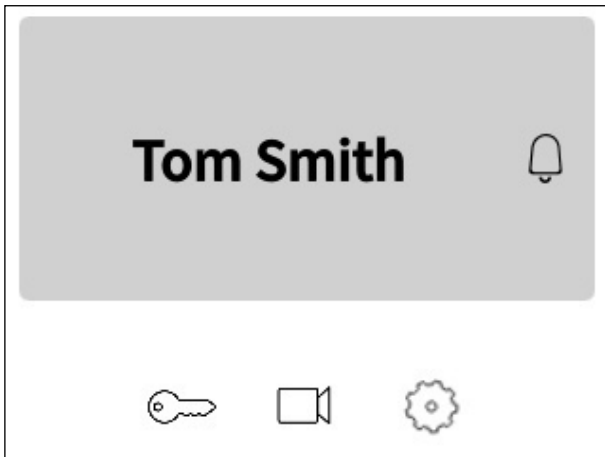
#### 18.1.1. Netzwerkkonfiguration über den Webbrowser


Über den Webbrowser im Menü: *System* → *Netzwerk*



- **Aktiviere frogCast:** Schalten Sie frogCast über das Kontrollkästchen ein, sodass Bluetooth-Nachrichten auch über eine Netzwerkverbindung weitergeleitet werden können.
- **Ethernet:** Aktivieren oder deaktivieren Sie Ihr Ethernet. Der Verbindungsstatus wird mit *true/false* angezeigt. Um sich mit dem Netzwerk zu verbinden oder die Verbindung zu trennen, nutzen Sie den On-Device-Touchscreen wie im nächsten Abschnitt beschrieben. Klicken Sie auf das Stift-Symbol, um Ihren Kabelanschluss zu bearbeiten.
- **WLAN:** Aktivieren oder deaktivieren Sie Ihr WLAN. Der Verbindungsstatus wird mit *true/false* angezeigt. Um sich mit dem Netzwerk zu verbinden oder die Verbindung zu trennen, nutzen Sie den On-Device-Touchscreen wie im nächsten Abschnitt beschrieben.

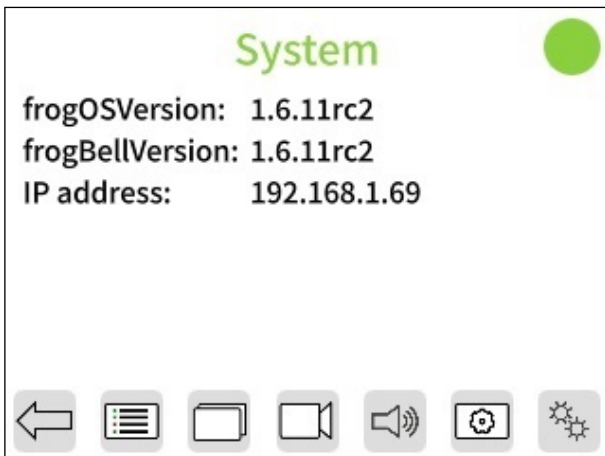
### 18.1.2. Netzwerkkonfiguration über den On-Device-Touchscreen.




- Tippen Sie , um in den Konfigurationsmodus zu gelangen.





- Geben Sie Ihre sechsstellige Admin-PIN ein und tippen Sie auf **OK**.

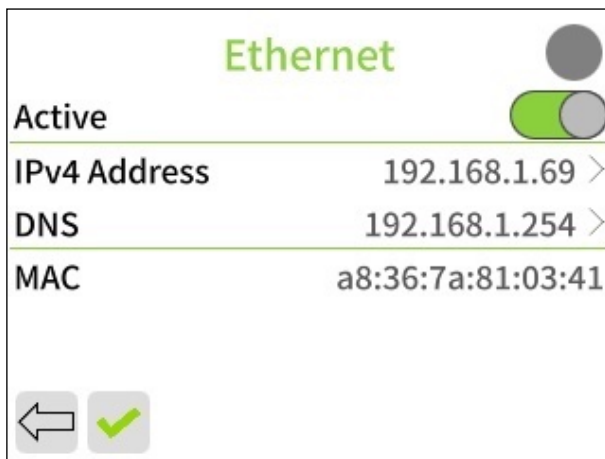




- Tippen Sie , um auf die zusätzlichen Einstellungsseiten zuzugreifen.



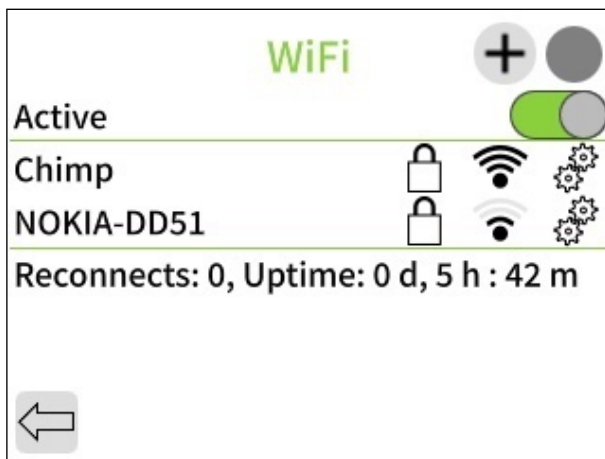
- Tippen Sie , um die Ethernet-Einstellungen zu konfigurieren.  
→ Springen Sie zu **Abschnitt 18.1.3**.
- Tippen Sie , um die WLAN-Einstellungen zu konfigurieren.  
→ Springen Sie zu **Abschnitt 18.1.4**.


### 18.1.3. Ethernet-Konfiguration über den On-Device-Touchscreen.



- Lassen Sie Ethernet aktiviert oder deaktivieren Sie es über den Kippschalter, falls WLAN verwendet wird.
- Tippen Sie auf **IPv4-Adresse** oder **DNS**, um deren Einstellungen zu ändern.
- Tippen Sie , um zurückzukehren, oder , um die Änderungen zu speichern und zur Netzwerkeinrichtungsseite zurückzukehren.

### 18.1.4. WLAN-Konfiguration über den On-Device-Touchscreen.



- Aktivieren Sie den Kippschalter, wenn WLAN verwendet wird.
- Warten Sie, bis die Netzwerk-Liste erscheint - dies kann in komplexen Setups einige Minuten dauern.
- Tippen Sie auf Ihr bevorzugtes WLAN-Netzwerk oder tippen Sie , um WLAN-Details manuell einzugeben.



- Für die manuelle Einrichtung tippen Sie und geben Sie den Netzwerknamen, das Passwort und den Sicherheitsmodus ein.
- Für ein aus der Liste ausgewähltes Netzwerk geben Sie das Passwort und den Sicherheitsmodus ein.
- Verwenden Sie die Bildschirmtastatur, um die Details einzugeben, und tippen Sie auf **Ok**.
- Schließlich tippen Sie auf **Connect**. Falls der erste Versuch fehlschlägt, warten Sie kurz und tippen Sie erneut auf **Connect**.

### 18.1.5. Fehlersuche bei Netzwerkverbindungsproblemen

#### Ethernet-Verbindungen:

- Stellen Sie sicher, dass alle Kabel fest angeschlossen und unbeschädigt sind.
- Testen Sie das Ethernet-Kabel mit einem anderen Gerät, um Kabelprobleme auszuschließen.
- Überprüfen Sie, ob der Netzwerkanschluss aktiv und korrekt konfiguriert ist.

## WLAN-Verbindungen:

- Bringen Sie das Gerät näher an den WLAN-Router, um die Signalstärke zu verbessern.
- Prüfen Sie auf Hindernisse oder Störungen, wie Wände oder andere elektronische Geräte.
- Stellen Sie sicher, dass die WLAN-Zutrittsdaten korrekt eingegeben wurden.

## Allgemeine Netzwerkprüfungen:

- Starten Sie Ihren Router oder Access Point neu.
- Vergewissern Sie sich, dass das Gerät im Netzwerk zugelassen ist (z. B. dass MAC-Adressfilterung deaktiviert ist).
- Setzen Sie sich mit Ihrem Administrator in Verbindung, um sicherzustellen, dass die Einstellungen korrekt sind und keine Einschränkungen vorliegen.

## 18.2. SIP-Server-Registrierung

Dieser Abschnitt erklärt, wie das Terminal bei einem Session Initiation Protocol (SIP)-Server für Telefonie- und Gegensprechanlagen-Funktionalität registriert wird. Dadurch kann das Terminal, Anrufe tätigen und empfangen, sich in VoIP-Systeme integrieren und Videoanrufe unterstützen.

### Schrittübersicht:

- Einzelne SIP-Server-Registrierung.
- Mehrere SIP-Server-Registrierungen (Mehrparteien-Szenarien).
- Testen der SIP-Konnektivität.

### 18.2.1. SIP-Grundlagen

Bevor Sie mit der Konfiguration fortfahren, ist es hilfreich, einige wichtige SIP-Konzepte zu verstehen:

- **„SIP-Server (Registrar-Server)“**: Der Hauptserver, der SIP-Registrierungen verarbeitet und Geräte authentifiziert. Dies ist die primäre Serveradresse für die Registrierung des Terminals.
- **„Outbound SIP-Server (Proxy-Server)“**: Ein sekundärer Server, der für die Weiterleitung ausgehender Anrufe verwendet wird, oft abweichend vom Registrar-Server. Einige Anbieter erfordern einen separaten Outbound-Server für die Anrufabwicklung.
- SIP-Konto (Benutzername & Autorisierungsbenutzername):
  - **„Username (SIP Extension)“**: Der eindeutige Identifikator, der dem Terminal zugewiesen wird (z. B. 1001 oder door@mybuilding.com).
  - **„Authorisation Username“**: Einige SIP-Anbieter verlangen einen von der SIP-Erweiterung abweichenden Autorisierungsbenutzernamen für die Anmeldung.
- **„SIP-URI (Uniform Resource Identifier)“**: Die SIP-Adresse des Terminals, formatiert wie eine E-Mail (z. B. sip:door@mybuilding.com).
- **„SIP Transport Protocols“**: Das Verfahren, mit dem SIP-Nachrichten gesendet werden:
  - **UDP** (am schnellsten, aber weniger zuverlässig)
  - **TCP** (zuverlässiger, besser für NAT-Durchquerung)
  - **TLS** (verschlüsselt und sicher, empfohlen für VoIP-Sicherheit)
- **„SIP Video Support“**: Falls aktiviert, kann das Terminal in Echtzeit Video zusammen mit Audioanrufen mittels kompatibler Codecs (z. B. H.264) übertragen.

## 18.2.2. SIP-Einrichtung über den Webbrowser

Über den Webbrowser im Menü: *Einstellungen* → *SIP-Server*

The screenshot shows the 'SIP-Server' configuration page in the frogTerminal web interface. The page is titled 'SIP-Server:' and has a sidebar menu on the left with options like General, Settings, SIP Server, Call destinations, PINs, Hardware, Recording, RTSP, RFID, Media, and System. The 'SIP Server' option is selected. The main content area is divided into 'General settings' and 'Primary server'.

**General settings:**

- Allow direct call:

**Primary server:**

- Server: sip.prod.frogblue.cloud
- Outbound server: [empty]
- Username: p-42618-43086
- Authorization user name: [empty]
- Password: [masked]
- Transport protocol: tls

**Additional servers:**

Name	Username:	Server	Outbound server	Authorization user name:	Password:	Transport protocol
frogTerminal1	frogterminal	sip.mysipserver.net	sip.mysipserver.net	frogterminal	[masked]	tls
frogTerminal1	u-92765	sip.companyb.net	sip.mysipserver.net	u-92765	[masked]	tcp
frogTerminal1	doorterminal	192.168.1.200	192.168.1.200	doorterminal	[masked]	udp

### Allgemeine Einstellungen:

- **Allow direct call:** Aktivieren/Deaktivieren, um direkte IP-Anrufe an diesem Terminal ohne Authentifizierung über einen SIP-Server zu erlauben bzw. zu verbieten.  
**Warnung! UNSICHER:** Nur für Tests oder lokale (fortgeschrittene) Nutzung. Mit Vorsicht verwenden, da dies zu böswilligen Anrufen oder Anrufübernahmen führen kann.

### Primärer Server:

- **Primary Server:** Bestimmt die Quelle der gespeicherten PIN-Codes für die Zwei-Faktor-Authentifizierung, mit drei Optionen:
  - **None:** Deaktiviert die PIN-Eingabe an diesem Terminal.
  - **Card:** Die gängigste Einstellung, die die Zwei-Faktor-Authentifizierung mit spezifischen PIN-Codes ermöglicht, die einzelnen Benutzern zugeordnet und auf der Zutrittskarte gespeichert werden.
  - **Terminal:** Sichert die Tür oder den Zutrittspunkt mit einem terminal-spezifischen PIN-Code. Diese PIN gilt für alle Benutzer an diesem Standort und überschreibt persönliche PINs.

Beim Auswählen von **Terminal** erscheint ein zusätzliches Eingabefeld, in dem Sie eine sechstellige PIN für den Zutritt an diesem Terminal festlegen können.

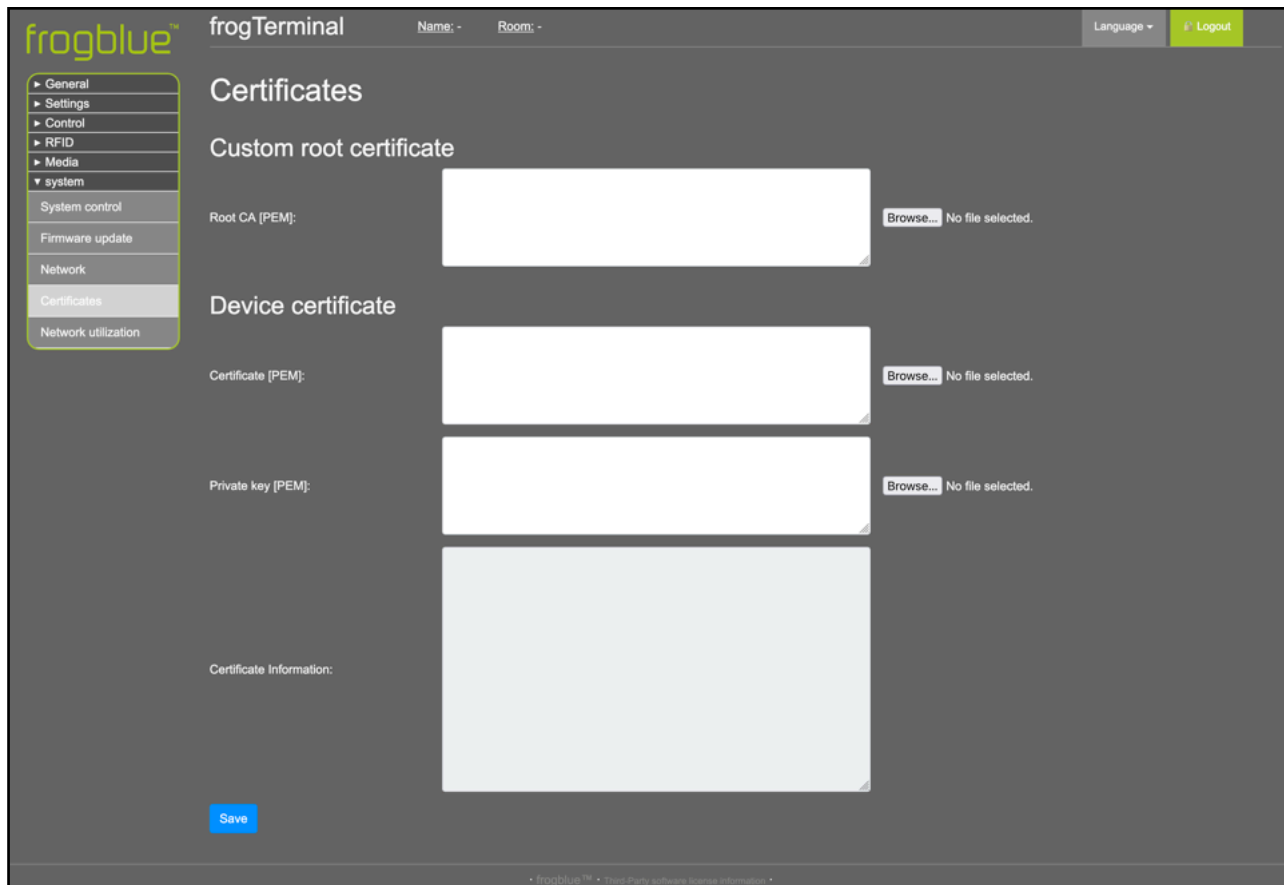
- **Time Table Source:** Gibt an, aus welcher Quelle zeitbasierte Zutrittsregeln stammen, mit drei Optionen:
  - **None:** Deaktiviert zeitbasierte Zutrittsregeln an diesem Terminal.
  - **Card:** Zeitregeln werden auf der Zutrittskarte gespeichert, wodurch individuelle Zeitpläne möglich sind (z. B. Allgemeines Personal: 9-17 Uhr, Reinigungskräfte: Fr-Sa 15-19 Uhr, Security: 24h).
  - **Terminal:** Die Zeitregeln werden lokal auf dem Terminal gespeichert. So kann jedes Terminal einen individuellen Zeitplan als Quelle für Zeitregeln haben. Vorhandene Zeitpläne auf einer Zutrittskarte werden auf diesem Terminal ignoriert.

### 18.3. Benutzerdefinierte Root-Zertifikate

Dieser Abschnitt erklärt, wie benutzerdefinierte Zertifikate auf dem frogTerminal für eine sichere Kommunikation konfiguriert werden. Das Terminal ermöglicht das Hochladen eines benutzerdefinierten Root-CA-Zertifikats sowie eines Gerätezertifikats und eines privaten Schlüssels im PEM-Format. Diese Funktionalität ist nützlich für Umgebungen, die sichere und private Verbindungen erfordern, insbesondere in internen Netzwerken oder bei der Aktivierung sicherer **API-Aufrufe** oder verschlüsselter Kommunikation.

#### Schrittübersicht:

- Hochladen eines benutzerdefinierten Root-CA-Zertifikats.
- Hochladen eines Gerätezertifikats und des entsprechenden privaten Schlüssels.
- Überprüfen der Zertifikatsinformationen.



### **Custom root certificate:**

Das Feld **Root CA (PEM)** ermöglicht das Hochladen eines benutzerdefinierten Root-Zertifikats im PEM-Format. Dieses wird verwendet, um Server- oder Peer-Zertifikate für eine sichere Kommunikation zu authentifizieren.

### **Anwendungsfälle:**

- Integration mit privaten oder internen CAs.
- Aktivierung sicherer API-Aufrufe oder verschlüsselter Kommunikation in privaten Netzwerken.

### **So laden Sie ein Root-Zertifikat hoch:**

- Klicken Sie auf **Browse** neben dem Feld **Root CA (PEM)**.
- Wählen Sie die entsprechende PEM-Datei aus, die Ihr Root CA-Zertifikat enthält, und klicken Sie auf **Open**.
- Klicken Sie auf **Save**, um Ihr benutzerdefiniertes Root-Zertifikat anzuwenden.

### **Device certificate:**

- Das Feld **Certificate (PEM)** ermöglicht das Hochladen des einzigartigen Zertifikats des Geräts zur Identifikation und Authentifizierung.
- Das Feld **Private Key (PEM)** ermöglicht das Hochladen des privaten Schlüssels, der mit dem Gerätezertifikat verknüpft ist.

### **Anwendungsfälle:**

- Sichere gegenseitige Authentifizierung mit Servern (z. B. in TLS-Handshake-Prozessen).
- Aktivierung verschlüsselter Kommunikation zwischen Geräten und Servern.

### **So laden Sie ein Gerätezertifikat hoch:**

- Klicken Sie auf **Browse** neben dem Feld **Certificate (PEM)**, wählen Sie die Zertifikatsdatei des Geräts aus und klicken Sie auf **Open**.
- Klicken Sie auf **Browse** neben dem Feld **Private Key (PEM)**, wählen Sie die Datei des privaten Schlüssels aus und klicken Sie auf **Open**.
- Stellen Sie sicher, dass beide Dateien korrekt gepaart und gültig sind.

### **Zertifikatsinformationen:**

- Das Feld **Certificate Information** bietet eine Zusammenfassung des hochgeladenen Gerätezertifikats, einschließlich Details wie dem Aussteller, dem Gültigkeitszeitraum und dem Betreff.
- Überprüfen Sie diese Informationen, um sicherzustellen, dass das Zertifikat korrekt hochgeladen und erkannt wurde.

### **Wichtige Hinweise**

- Stellen Sie sicher, dass alle Dateien im **PEM-Format** vorliegen, bevor Sie sie hochladen. Nicht unterstützte Dateiformate führen zu Fehlern.

- Das Hochladen falscher oder ungültiger Zertifikate kann zu Verbindungsproblemen oder Unterbrechungen der Kommunikation führen.
- Für private Netzwerke oder benutzerdefinierte Anwendungen konsultieren Sie Ihren Systemadministrator, um die korrekten Zertifikate zu erhalten.
- Zertifikate und private Schlüssel müssen sicher gespeichert und gehandhabt werden, um unbefugten Zugriff zu verhindern.

## 19. Sicherheit

Über den Webbrowser im Menü: **System** → **Sicherheit**

### 19.1. Admin PIN

**PIN für die Einstellungen des SIP-Terminals:** Legen Sie eine exakt sechsstellige PIN fest, welche zur Verwaltung des frogTerminals über den On-Device-Touchscreen verwendet wird, um Zugriff auf die lokale Systemsteuerung zu erhalten.

### 19.2. Admin Passwort

**Änderung des Admin-Passwortes:** Hier können Sie das Web-Administrator-Passwort ändern. Beachten Sie, dass Sie das alte Passwort eingeben und dann Ihr gewünschtes neues Passwort zweimal wiederholen müssen, bevor Sie auf **Passwort Ändern** klicken.

## 20. Integration mit Drittanbieter-Videosystemen

Integrieren Sie das Terminal in externe Video-Streaming- oder Management-Systeme.

### 20.1. HTTPS- oder Web-Integration - Unverschlüsselter MJPEG-Stream

Das **frogTerminal** unterstützt einen **MJPEG-Stream** oder **Fast-Stream** über **HTTPS** zur Kompatibilität mit Altsystemen oder für einfache Integrationen in Webseiten. Eine **HTTPS-Authentifizierung** ist erforderlich und kann im Standard-HTTP-Format übermittelt werden, zum Beispiel:

- **Standard-URL:** `https://<IP-Adresse>/cgi-bin/cam.cgi`
- **Mit Authentifizierung:** `https://<Benutzername>:<Passwort>@<IP-Adresse>/cgi-bin/cam.cgi`

### 20.2. RTSP-Einstellungen

Menü: **System** → **RTSP-Einstellungen**

Das **frogTerminal** unterstützt das **Real-Time Streaming Protocol (RTSP)** für die Integration seines Kamera-Video-Streams in **Drittanbieter-Videosysteme**. Audio-Unterstützung befindet sich derzeit in der Entwicklung.

RTSP ist ein weit verbreitetes Streaming-Protokoll, das es Clients ermöglicht, Echtzeit-Video-Feeds von IP-Kameras und Mediaservern anzufordern, zu steuern und zu empfangen. Es bildet die Grundlage für **ONVIF** (Open Network Video Interface Forum), den Industriestandard für die Interoperabilität zwischen IP-basierten Sicherheitsgeräten. Die **ONVIF**-Unterstützung für das **frogTerminal** befindet sich derzeit in der Entwicklung.

Viele beliebte Video-Management-Systeme (VMS), wie **Milestone XProtect** und **Genetec Security Center**, unterstützen die direkte Integration von **RTSP-Streams**, sodass das **frogTerminal** als Videoquelle hinzugefügt werden kann, ohne dass zusätzliche Treiber oder Plugins erforderlich sind.

#### RTSP-Stream URL-Format

Um auf den RTSP-Stream des **frogTerminals** zuzugreifen, verwenden Sie das folgende URL-Format:

`rtsp://<Benutzername>:<Passwort>@<IP-Adresse>:<Port>/cam`

- **<Benutzername>:** Der festgelegte RTSP-Benutzer (rtsp) oder ein Admin-Benutzer.
- **<Passwort>:** Das Passwort für den RTSP-Benutzer oder ein Admin-Konto.
- **<IP-Adresse>:** Die lokale oder externe IP des **frogTerminals**.
- **<Port>:** Der RTSP-Dienstport (Standard: 554, sofern in der Konfiguration nicht geändert).
- **/cam:** Der RTSP-Stream-Pfad.

#### Optimale Einstellungen für niedrige Latenz und hohe Bildrate

Um die beste Leistung bei niedriger Latenz und hoher Bildrate zu erzielen, stellen Sie sicher, dass:

- **Kein browserbasierter HTTPS- oder Web-Stream** aktiv ist (z. B. Live-Kamera-Stream in einem Browser).
- Die folgenden **Bildeinstellungen** angewendet werden:
  - **Image Enhancement:** Auf **Aus** stellen.
  - **Image Resolution:** Auf maximales **HD** einstellen.

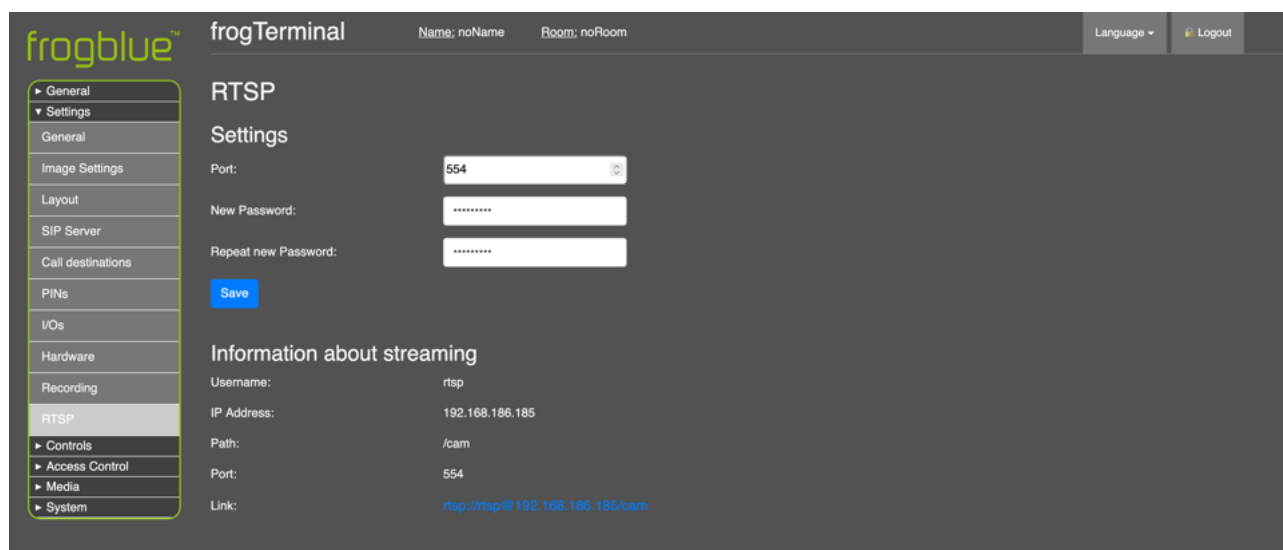
- **JPEG Compression Quality:** Auf **60%** einstellen.
- Die **On-board-Aufnahme** für optimale Leistung **deaktiviert** ist. Stattdessen verwenden Sie ein **VMS-System** zur Videoaufzeichnung.

### Benutzerzugriff:

- Der dedizierte RTSP-Benutzer (rtsp) kann ausschließlich für das RTSP-Streaming verwendet werden.
- Admin-Benutzer können auch mit ihren Zutrittsdaten auf den RTSP-Stream zugreifen.

### Weitere Hinweise:

- Stellen Sie sicher, dass **RTSP** am frogTerminal **aktiviert** ist und dass Firewall-Regeln den Datenverkehr über den angegebenen RTSP-Port zulassen.
- Für den **Fernzugriff** sind ggf. Portweiterleitung oder eine **VPN-Verbindung** erforderlich, abhängig von der Netzwerkkonfiguration.
- Die **ONVIF-Unterstützung ist geplant**, was eine weitere Integration mit automatischer VMS-Erkennung und zusätzlichen Videosicherheitsplattformen ermöglichen wird.
- **Latenz und Stream-Stabilität** hängen von den Netzwerkbedingungen und den Encoding-Einstellungen ab.



### Port

- Definiert den Port, der für den RTSP-Streaming-Dienst verwendet wird.
- Standard: „554“ (Standard-RTSP-Port).
- Wenn Ihr Netzwerk einen anderen Port erfordert, geben Sie die gewünschte benutzerdefinierte Portnummer ein.
- Stellen Sie sicher, dass der ausgewählte Port in Ihrer Firewall/Ihrem Router geöffnet ist, falls Sie remote auf den Stream zugreifen.

### Neues Passwort

- Legen Sie ein neues Passwort für den RTSP-Benutzer (rtsp) fest.
- Dies ist ein dediziertes Passwort für die Verbindung zum Stream über die RTSP-URL.

- **Mindestanforderungen:** Mindestens acht Zeichen, einschließlich einer Mischung aus Großbuchstaben, Kleinbuchstaben und Zahlen zur Sicherheit.

### Neues Passwort wiederholen

- Geben Sie das neue Passwort erneut ein, um es zu bestätigen.

### Speichern

- Speichert die aktualisierten Port- und Passworteinstellungen.
- Änderungen treten sofort nach dem Speichern in Kraft.
- Aktualisieren Sie Ihre RTSP-Einstellungen nach dem Speichern in externen Anwendungen, falls Sie das Passwort oder den Port geändert haben.

## 20.3. RTSP-Stream-Integration

Dieser Abschnitt bietet eine schrittweise Anleitung, wie Sie den RTSP-Stream des frogTerminals mit OBS Studio und VLC Media Player integrieren.

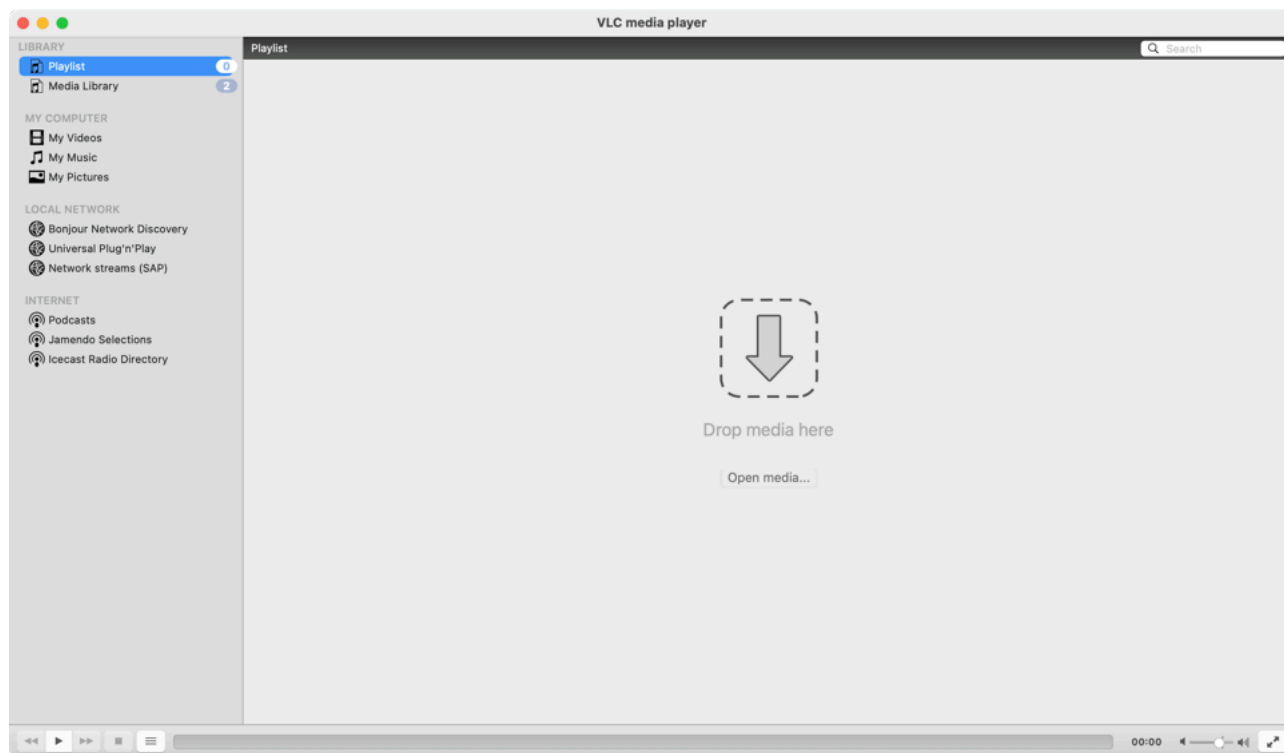
Stellen Sie sicher, dass:

- **RTSP** auf dem frogTerminal aktiviert ist.
- Die korrekte RTSP-URL verwendet wird.

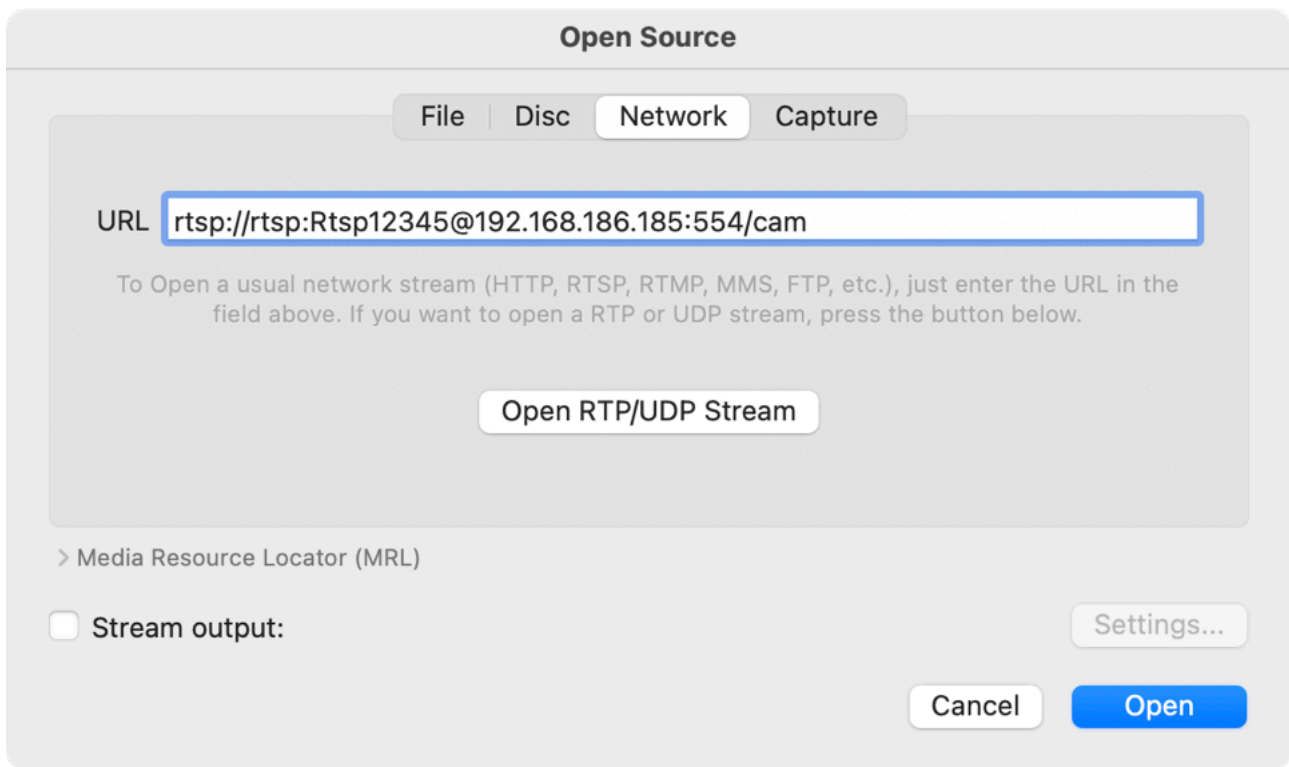
### RTSP-Integration mit VLC Media Player

VLC Media Player ist ein Open-Source-Videooplayer, der **RTSP-Streaming** unterstützt. Um den **RTSP-Stream des frogTerminals** in VLC zu integrieren:

- Öffnen Sie VLC Media Player.



- Klicken Sie auf **Open media**.



- Wechseln Sie zum Reiter **Network**.
- Geben Sie die **RTSP-URL** ein. Der Benutzername und das Passwort können im HTTP-Format übermittelt oder im nächsten Schritt eingegeben werden.



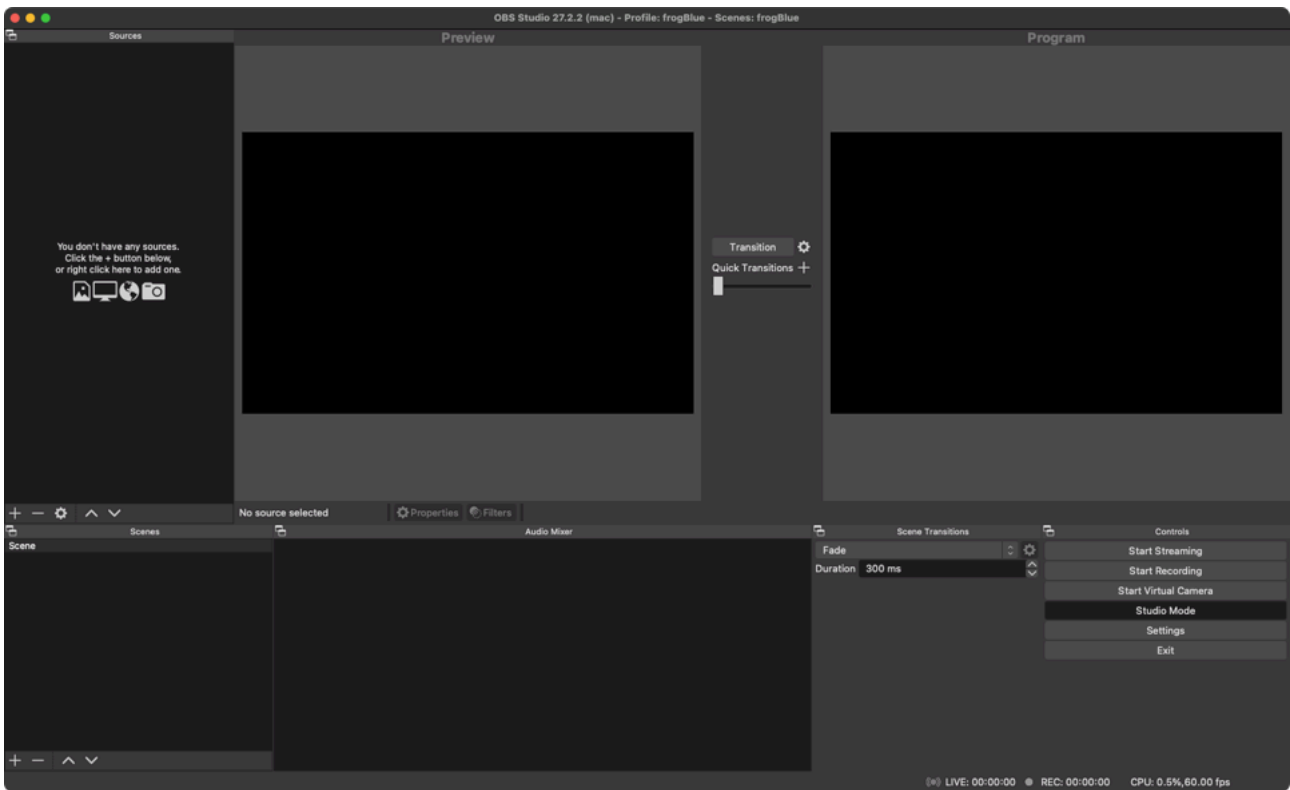
Der Kamerastream sollte nun im VLC-Hauptfenster erscheinen. Standardmäßig puffert VLC den Stream, was zu einer Verzögerung von mehreren Sekunden führen kann.

**Hinweis:** VLC ist primär für das **Streaming über das Internet** konzipiert und enthält integrierte Pufferungsmechanismen, die die **Latenz erhöhen** können, was die Echtzeitleistung beeinträchtigen kann. Um VLC für Streaming mit **niedriger Latenz** zu optimieren, können Anpassungen an den Pufferungseinstellungen erforderlich sein.

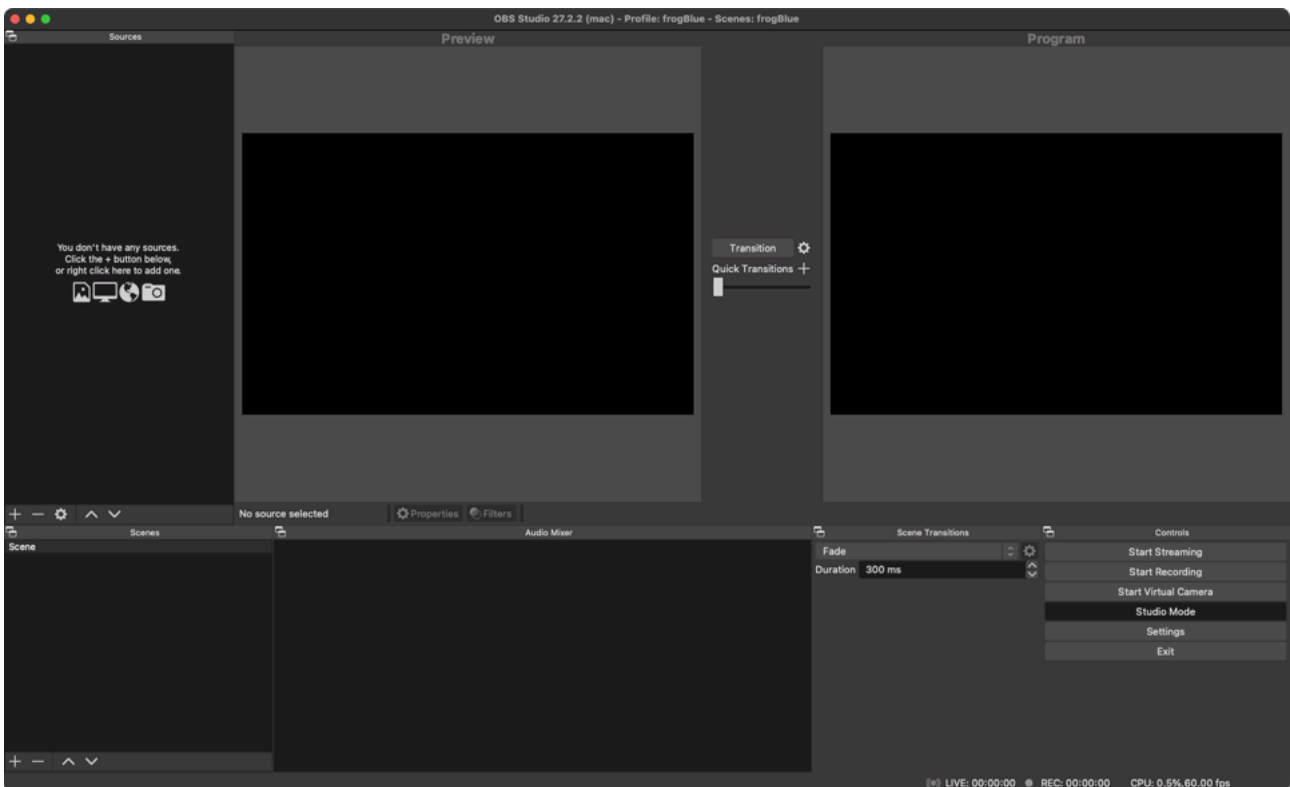
## RTSP-Integration mit OBS Studio

**OBS Studio** ist ein weit verbreitetes Open-Source-Streaming- und Aufzeichnungstool. Folgen Sie diesen Schritten, um den **RTSP-Stream des frogTerminals** in OBS zu integrieren:

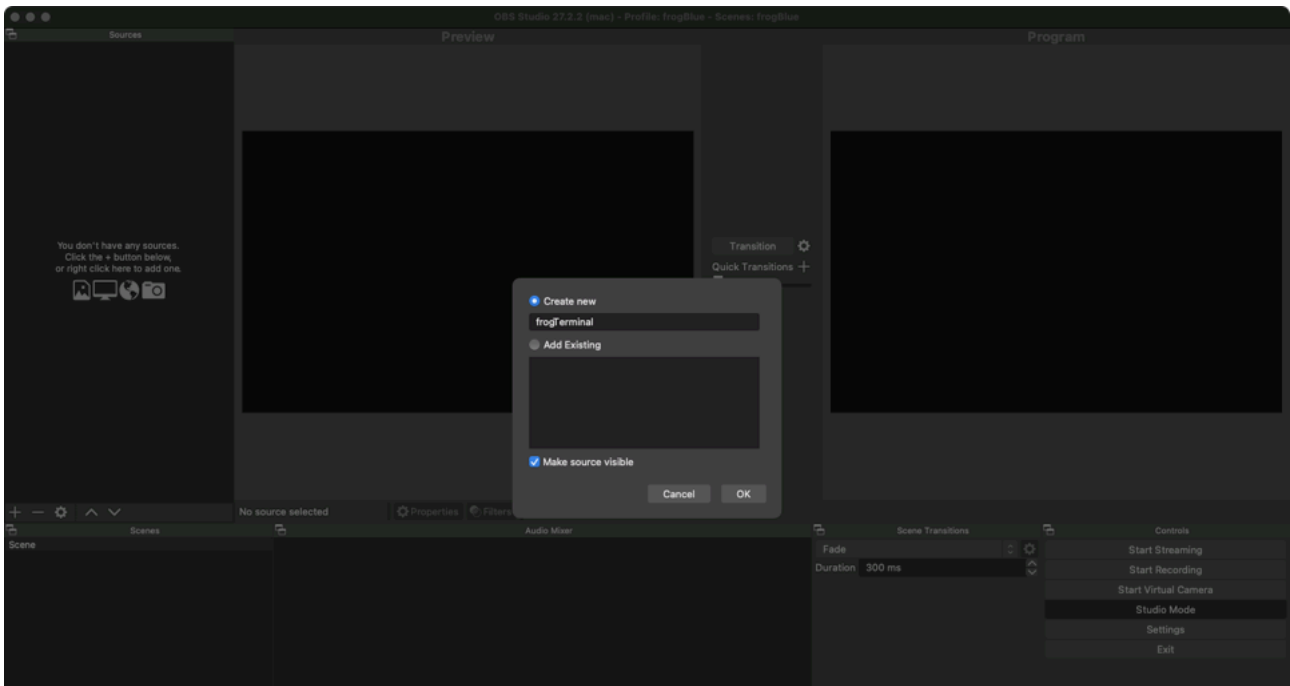
- Öffnen Sie **OBS Studio**.



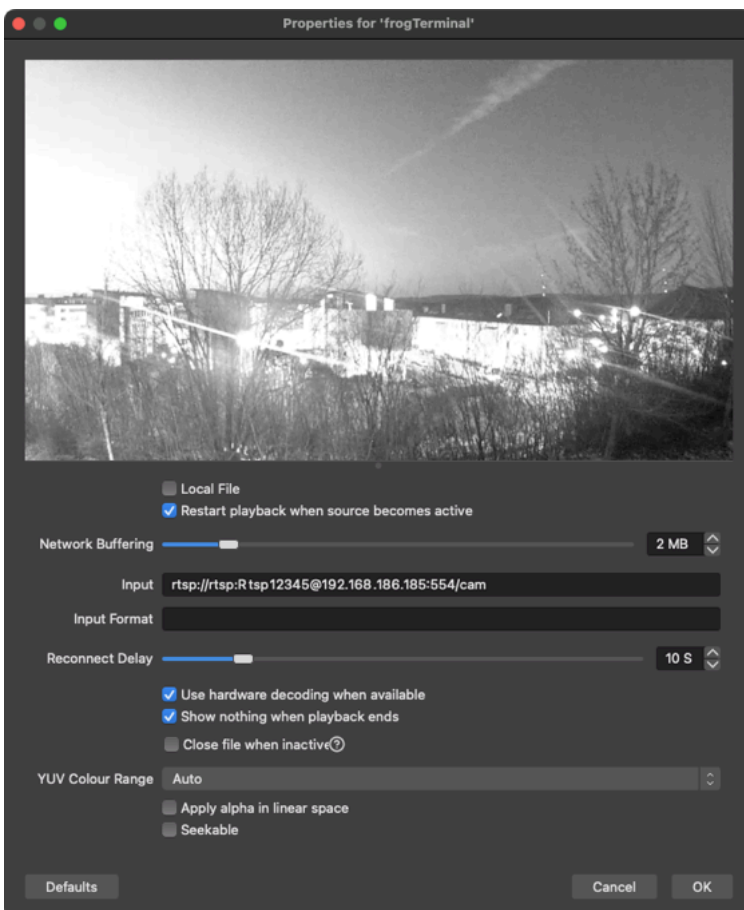
- Klicken Sie unter **Sources** auf **+**, um eine neue Videoquelle hinzuzufügen.



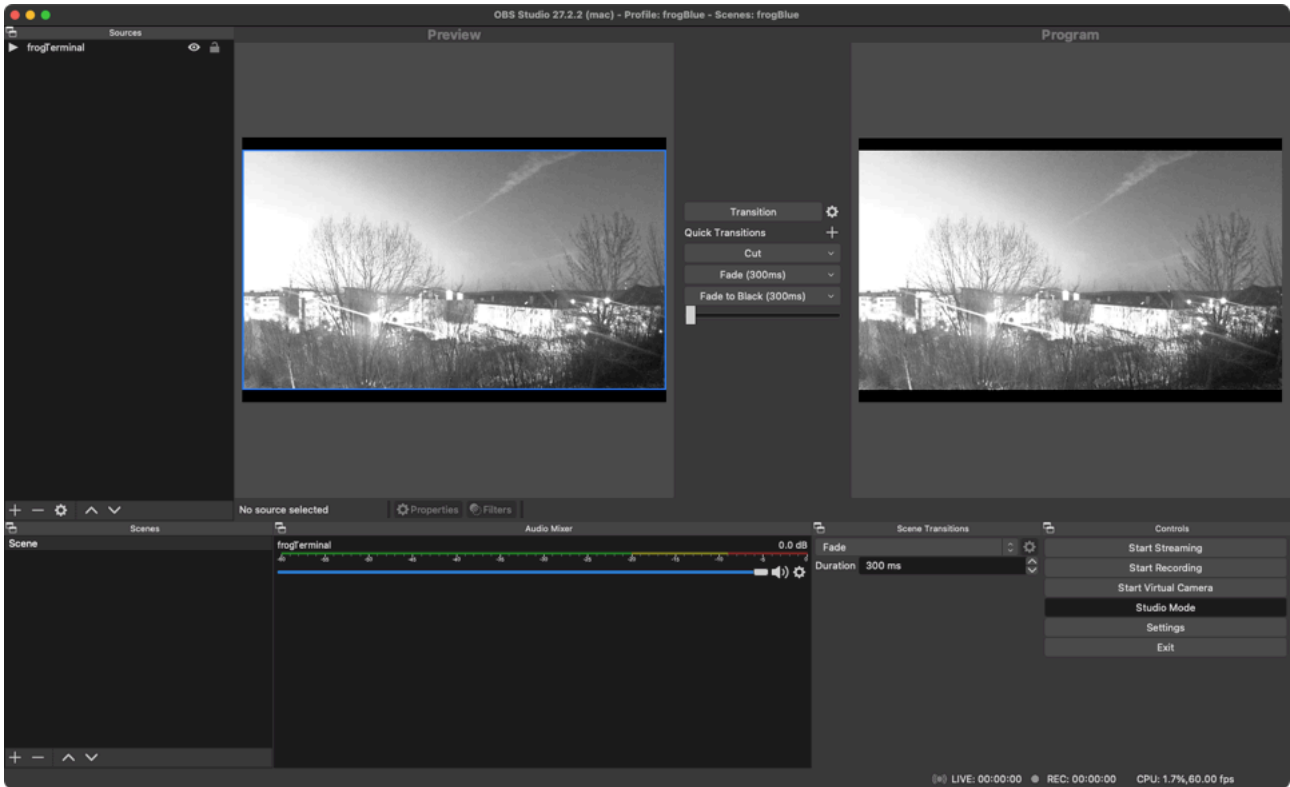
- Wählen Sie **Media Source**.



- Geben Sie Ihrer Quelle einen Namen, z. B. „frogTerminal“.
- Klicken Sie auf **OK**.



- Entfernen Sie das Häkchen bei **Local File**.
- Geben Sie die **RTSP-URL** ein. Der Benutzername und das Passwort können im HTTP-Format übermittelt oder im nächsten Schritt eingegeben werden.
- Setzen Sie ein Häkchen bei **Use hardware decoding when available**.
- Klicken Sie auf **OK**.



Der Livestream der frogTerminal-Kamera sollte nun in OBS Studio sichtbar sein.

**Hinweis:** Auf einigen **Betriebssystemen** oder **OBS-Versionen** kann ein **Popup-Fenster** erscheinen, das um Erlaubnis bittet, **OBS Studio** den Zugriff auf Ihr **Netzwerk** oder durch Ihre **Firewall** zu gestatten. Stellen Sie sicher, dass Sie diese **Erlaubnis bestätigen**, um den Stream zu aktivieren.  
Zusätzlich kann es auf bestimmten Systemen erforderlich sein, **OBS Studio** nach Abschluss der Einrichtung und Bestätigung etwaiger Popups **neu zu starten**. Sollte der Stream nicht sofort erscheinen, versuchen Sie, **OBS Studio zu schließen und erneut zu öffnen**.

## 20.4. Integration mit MOBOTIX MxManagementCenter

### 20.4.1. Übersicht

#### **frogTerminal - MxManagementCenter**

Das **frogTerminal** bietet Funktionen zur Integration mit der MOBOTIX MxManagementCenter-Software.

**Unterstützte Version:** MxManagementCenter 2.9.2

**Protokoll:** MxEventStream über Port 8035

Vom **frogTerminal** unterstützte Funktionen:

- Video- & Audiostream (MJPEG)
- Anrufe vom **frogTerminal** an MxMC (MxMC-Hintergrundalarne)
  - Live-Video-Popup bei Anruf
  - Gegensprechen (Push-to-Talk)
  - Tür öffnen
- Licht einschalten (Funktion in Vorbereitung)
- Ereignisbildeanzeige aus dem MxMC-Ereignisstreifen (rechte Seitenleiste)
- Erweiterte MxMC-Button-Integration über API (IP-Messages / WebHooks)

Unterstützte Anwendungen umfassen Türterminals, Rufstationen, Hilfs- oder Informationspunkte mit integriertem Touchdisplay und API-Unterstützung, wodurch fortgeschrittene Benutzer die Anwendungen noch weiter anpassen können.

#### **frogTerminal - als IP-Gateway zum frogblue-Automationssystem**

Das **frogTerminal** bietet Funktionen zur Integration mit IP-basierten Systemen.

#### **frogDisplay - als IP-Rufstation für das MOBOTIX-Türstationssystem**

Das **frogDisplay** unterstützt die Integration mit MOBOTIX-Türstationen (T24, T25, T26) und kann als Endpunkt für Türklingel-Ereignisse genutzt werden, die über das MOBOTIX-„Concierge“-System ausgelöst werden.

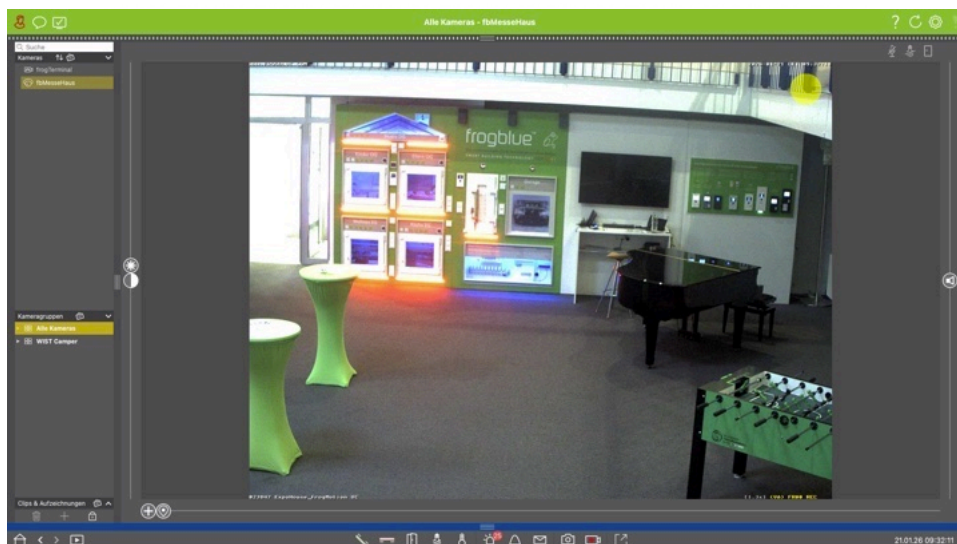
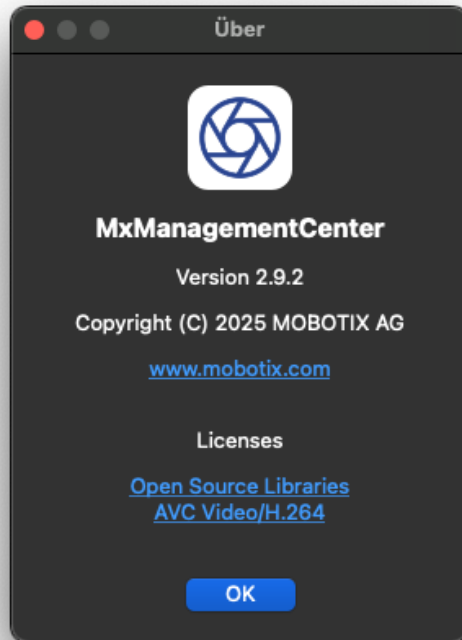
#### **MOBOTIX-Kameragerät mit frogLink als Gateway zum frogblue-Automationssystem**

Das **frogLink** bietet Funktionen zur Integration von frogblue-Automationssystemen mit USB-FTDI-kompatiblen Systemen.

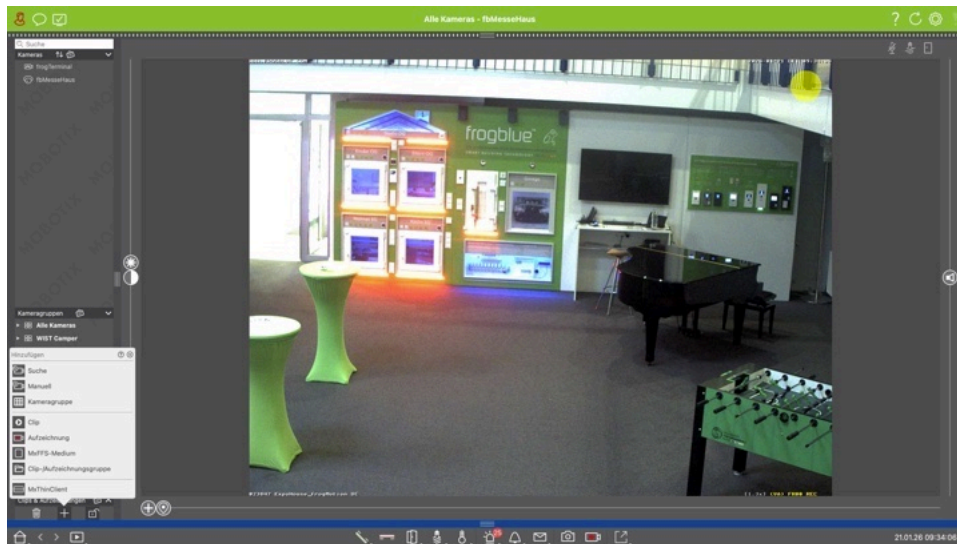
## 20.4.2. Integration Schritt für Schritt

### Hinzufügen des frogTerminal zu MxManagementCenter

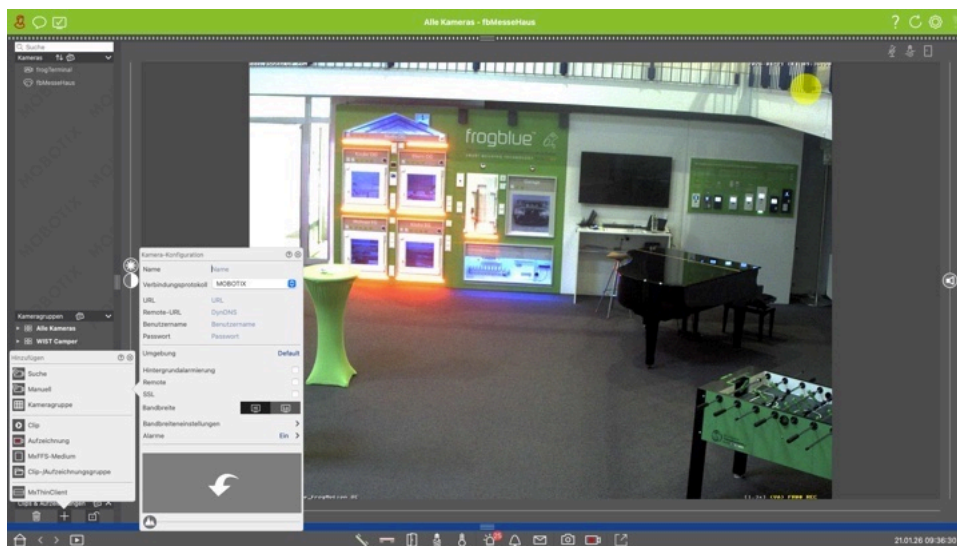
Um das frogTerminal als Gerät zur MOBOTIX MxManagementCenter-Software hinzuzufügen, öffnen Sie Ihre MxMC-Version 2.9.2.



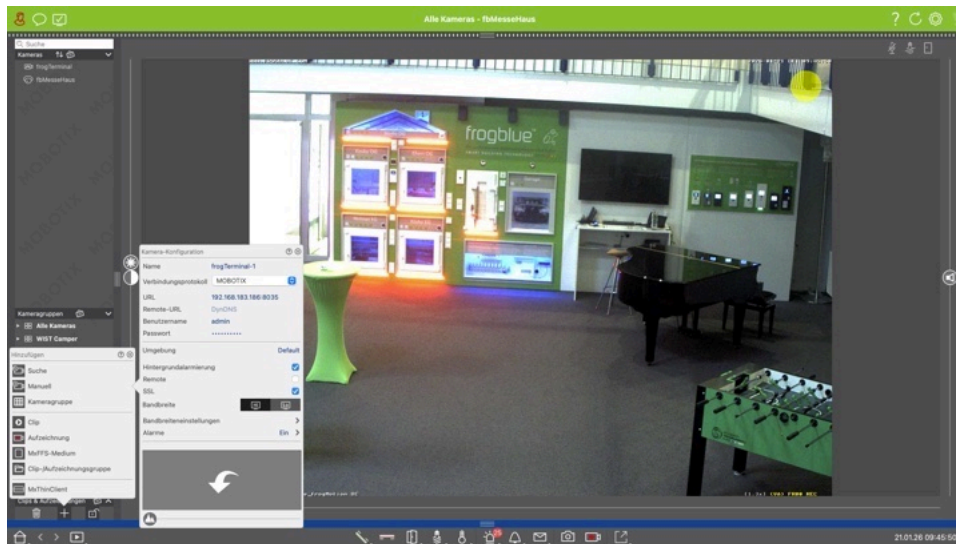
- Klicken Sie auf das **Schlosssymbol** unten in der linken Seitenleiste, um die Oberfläche zu entsperren.



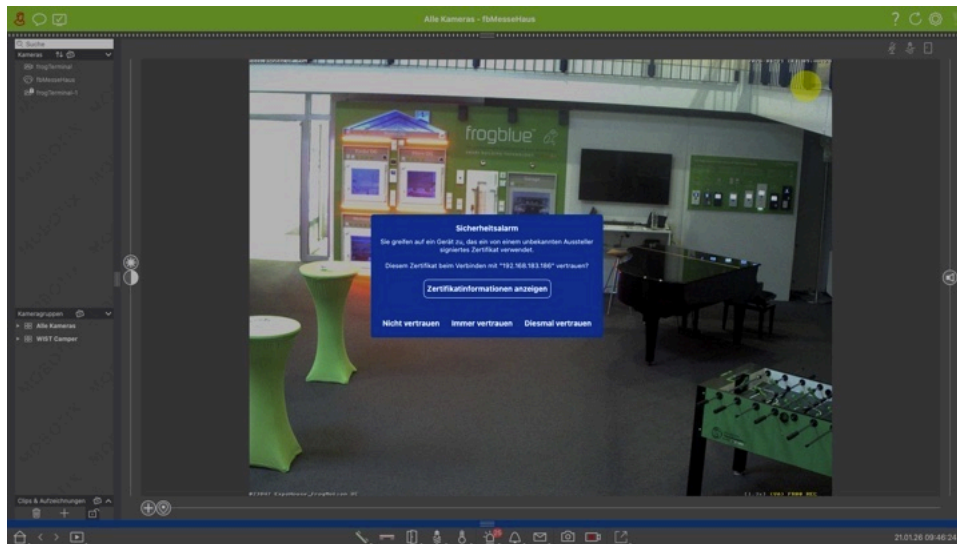
- Klicken Sie auf das **+**-Symbol unten in der linken Seitenleiste, um ein neues Geräteelement hinzuzufügen.



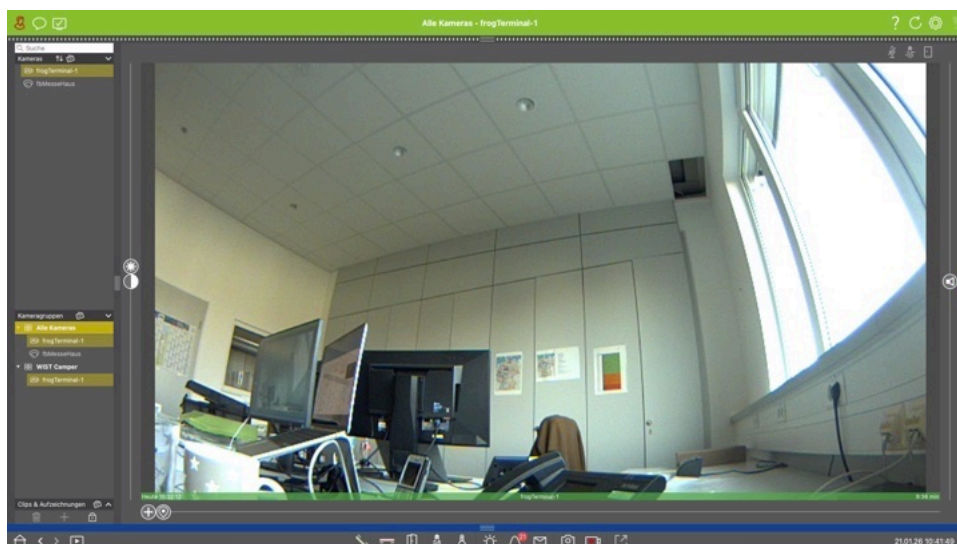
- Klicken Sie auf das **Manuell**-Symbol, um eine neue Kameraquelle hinzuzufügen.



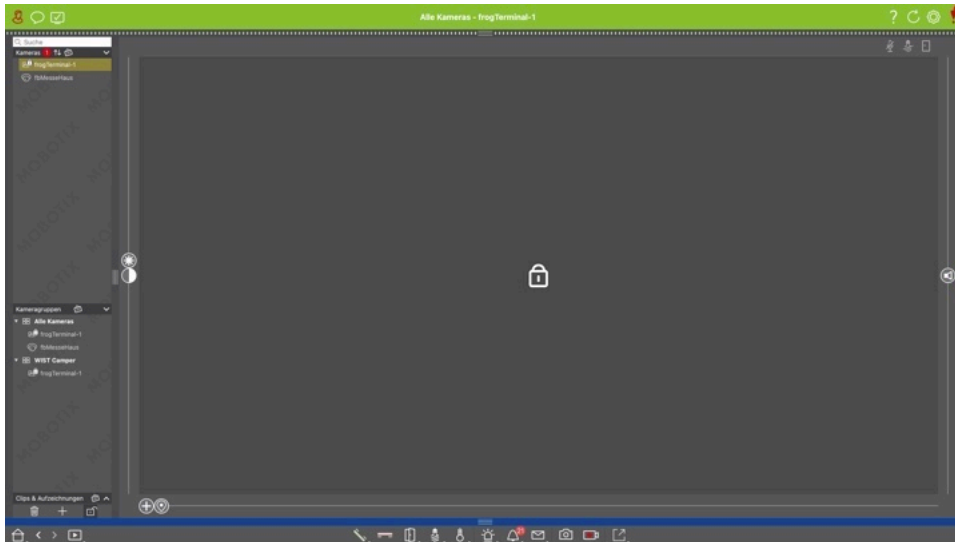
- **Name:** Geben Sie den Namen ein, unter dem Ihr frogTerminal in MxMC angezeigt werden soll.
- **Verbindungsprotokoll:** Wählen Sie **MOBOTIX** aus den Optionen.
- **URL:** Geben Sie die IP-Adresse oder URL Ihres frogTerminal gefolgt von einem Doppelpunkt und dem Port 8035 ein, z. B. „192.168.178.58:8035“.
- **Benutzername:** Geben Sie den Web-Benutzernamen für den Zugriff auf das frogTerminal ein.
- **Passwort:** Geben Sie das Web-Passwort für das frogTerminal ein.
- **Hintergrundalarme:** Aktivieren Sie diese Option, um Hintergrundalarme zu ermöglichen. Dies ist erforderlich, damit Anrufe ausgelöst werden können, wenn das Terminal nicht aktiv gestreamt wird.
- **SSL:** Aktivieren Sie diese Option, um eine sichere (SSL-)Verbindung zum frogTerminal zu verwenden. Pflichtanforderung.
- Um Ihre Einstellungen zu bestätigen, klicken Sie außerhalb der Eingabefelder - zum Beispiel auf den grauen Bereich der linken Seitenleiste.



- Wenn ein Sicherheitswarnhinweis erscheint, klicken Sie auf **Immer vertrauen**, um die sichere Verbindung zu akzeptieren. Für temporäre Tests können Sie auch **Diesmal vertrauen** auswählen.



- Sie sollten nun einen Live-Video-Stream von Ihrem frogTerminal in MxMC sehen.



Falls die Verbindung nicht hergestellt wird:

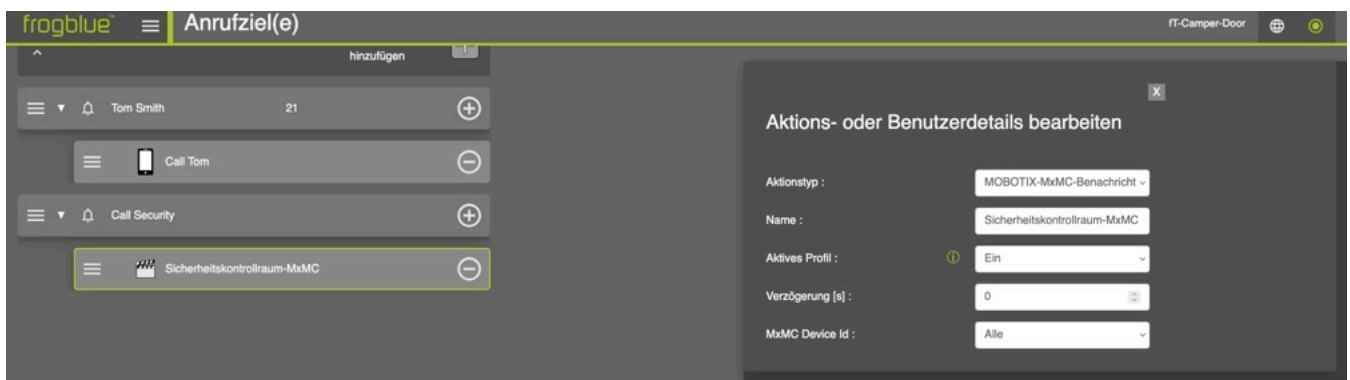
- Klicken Sie auf den Reconnect-Button (Aktualisierungssymbol oben rechts).
- Akzeptieren Sie alle angezeigten Sicherheitswarnhinweise.
- Prüfen Sie im Fehlerfall:
  - Ihre Netzwerkeinstellungen (IP-Adresse, Hostname und Port).
  - Ob der Port 8035 korrekt an Ihr frogTerminal weitergeleitet wird. (Dieser Port wird für das MOBOTIX-MxEventStream-Protokoll verwendet.)

## frogTerminal - Anrufe an MxManagementCenter

Das **frogTerminal** kann Anrufe direkt an die MxManagementCenter-Software über das MxEventStream-Protokoll tätigen.

Für die Konfiguration eines Anrufs an Ihr MxMC benötigen Sie die IP-Adresse des Rechners, auf dem die MxMC-Software installiert ist. Öffnen Sie anschließend im Browser die Benutzeroberfläche Ihres frogTerminal und gehen Sie zu **Einstellungen** → **Anrufziele**.

Fügen Sie ein Klingelschild hinzu oder wählen Sie ein vorhandenes Klingelschild aus und klicken Sie auf ►, um die Einstellungen für Anrufaktionen zu erweitern.

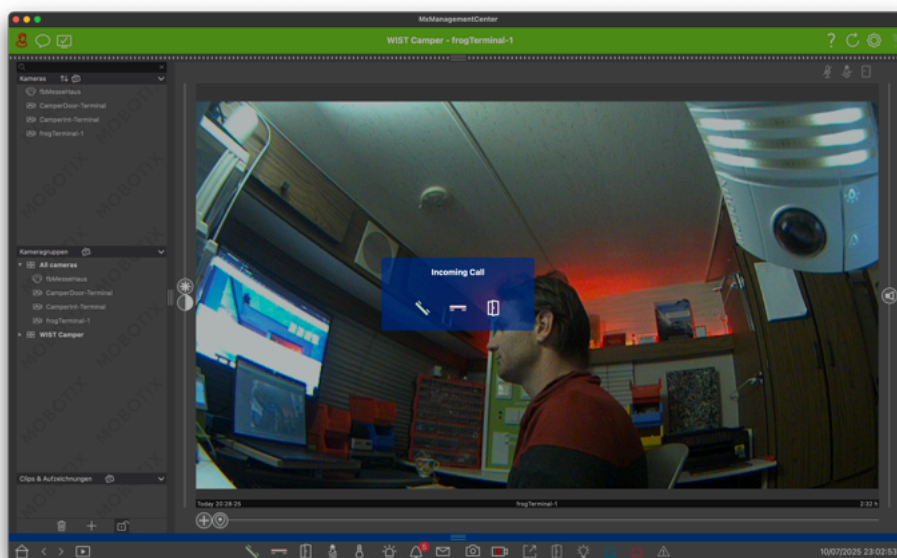
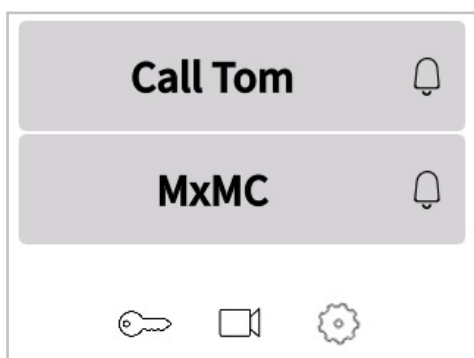


- Klicken Sie auf **Klingelschild hinzufügen** +, um eine Anrufaktion hinzuzufügen, und wählen Sie die neue Aktion aus, um sie zu bearbeiten.
- **Aktionstyp**: Wählen Sie im Dropdown-Menü **MxMC benachrichtigen** aus.

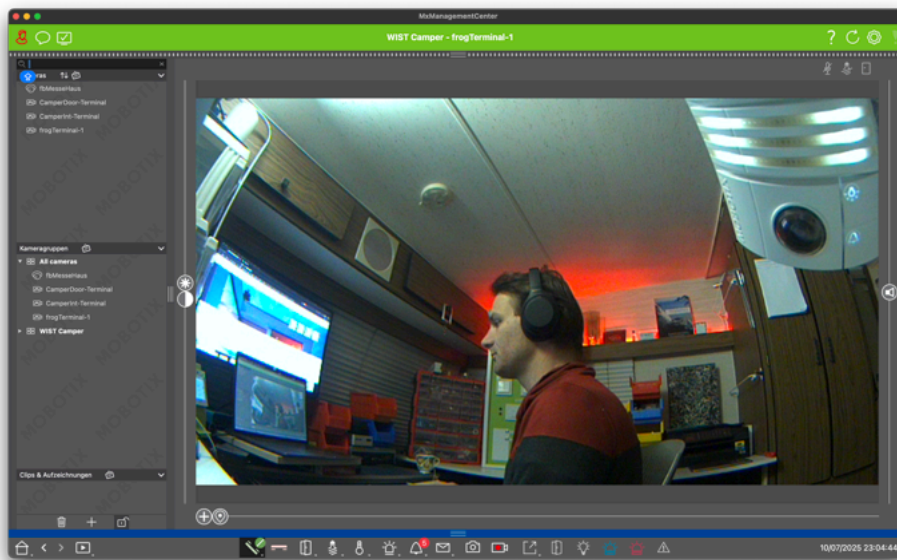
- **Name:** Geben Sie einen Namen für die Aktion ein, z. B. „Sicherheitskontrollraum-MxMC“.
- **Aktives Profil:** Wählen Sie ein Zeitprofil aus, in dem die Aktion aktiv ist.
- **Verzögerung [s]:** Zeit in Sekunden, bis die Benachrichtigung gesendet wird.
- **MxMC Device ID:** Wählen Sie *Alle*, um alle im Netzwerk laufenden MxMC-Instanzen zu benachrichtigen, oder wählen Sie eine bestimmte Instanz aus der Liste der eindeutigen IDs aus. Die Instanzen werden automatisch erkannt, sobald sich MxMC mit Ihrem frogTerminal verbindet.
- Klicken Sie auf **Speichern**, um die neue Klingelaktion **MxMC benachrichtigen** zu erstellen.

Tipp: Anrufe können auch direkt vom MxMC an das frogTerminal getätigt werden, indem Sie während einer Live-Stream-Verbindung auf das Telefonsymbol klicken.

Tippen Sie anschließend auf das neu erstellte Klingelsymbol (z. B. „MxMC“) auf der Klingel-Seite des frogTerminal-Touchscreens.



- Ein Anruf wird ausgelöst und sollte in MxMC angezeigt werden.
- Das Türsymbol löst direkt den Türöffner des frogTerminals aus, wie unter **Steuerung** → **Türen** definiert.
- Das grüne Telefonsymbol ermöglicht das Annehmen des Anrufs und startet Live-Video und -Audio vom frogTerminal zu MxMC.
- Das rote Telefonsymbol lehnt den Anruf ab.



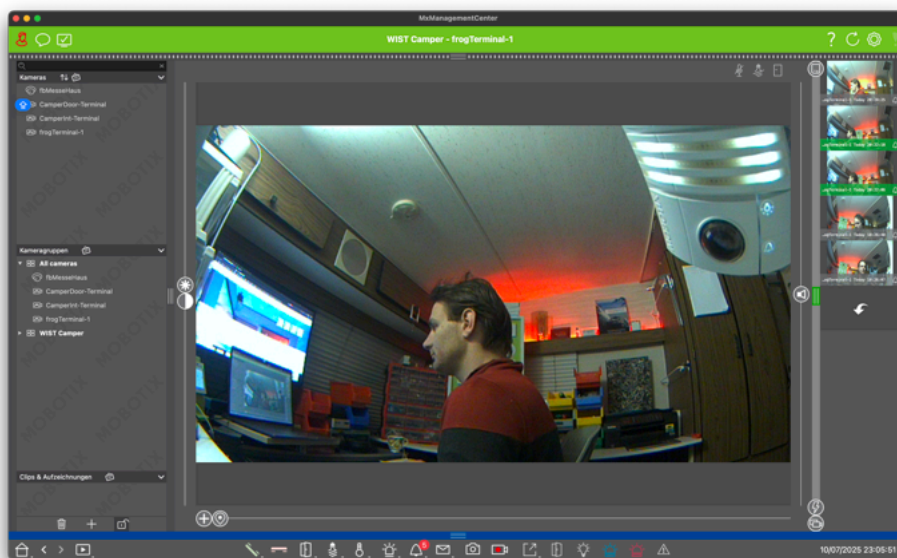
Während eines Anrufs:

- Sprechen: Halten Sie das grüne Anrufsymbol gedrückt.
- Tür öffnen: Klicken Sie auf das Türsymbol, um die Tür auszulösen.
- Licht schalten: Klicken Sie auf das Lichtsymbol, um das Licht auszulösen.
- Anruf beenden: Klicken Sie auf das rote Telefonsymbol.

### frogTerminal - Ereignisprüfung mit MxManagementCenter

Das frogTerminal bietet eine einfache Bild-Ereignisprüfung über MxMC.

Um Ereignisse zu prüfen, öffnen Sie in MxMC die rechte Seitenleiste mit dem Ereignisstreifen.



- Klicken Sie auf ein Ereignisbild, um es im Vollbildmodus anzuzeigen.

## 21. Erweiterte Integration und API-Funktionen

**Hinweis:** Spezialfunktionen! Setzen Sie sich mit Ihrem frogblue-Partner oder dem lokalen frogblue-Kompetenzzentrum in Verbindung für mehr Details.

### 21.1. Benutzerdefinierte Anzeigeoberflächen

Passen Sie die Benutzeroberfläche Ihres frogTerminal an, um beeindruckende Designs und fortschrittliche Integrationen zu erreichen. Diese hochwertige, smarte Zutrittskontrollschnittstelle ist die ideale Lösung, um Ihr System oder Ihr SaaS-Angebot aufzuwerten - mit verbesserter Ästhetik und erweiterten Funktionalitäten.

### 21.2. Zeiterfassung und Anwesenheitsmanagement

Nutzen Sie das frogTerminal, um die Zeiterfassung der Mitarbeiter zu optimieren. Konfigurieren Sie einfache Check-in-, Pausen- und Check-out-Optionen und exportieren Sie die Anwesenheitsprotokolle in Ihr bevorzugtes Workforce-Management-System für eine effiziente Dokumentation.

Beispielanwendungen umfassen:

- **Logistik:** Benachrichtigen Sie Lagerautomationssysteme, um einen Auftrag bei Zutritt vorzubereiten oder zu versenden. Automatisches Beleuchten eines Weges zum Liefertor für effiziente Navigation.
- **Gesundheitswesen:** Lösen Sie einen Rufsystemaufruf für Pflegepersonal aus oder loggen Sie Besucherdetails von Patienten, um die Lieferung kritischer Medikamente zu bestätigen - einschließlich QR-Code-Verifizierung, um sicherzustellen, dass das richtige Medikament der richtigen Person verabreicht wird.
- **Gebäudeautomation:** Aktivieren Sie die Beleuchtung und passen Sie die HVAC-Einstellungen entlang einer definierten Route für den Benutzer an oder rufen Sie automatisch einen Aufzug zur richtigen Etage.

## 22. Wartung und Fehlersuche

### 22.1. Firmware-Updates

Halten Sie das Terminal mit den neuesten Funktionen und Sicherheitspatches auf dem aktuellsten Stand.

### 22.2. Systemsteuerung - Konfigurationsdateien, Neustart und Werkseinstellungen

Dieser Abschnitt beschreibt, wie die gesamte Konfiguration herunter- oder hochgeladen, das System neu gestartet oder das Gerät auf Werkseinstellungen zurückgesetzt wird.

**Terminal über das Webinterface auf Werkseinstellungen zurücksetzen**


Menü: **System** → **Systemsteuerung**

Um einen Werksreset durchzuführen, klicken Sie auf **Auf Werkseinstellungen zurücksetzen** und dann auf **Ja** zur Bestätigung. Warten Sie, bis im Browser die Meldung **Done** erscheint und der Terminalbildschirm zum Begrüßungsbildschirm mit der Option **Start Wizard** zurückkehrt. Bitte beachten Sie, dass der Reset-Prozess mehrere Minuten in Anspruch nehmen kann, um alle Protokolle

und Aufnahmen zu löschen. Für optimale Ergebnisse erlauben Sie ausreichend Zeit und führen Sie nach dem Reset einen Neustart oder eine Stromunterbrechung durch.

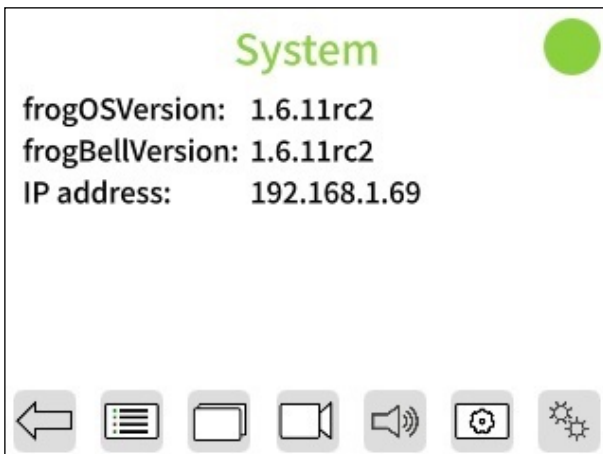
### Über die On-Screen-Oberfläche




- Tippen Sie , um in den Konfigurationsmodus zu gelangen.




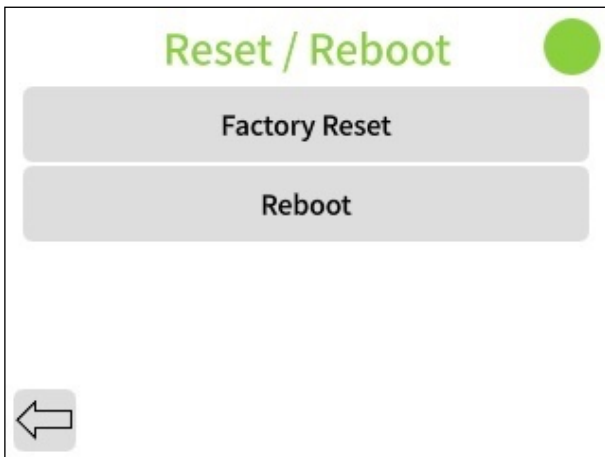
- Geben Sie Ihre sechsstellige Admin-PIN ein und tippen Sie auf **OK**.



- Tippen Sie , um auf die zusätzliche Einstellungsseite zuzugreifen.

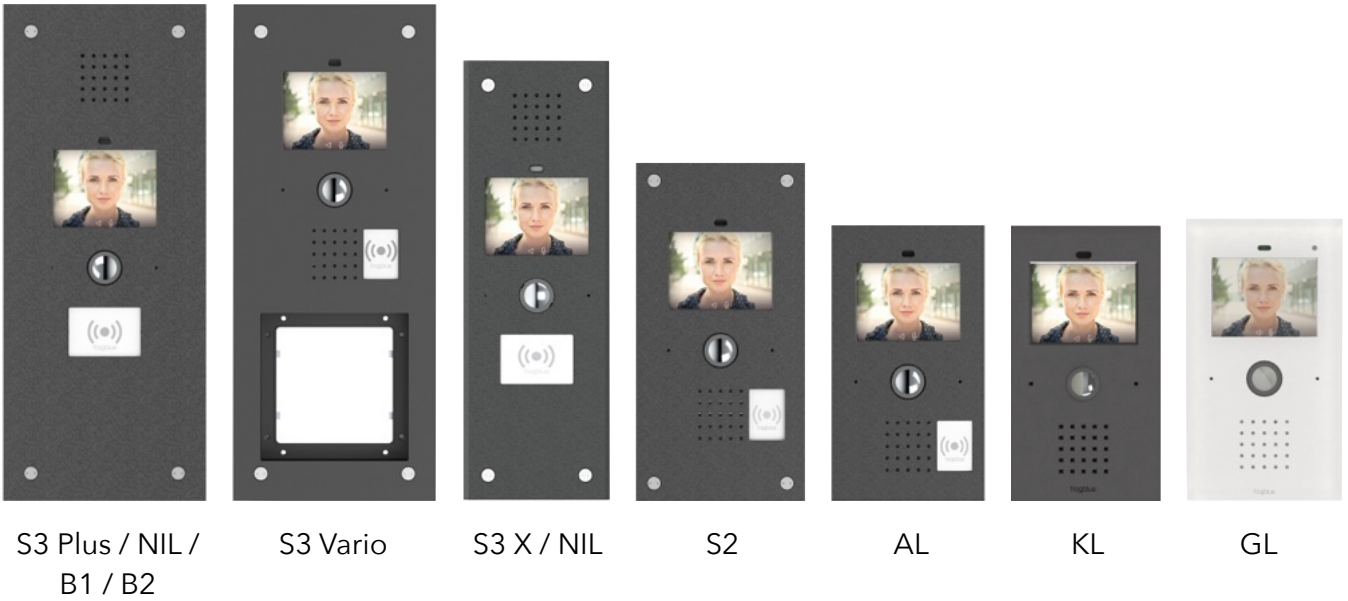


- Tippen Sie , um das Menü für System-Reset und Neustart zu öffnen.












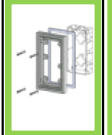
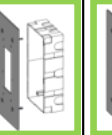
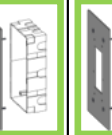

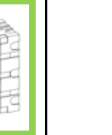

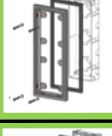
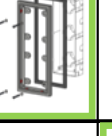

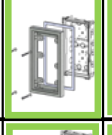
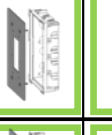
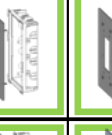
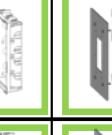



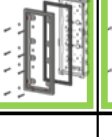
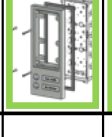


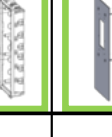
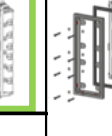

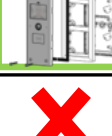




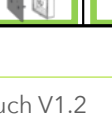


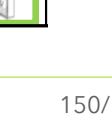
**Hinweis:** Ein Hard-Reset kann mit der frogProject App durchgeführt werden, wenn alle PINs & Passwörter vergessen wurden. Wenden Sie sich an Ihren frogblue-Partner oder das lokale frogblue-Kompetenzzentrum für Unterstützung.

## D. Terminal Versionen

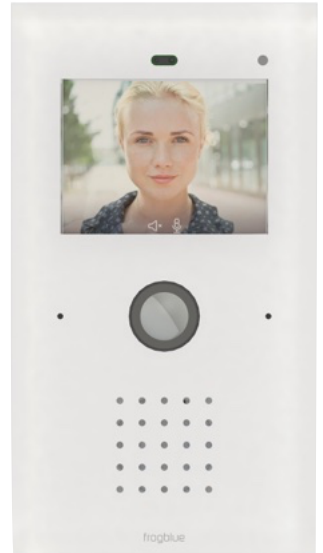
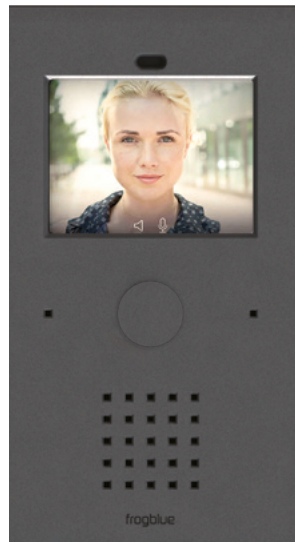
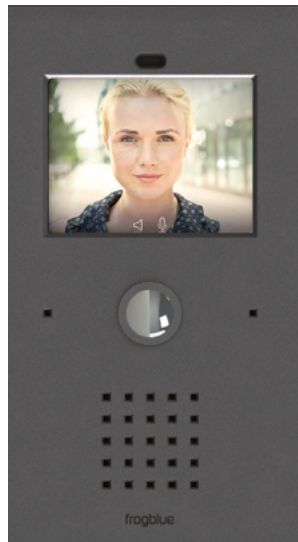
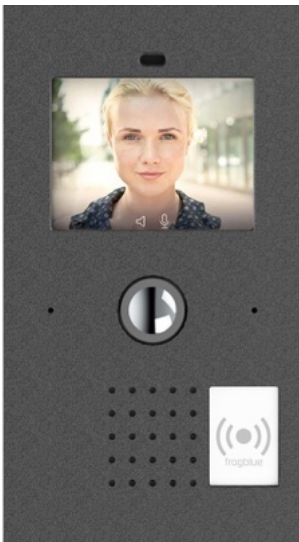


Verfügbar in weiß, silber und anthrazit.

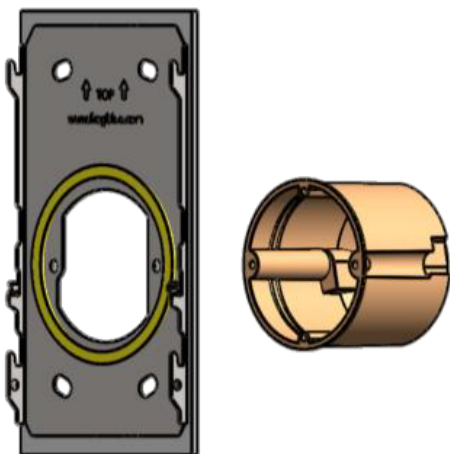
### Ersetzungsanleitung

								
	S3 X / NIL	S3 Plus / NIL / B1 / B2	S3 Vario	S2	AL	GL	Station	KL
Siedle © 2er flush-mounted box	✗		✗					
Siedle © 3er flush-mounted box				✗	✗	✗	✗	✗
Mobotix © 2er flush-mounted box	✗		✗					
Mobotix © 3er flush-mounted box								
Siedle © 3er Onwall box		✗	✗	✗	✗	✗	✗	✗
Mobotix © 3er Onwall box		✗	✗	✗				
Mobotix © 2er Onwall box	✗	✗	✗	✗				

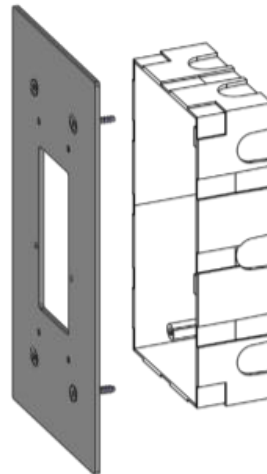
## Terminal Versionen AL / KL Station / GL



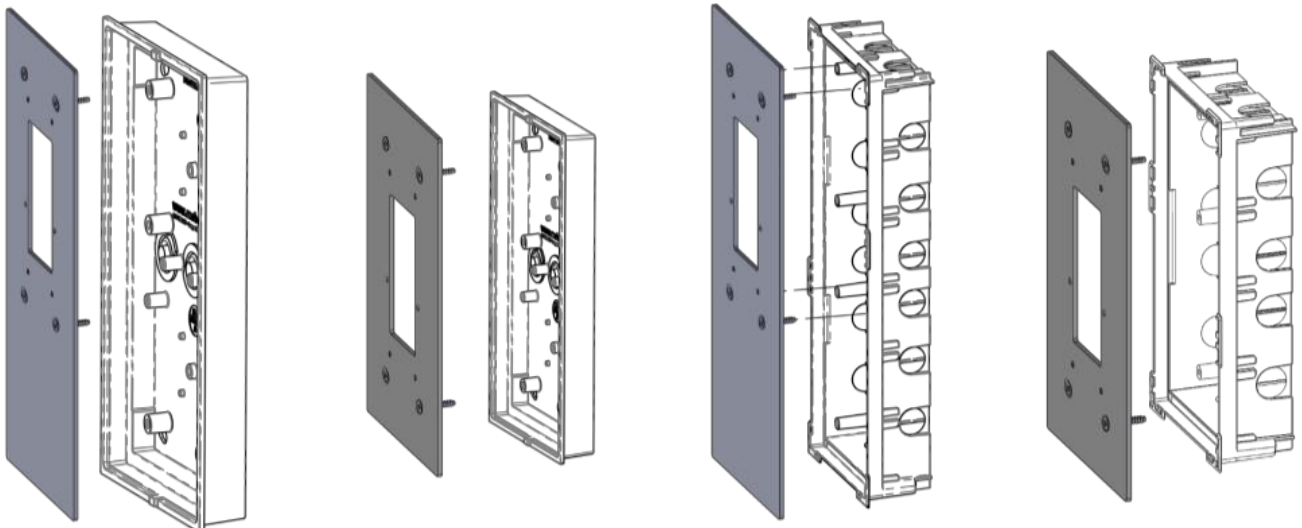
### Neue Installation



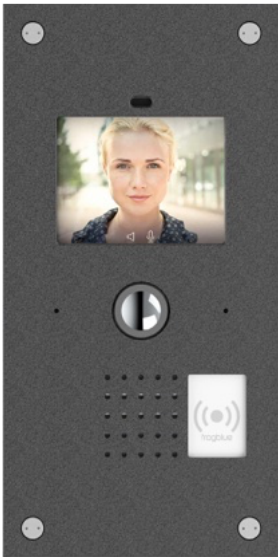
### Ersatz bei bestehender SIEDLE Installation



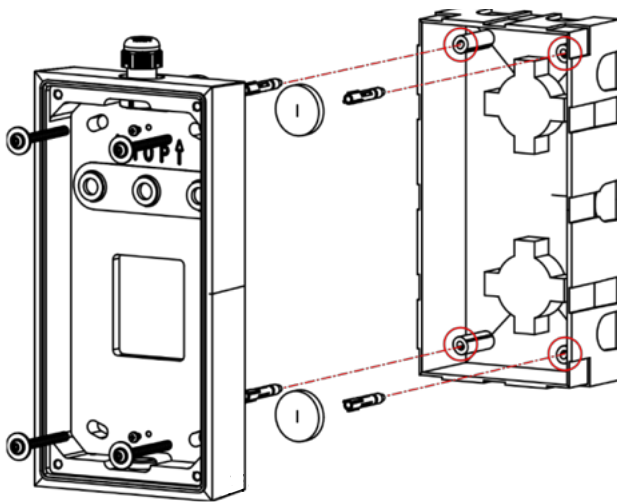
### Ersatz bei bestehender MOBOTIX Installation



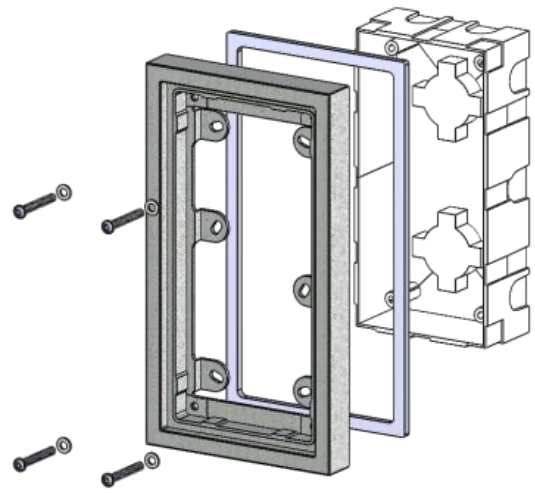
## Terminal Version S2



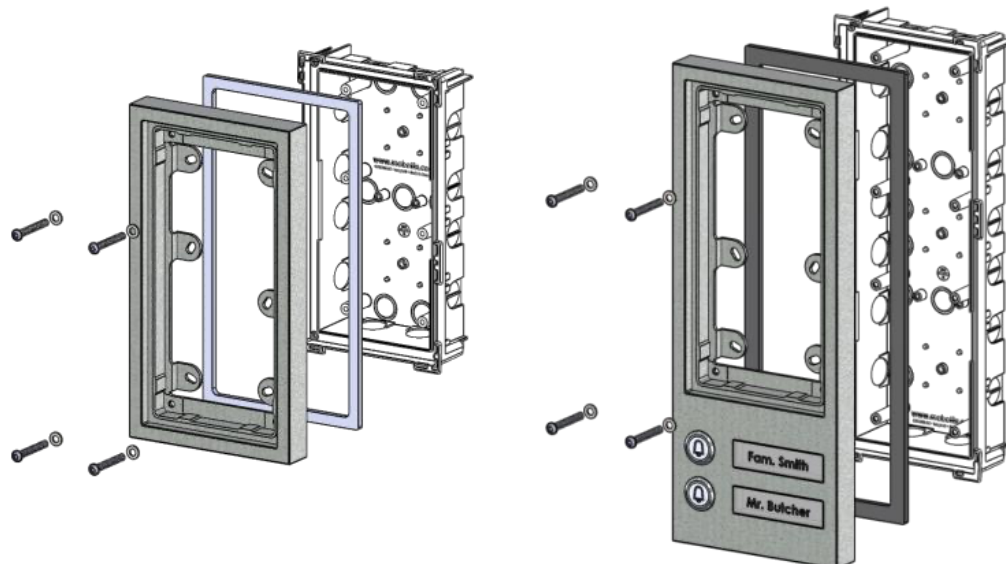
### Neue Installation



### Ersatz bei bestehender SIEDLE Installation

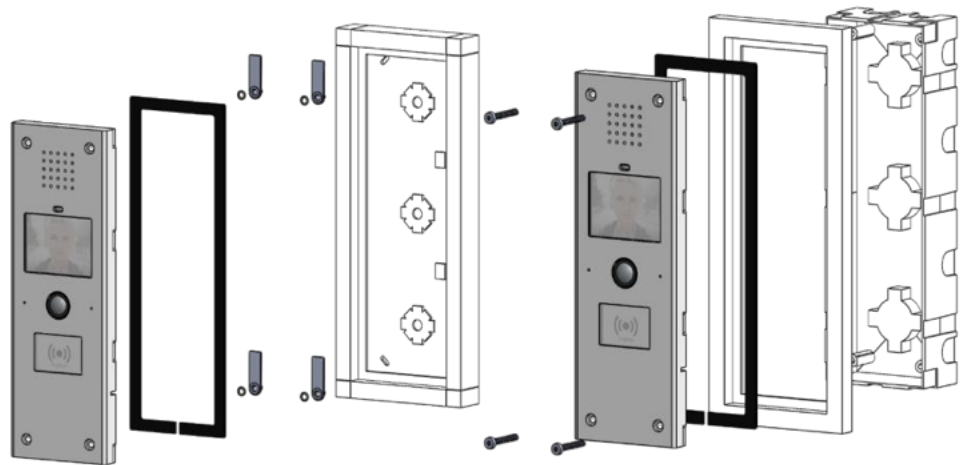
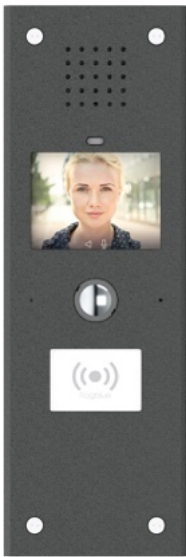


### Ersatz bei bestehender MOBOTIX Installation

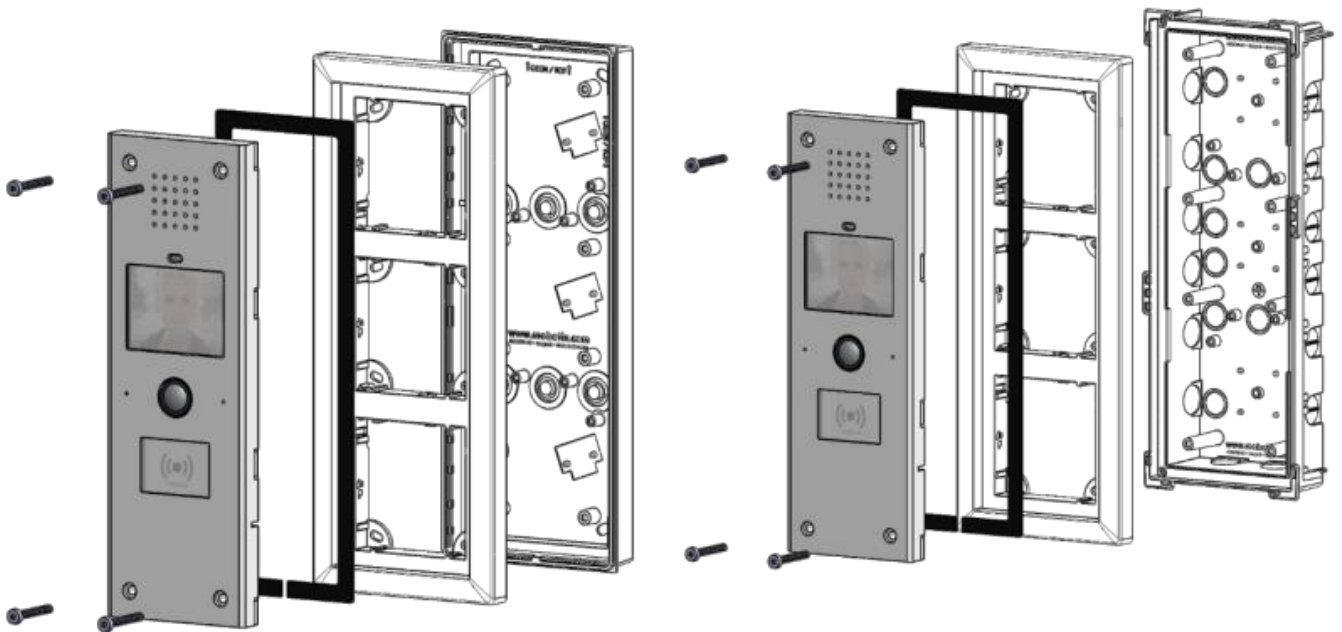


## Terminal Version S3 X / NIL

### Ersatz bei bestehender SIEDLE Installation



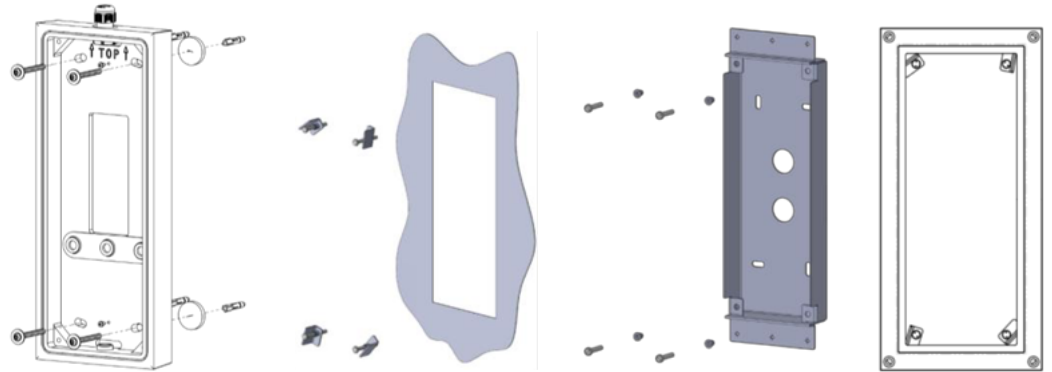
### Ersatz bei bestehender MOBOTIX Installation



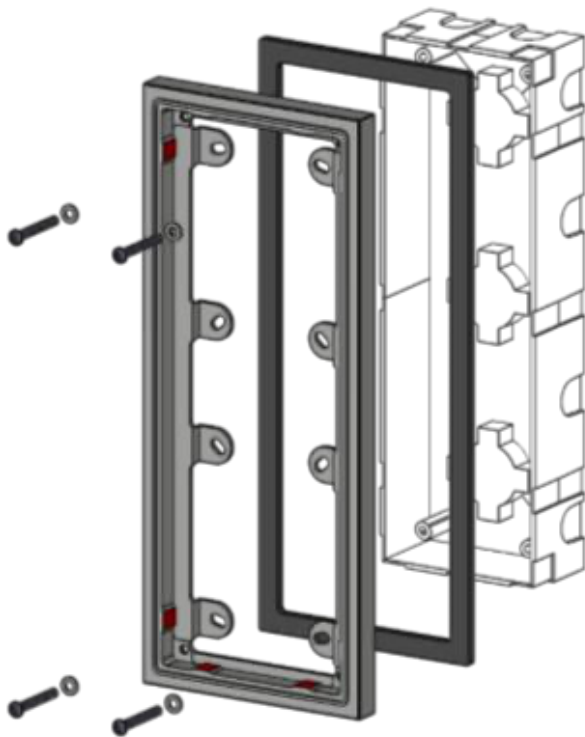
# Terminal Version S3 Vario



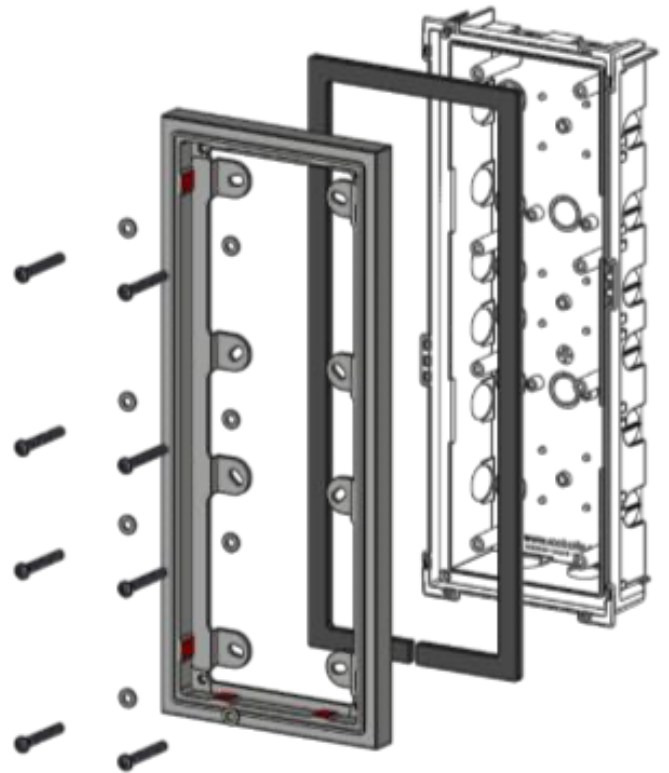
Neue Installation



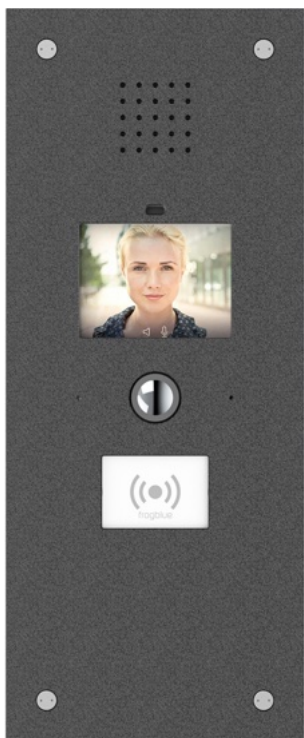
Ersatz bei bestehender SIEDLE Installation



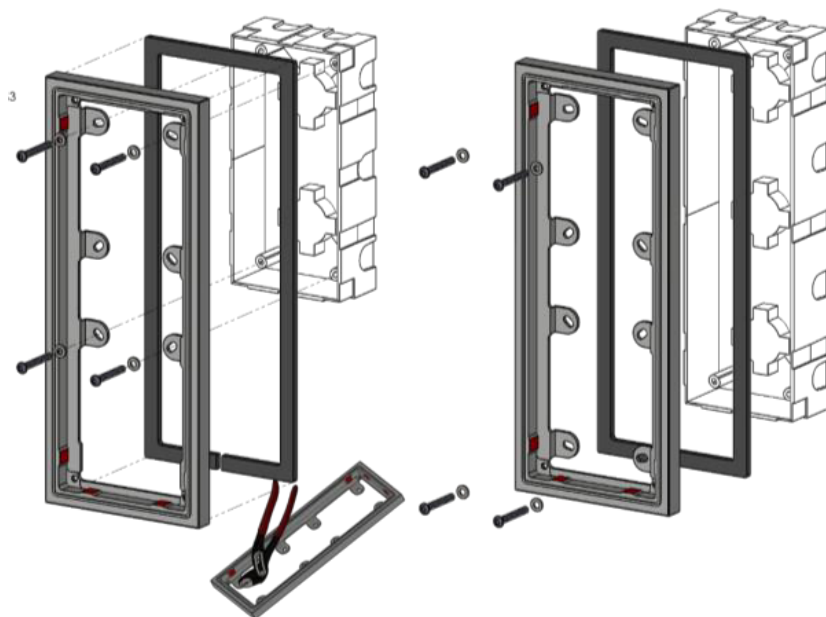
Ersatz bei bestehender MOBOTIX Installation



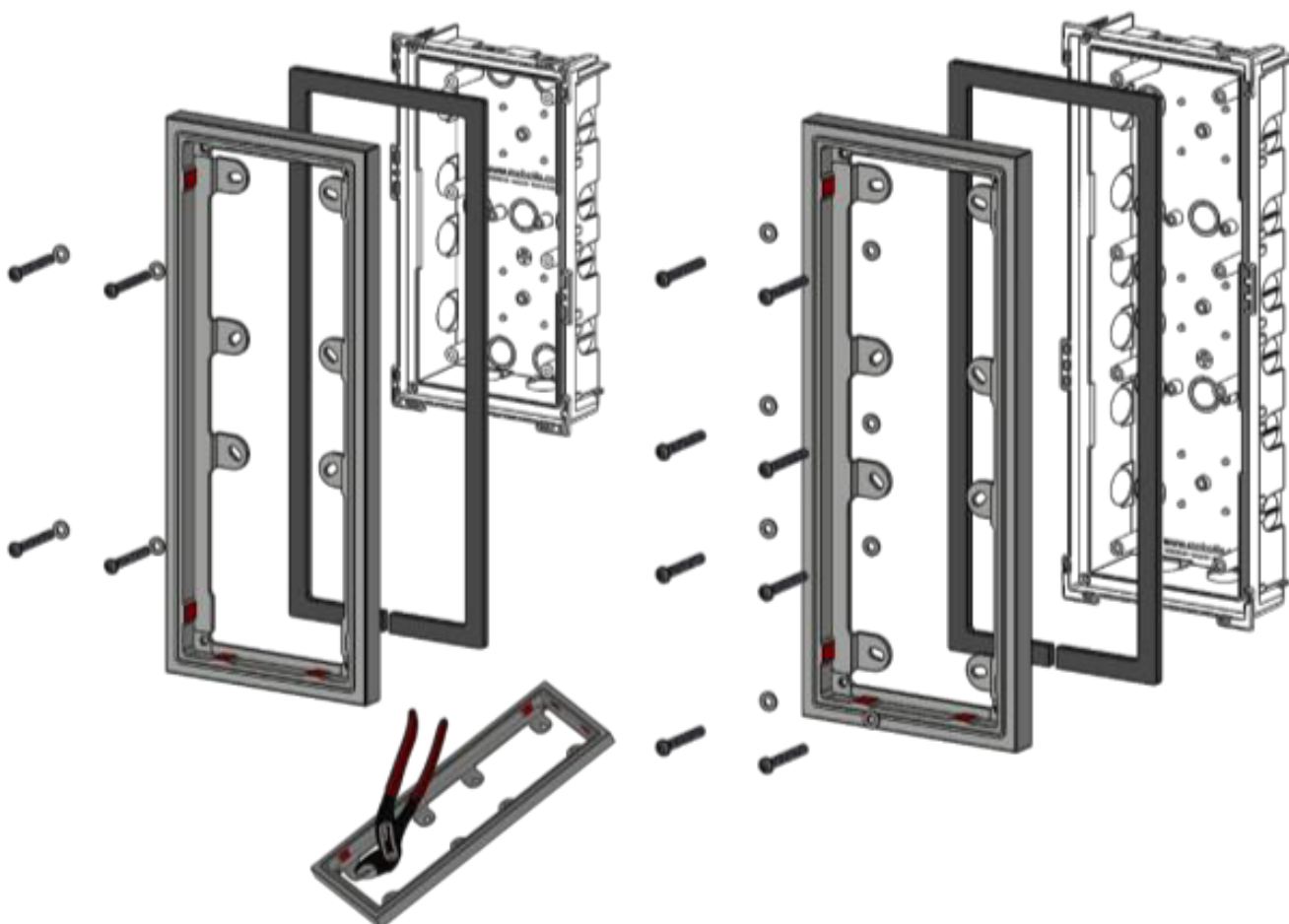
# Terminal Version S3 Plus / B1 / B2 / NIL



Ersatz bei bestehender SIEDLE Installation



Ersatz bei bestehender MOBOTIX Installation





Wir verknüpfen drahtlos via **Bluetooth**<sup>®</sup> Leuchten, Jalousien, Lüfter, Fenster, Türen, Heizung, Türsprechstellen und normale Lichtschalter.

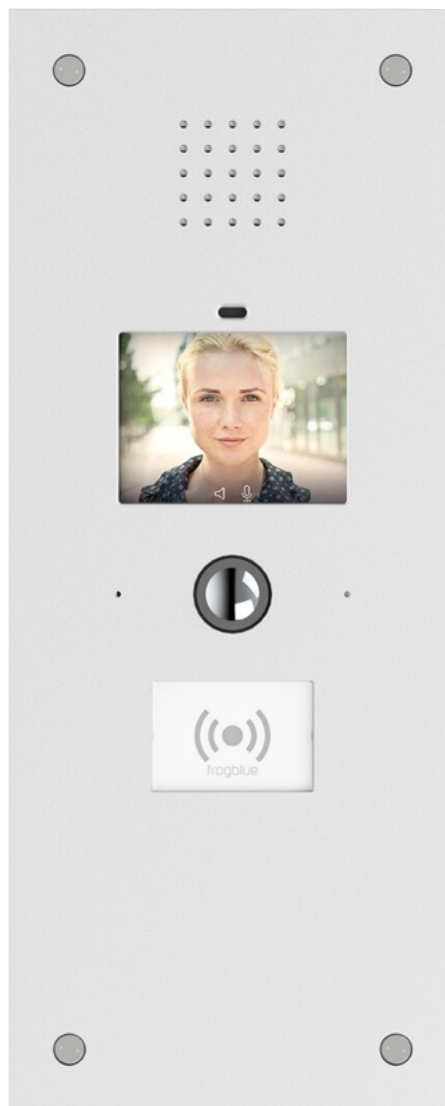
Unsere frogs werden hinter üblichen Lichttastern/Steckdosen installiert und benötigen lediglich 230V. Steuerleitungen entfallen, denn Verbindungen werden virtuell geknüpft.

Eine **einzige App** steuert das gesamte Haus entweder lokal über Bluetooth<sup>®</sup> oder weltweit per Smartphone. Frogblue wird unkompliziert ohne Server und ohne Schaltschrank installiert und kinderleicht konfiguriert.

Unsere Türsprechstelle **frogTerminal** unterstützt den weltweiten SIP-Telefon-Standard und ist deshalb voll mehrparteien tauglich. Zusammen mit dem integrierten RFID-Leser und einer PIN wird eine dezentrale Zutrittslösung mit 3-Faktor-Authentifizierung ermöglicht.

Unsere großen Stärken sind die **Zuverlässigkeit und Sicherheit** eines ausgereiften Systems, das auch nach Jahren noch den Anforderungen des Nutzers angepasst werden kann.

**Hinweis:** die Software und Benutzer-Oberflächen sind in mehr als 20 Sprachen verfügbar!



Copyright 2025, fb Vertriebs AG

Alle Rechte vorbehalten. Texte, Bilder und Grafiken unterliegen dem Schutz des Urheberrechts. Der Inhalt dieser Broschüre darf nicht kopiert, verbreitet oder verändert werden. Verbindliche technische Daten entnehmen Sie bitte unserem Systemhandbuch. Technische Änderungen vorbehalten. frogblue und die Bildmarke sind eingetragene Marken der fb Vertriebs AG.

