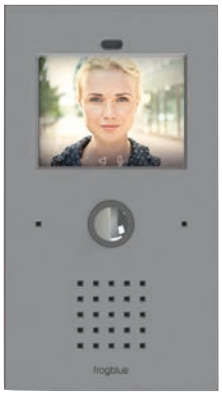
# frogTerminal Installationshandbuch

## 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

S3X

S3 Plus

S3 Plus B1

S3 Plus B2

S3 Vario

# frogTerminal Installationshandbuch

Funktionsübersicht und technische Beschreibung


**A. Einführung, Systemübersicht und Hauptmerkmale 7**

**1. Übersicht 7**

**2. Hauptvorteile des frogTerminals 8**

**3. Telefonie-Übersicht 8**

3.1. Weltweiter Telefonie-Standard 8
3.2. Direkte Integration von Endgeräten 9
3.3. Das frogDisplay 9
3.4. Die frogStation 9
3.5. Integration mit Telefoniesystemen 10
3.6. frogSIP-App und das Anrufen eines Smartphones 10
3.7. Mischbetrieb 10
3.8. Video-Gegensprechanlage 11

**4. Überblick über die Zutrittskontrolle 11**

4.1. Einführung 11
4.2. Dezentrale Zutrittskontrolle 11
4.3. NFC/RFID-Karteninformationen 11
4.4. Zutritts-Funktionen 12
4.5. Besondere Zutrittsfunktionen 12
4.6. Übersicht der frogTerminal Zutrittskontrolleinstellungen 13
4.7. Hinzufügen und Sperren von RFID-Karten 14
4.8. Benutzeranzeige am Terminal 14

**5. Hardware-Integrationen 14**

5.1. Relais und Eingänge 14
5.2. IP-Link-Integration 15
5.3. PIN-Steuerung 15
5.4. USB-C Erweiterung (USB 2.0 kompatibel) 15
5.5. Bluetooth Mesh-Integration 15
5.6. Vario Modul-Slot 15

**6. Kernfunktionen 16**

6.1. Funktionen der Zutrittskontrolle 16
6.2. SIP-Telefoniefunktionen 16
6.3. Funktionen für Aufnahme und Ereignisverwaltung 17
6.4. SIP-Telefonie-Registrierung und Kosten 17

**7. Zutrittskontrollmanagement 17**

7.1. Cloud-basiertes Zutrittskontrollmanagement (frogAccessControl) 17
7.2. Lokale Benutzerverwaltung (frogEasyAccess) 17

7.3. RFID-Kartenverschlüsselung 18
7.4. Initialisierung und Authentifizierung von RFID-Karten 18
7.5. Auf der Karte gespeicherte Informationen 19
7.6. Terminal-Einstellungen 19
7.7. Hinzufügen und Sperren von Karten 19
7.8. Benutzeroberfläche für die Zutrittskontrolle 20

**8. Inbetriebnahme 20**
8.1. Einrichtungsprozess 20
8.2. Initiale Einrichtungsanforderungen 20

**9. Vorteile & Differenzierung 21**

**10. Zusätzliche Funktionen 22**
10.1. Mehrparteien-Türklingelfunktionalität 22
10.2. Erweiterte SIP-Telefoniefunktionen 22
10.3. Innovationen in der Zutrittskontrolle 22
10.4. Integration mit Drittanbietersystemen 22
10.5. Cloud-basiertes Management 23
10.6. Lokale Management-Funktionen 23
10.7. Strom- und Anschlussoptionen 24
10.8. Zeiterfassung und Anwesenheitsmanagement 24

**B. Technisches Installationshandbuch 25**

**1. Einführung 25**
1.1. Zweck des Handbuchs 25
1.2. Sicherheit & Konformität 25
1.3. Benötigte Werkzeuge & Ausrüstung 25
1.4. Systemübersicht 26
1.5. Installationsablauf 26
1.6. Support & Dokumentation 26

**2. Vor-Installationsanforderungen 27**
2.1. Standortanforderungen 27
2.2. Strom & Konnektivität 27
2.3. Abmessungen & Gewicht 28
2.4. Standortbewertung 29
2.5. Benötigte Komponenten für die Installation 29
2.6. Lieferumfang 29

**3. Physischer Installationsprozess 30**
3.1. Montage des Geräts 30
3.1.1. Standardmontage an der Oberfläche 30
3.1.2. Aufsatzmontage 31
3.2. Anschluss von Strom & Netzwerk 31

**4. Ersteinrichtung & Konfiguration On-Device Touchscreen-Installationsassistent 31**
4.1. Installationsassistent – Schritt 1: Sprache und Zeitzone einstellen 32

4.2. Installationsassistent – Schritt 2: Admin-PIN festlegen 33
4.3. Installationsassistent – Schritt 3: Web-Passwort / HTTPS Admin-Passwort festlegen 34
4.4. Installationsassistent – Schritt 4: frogblue Mesh Setup 35
4.5. Installationsassistent – Schritt 5: Gerätenamen festlegen 36
4.6. Installationsassistent – Schritt 6: Startbildschirm-Layout festlegen 36
4.7. Installationsassistent – Schritt 7: frogTerminal mit Ihrem Netzwerk verbinden 37
4.8. Installationsassistent – Schritt 8: Verbindung zur frogCloud herstellen 38
4.9. Installationsassistent – Schritt 9: Login zu oder Registrierung eines frogCloud-Kontos 38
4.10. Installationsassistent – Schritt 10: Bestätigen Sie die Aktivierungs-E-Mail des Kontos 39
4.11. Installationsassistent – Schritt 11: Cloud-Projekt erstellen 39
4.12. Installationsassistent – Schritt 12: Türklingeltasten erstellen 39
4.13. Installationsassistent – Schritt 13: Mit einem smarten Gerät koppeln 40
4.14. Startansicht und Erklärungen der Anzeigemodi 40
4.15. Installationsassistent – Schritt 14: Startansicht auswählen 42
4.16. Installationsassistent – Schritt 15: Assistent abschließen 42

**5. frogSIP App Benutzeroberfläche 43**

5.1. Einführung in frogSIP 43
5.2. Übersicht des Begrüßungsbildschirms 43
5.3. Neues frogCloud-Benutzerkonto über die frogSIP App erstellen 44
5.4. Anmeldung in der frogSIP App mit einem bestehenden frogCloud-Benutzerkonto 46
5.5. Übersicht der Hauptbenutzeroberfläche der App 48
5.5.1. In-Call Symbolleiste 50
5.5.2. Logs & Wiedergabe Symbolleiste 50
5.6. Kopplung des Terminals mit der frogSIP App 51
5.7. Anrufen, Wiedergabe und Verwaltung des frogTerminals mit frogSIP 54
5.7.1. Empfang von Anrufen 54
5.7.2. Automatische Anrufannahme-Konfiguration 54
5.7.3. Anrufe initiieren 54
5.7.4. Zutritts- & Ereignisprotokolle und Wiedergabe eines frogSIP-Anrufs 56

**6. Zutrittskontrollkonfiguration 57**

6.1. Einführung in die Zutrittskontrolle von frogTerminal 57
6.2. PINs, Zutrittscodes 57
6.3. Grafisches Feedback für Zutrittsereignisse 57
6.4. Dezentrale Zutrittskontrolle 60
6.5. Karteninformationen 60
6.6. Zutritts-Funktionen 61
6.7. Spezialfunktionen 61
6.8. RFID-Verschlüsselung und Zonen 61
6.8.1. RFID-Verschlüsselung und Zonen über den Webbrowser (Terminal-Einstellungen) 62
6.8.2. RFID-Verschlüsselung und Zonen über den On-Device-Touchscreen. 65
6.9. Hinzufügen und Sperren von Karten 65
6.9.1. Hinzufügen und Sperren von Karten über den Webbrowser 66
6.9.2. Hinzufügen und Sperren von Schlüsseln/Karten über den On-Device-Touchscreen 70

6.9.3. Lesen & Formatieren von Schlüsseln/Karten 72
6.9.4. Über den Webbrowser (RFID → ZutrittsListe) 72
6.9.5. Über den On-Device-Touchscreen 72

**7. Telephony Call Destination Einrichtung 74**
7.1. Klingelsignale / Ruftasten 74
7.1.1. Klingelaktionen: frogSIP-Benutzer einladen 75
7.1.2. Klingelaktionen: Direkte SIP-Anrufe per IP 76
7.1.3. Klingelaktionen: SIP-Anrufe über SIP-Server 77
7.1.4. Klingelaktionen: frogMessage senden 77
7.1.5. Klingelaktionen: Hardware-Relais auslösen 78
7.1.6. Klingelaktionen: Öffner-Sequenz starten 78
7.1.7. Klingelaktionen: IP-Notify senden 79
7.1.8. Klingelaktionen: Bild anzeigen 80
7.2. Authentifizierungs-Anrufziel 80
7.3. Automatische Aktionen 80

**8. Kameraeinstellungen und Aufnahmeverwaltung 81**
8.1. Konfiguration der Kameraeinstellungen 81
8.2. Optimale Einstellungen für geringe Latenz und hohe Bildrate 82
8.3. Ereignis-Aufnahmeeinstellungen 82

**9. Admin-PIN & Funktions-PINs 83**

**10. Ein- / Ausgabe-Einstellungen 84**

**11. Hardware-Einstellungen: Näherungssensor & Touchscreen-Display 85**

**12. Touchscreen-Display-Layout 86**

**13. Allgemeine Terminal-Einstellungen 87**

**14. Türsteuerungseinstellungen 88**

**15. Onboard-Medieneinstellungen 89**
15.1. Audio-Dateien 89
15.2. Bilddateien 89
15.3. Video-Dateien 89
15.4. Streamliste 89
15.5. Ereignisbilder 90

**16. Konfiguration des frogTerminals für Automatisierung via frogCast/frogMesh 91**

**17. Netzwerkkonfiguration 92**
17.1. Ethernet- oder WLAN-Einrichtung 92
17.1.1. Netzwerkkonfiguration über den Webbrowser. 92
17.1.2. Netzwerkkonfiguration über den On-Device-Touchscreen. 92
17.1.3. Ethernet-Konfiguration über den On-Device-Touchscreen. 93
17.1.4. WLAN-Konfiguration über den On-Device-Touchscreen. 94
17.1.5. Fehlersuche bei Netzwerkverbindungsproblemen 94
17.2. SIP-Server-Registrierung 95

17.2.1. SIP-Grundlagen 95
17.2.2. SIP-Einrichtung über den Webbrowser 96
17.3. Benutzerdefinierte Root-Zertifikate 97

**18. Integration mit Drittanbieter-Videosystemen 99**
18.1. HTTPS- oder Web-Integration – Unverschlüsselter MJPEG-Stream 99
18.2. RTSP-Einstellungen 99
18.3. RTSP-Stream-Integration 101
18.4. Integration mit MOBOTIX MxManagementCenter 106

**19. Erweiterte Integration und API-Funktionen 109**
19.1. Benutzerdefinierte Anzeigeoberflächen 109
19.2. Zeiterfassung und Anwesenheitsmanagement 109

**20. Wartung und Fehlersuche 110**
20.1. Firmware-Updates 110
20.2. Systemsteuerung – Konfigurationsdateien, Neustart und Werkseinstellungen 110

# 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 Telefoniesystems 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 Netzwerkkabel
- 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 für die automatische Konfiguration von Displays (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 zugewiesen wird. 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 Telefoniesystemen

IP-Telefoniesysteme 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 Telefonsysteme fungieren.

In Mehrparteien-Umgebungen verlassen sich Mieter oft auf separate Telefonsysteme. Die Lösung: Das frogTerminal unterstützt die gleichzeitige Registrierung und arbeitet mit mehreren SIP-Servern gleichzeitig, was eine nahtlose Integration über verschiedene Telefoniesysteme 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 Telefoniesystemen (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. Dieser 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 globaler 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 Terminals-Einstellungen 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 Parkschranke
- 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. Zunächst unterstützt es die einfache Integration von Modulen, ohne dass die ProjectApp verwendet wird. In späteren Updates wird es vollständig in frogblue-Projekte integriert.

Unterstützte Module:

- frogEntry: Für die Türöffnung (drei Eingänge, zwei 12V Ausgänge)
- frogRelay-LV: 24V-Version mit zwei Ausgängen und zwei Eingängen, geeignet für Torsteuerung
- frogDim: Für die Lichtsteuerung

### 5.6. Vario Modul-Slot

Das frogSIP Terminal Vario beinhaltet einen dedizierten Slot für ein Vario-Modul, das 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.

Key Benefits:

- 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 sechsstelliger 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:

Netzwerkkonfiguration: 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)
- Anrufbenachrichtigungen 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 v**erzögert 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 Netzwerkkabel
- 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. 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 elektrischen und 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
- Netzwerkkabel (Cat 5e oder höher, wenn Ethernet verwendet wird)
- 8-Pin Phoenix-Steckverbinder für den Netzwerkkabelanschluss (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 Anruffunktionen
- 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 Netzwerkkabel 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**
- Technischen Support über **autorisierte Partner** oder das nächstgelegene **frogblue CompetenzCenter**
- Online-Fehlerbehebung und FAQs

# 2. Vor-Installationsanforderungen

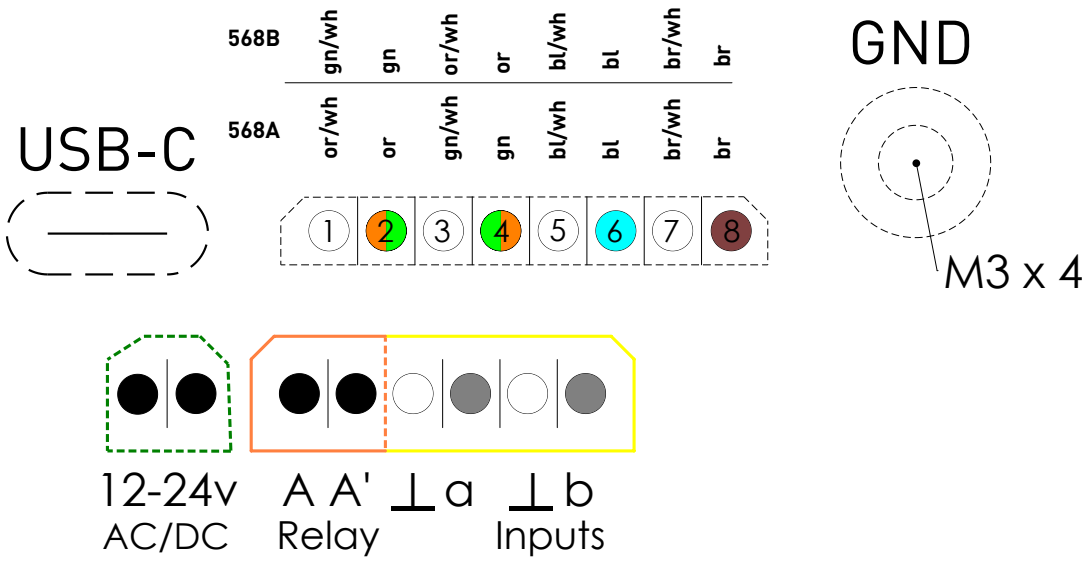
## 2.1. Standortanforderungen

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.
- **Netzwerkkonnektivität**: 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:

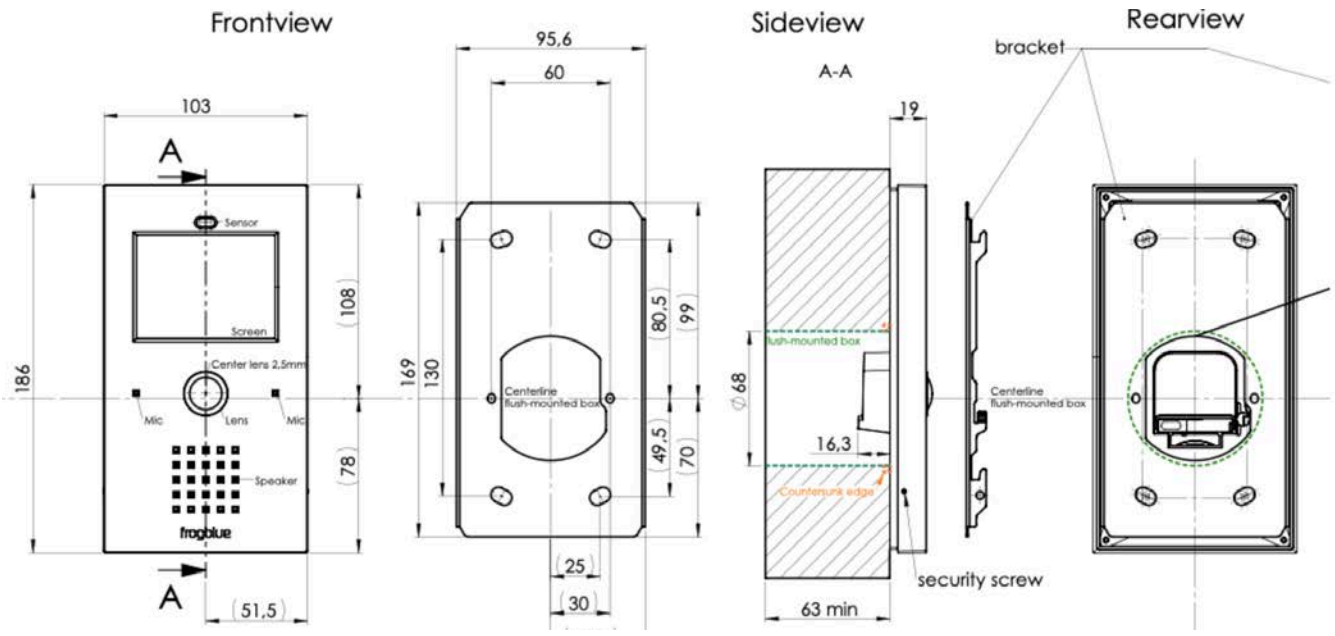



- Stromoptionen:
  - Power over Ethernet (PoE 802.3af, Class 3) über 8-Pin-Steckverbinder (PTSM 0.5/8-P-2.5)
  - 12V–24V DC externe Stromversorgung über 2-Pin-Steckverbinder (PTSM 0.5/2-P-2.5)
  - 24V AC Stromquelle über 2-Pin-Steckverbinder (PTSM 0.5/2-P-2.5)
  - Standby-Verbrauch beträgt ca. 5W
- Netzwerkoptionen:
  - 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 Kontakte (Eigenversorgung 2 V / max. 1mA) – Niederspannungskontakte (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.
- Anschlusstipps:
  - 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 Ø 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 → Support → Software)
- Montagehalterung und Schrauben (im Lieferumfang enthalten)
- Stromquelle (PoE-Injector, DC-Netzadapter oder AC-Stromanschluss)
- Netzwerkkabel (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 frogTerminalALU. Folgende Artikel sind im Lieferumfang enthalten:

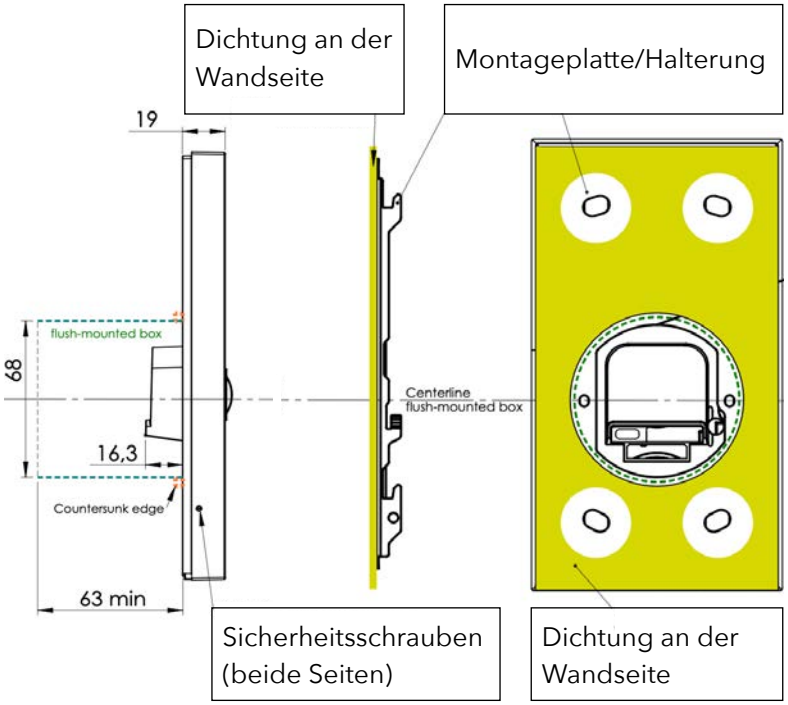
- Paketbeilage-Aufkleber mit Seriennummer, Barcode, Versionsinformation
- frogTerminal, Aluminium-Montageplatte mit angebrachtem Dichtungseinsatz
- 4 × Schrauben (Ø4,5 × 40 mm)
- 4 x Isolationsbefestigungen – Kunststoff-Spreizdübel
- 4 × Dübel (UX6)
- 1,5 mm Inbusschlüssel (für die Verriegelung der Seitenschrauben)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

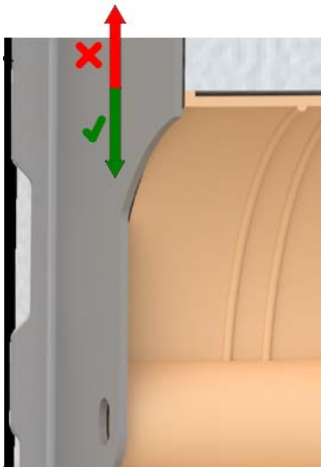
# 3. Physischer Installationsprozess

## 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.



**Wichtig:** Der Rand der Halterung darf nicht höher sein als die Dose! Die Kante der Unterputzdose sollte bündig mit der Wand abschließen.

### 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 frogTerminalALU.

- Bereiten Sie eine Aussparung mit einer Mindesttiefe 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 (größere 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.
- Anschlusstipps:
- 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

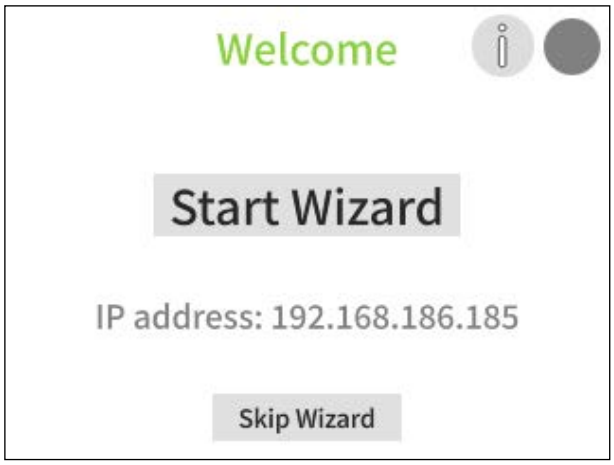
Der On-Device-Assistent vereinfacht die initiale Konfiguration des frogTerminals, indem er Sie schrittweise durch die wesentlichen Einstellungen führt. Dieser Abschnitt sorgt für ein reibungsloses Installationserlebnis, selbst für Benutzer mit geringen technischen Kenntnissen.

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".**

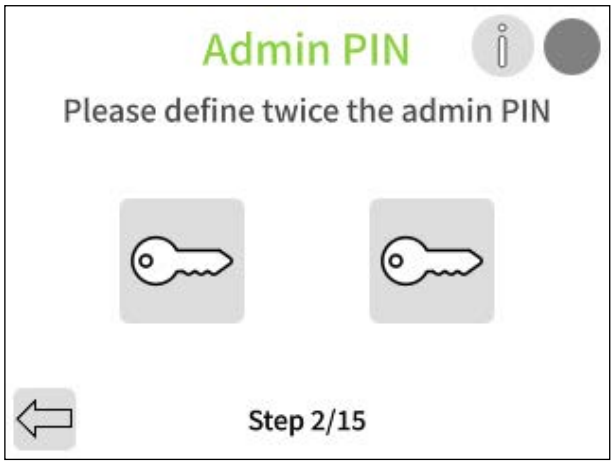



- Tippen Sie auf „Start Wizard".

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

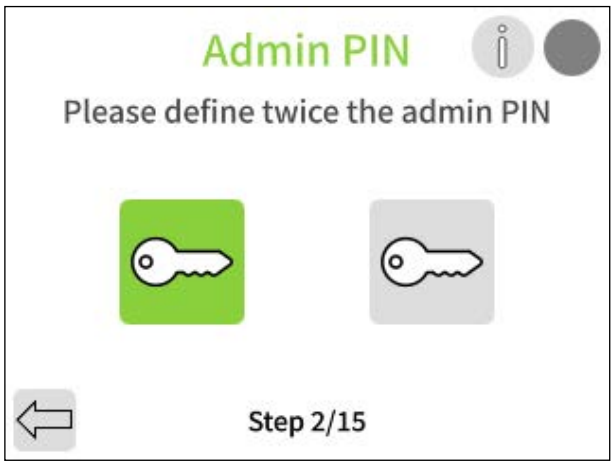

- Tippen Sie auf die Dropdown-Menüs, um Ihre bevorzugte Sprache und Zeitzone auszuwählen.
- Tippen Sie auf den „Weiter"-Pfeil ⇨.

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



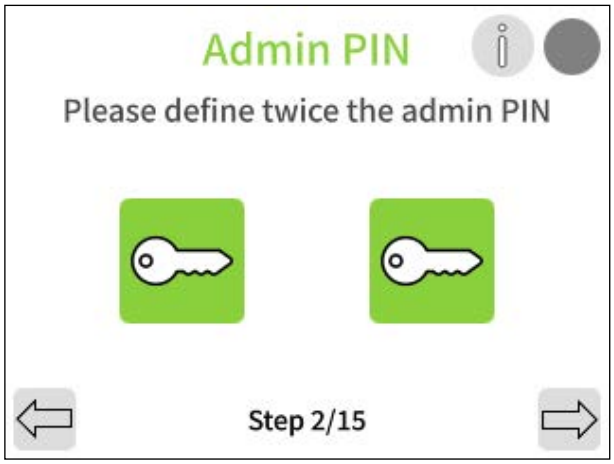

- Tippen Sie auf das erste Schlüssel-Symbol.


- 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 den „Weiter“-Pfeil ⇨.

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


- Tippen Sie auf das hellgraue „Password“-Texteingabefeld (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.

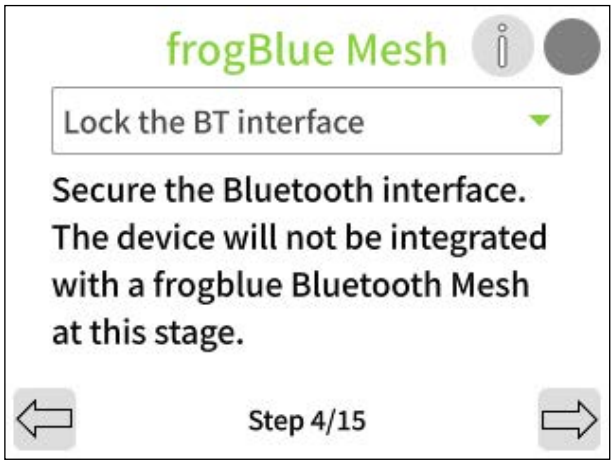

- Tippen Sie auf den „Weiter“-Pfeil ⇨.

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

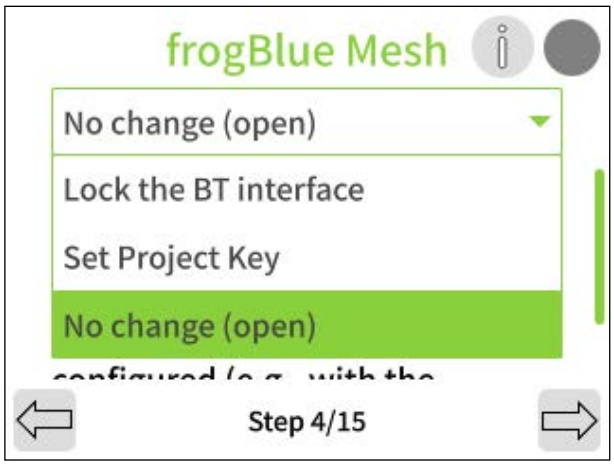
Die werkseitigen Standard-Login-Daten für den Zugriff auf die Kamera via Webbrowser lauten:

- 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 den „Weiter“-Pfeil oder geben Sie den "Project Key" ein und tippen Sie auf den „Weiter“-Pfeil ⇨.

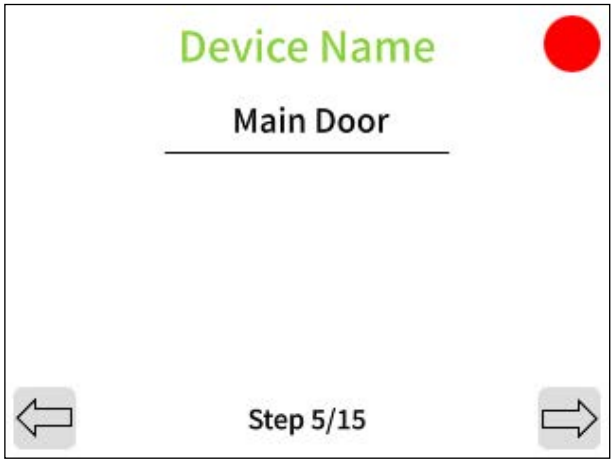
**Sperren Sie die BT-Schnittstelle**: Das frogblue Mesh ist gesperrt und muss durch einen Factory Reset freigeschaltet werden (siehe Abschnitt 20.2 „Systemsteuerung – Konfigurationsdateien, Neustart und Werkseinstellungen“).

**„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 den „Weiter“-Pfeil ⇨ .

### 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.

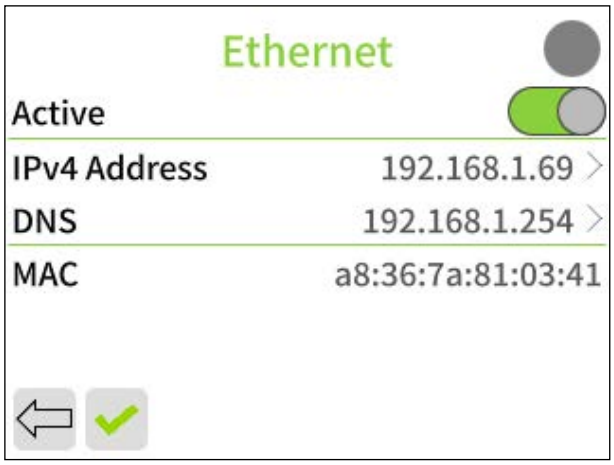
**Hinweis**: Derzeit in Entwicklung – ein Software-Update befindet sich in Arbeit, durch das der Startbildschirm Optionen zur Anpassung von Bildern, Logos, Stilen, Suchfunktionen und scrollbaren Anruflisten enthalten wird.


- 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 den „Weiter“-Pfeil ⇨, um fortzufahren.

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

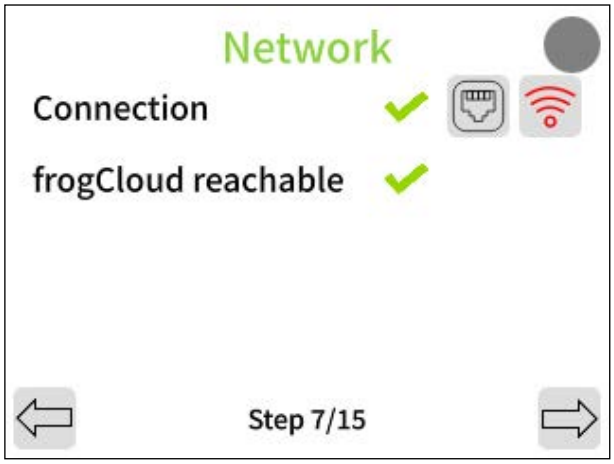

- Tippen Sie auf die Symbole für Ethernet und WLAN, um die Einstellungen für die jeweilige Schnittstelle zu konfigurieren.

**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 das Symbol „Zurück“ 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 den „Weiter"-Pfeil, um fortzufahren.

**Hinweis**: Sollten Verbindungsprobleme auftreten, siehe Abschnitt „17.1.5 Fehlersuche bei Netzwerkverbindungsproblemen“.

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

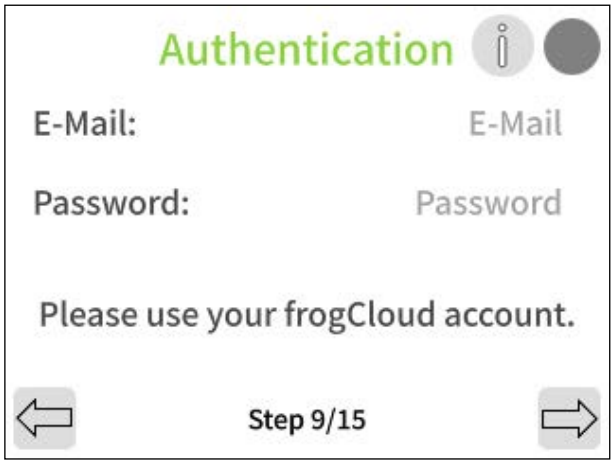
Für eine schnelle und einfache Verbindung mit einem smarten Gerät wird ein frogCloud-Konto empfohlen.


- 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.

### 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 den "Weiter"-Pfeil ⇨, um fortzufahren.

Registrierung für ein neues frogCloud-Konto:

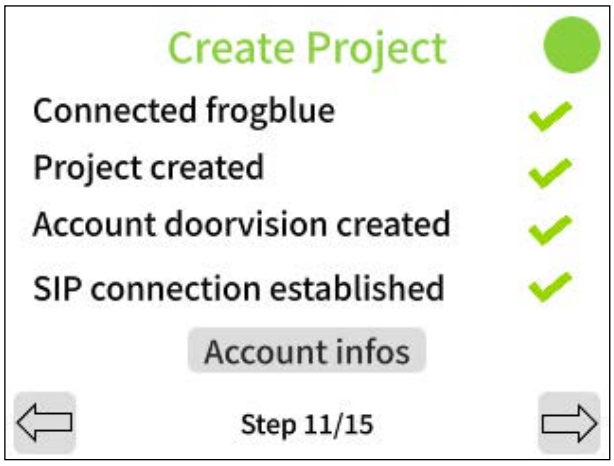

- Tippen Sie in die Texteingabefelder „E-Mail" und „Password".
- Geben Sie mit der Bildschirmtastatur Ihre E-Mail-Adresse und ein von Ihnen gewähltes Passwort für Ihr frogCloud-Konto ein.
- Tippen Sie auf den "Weiter"-Pfeil ⇨, um fortzufahren.

### 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.

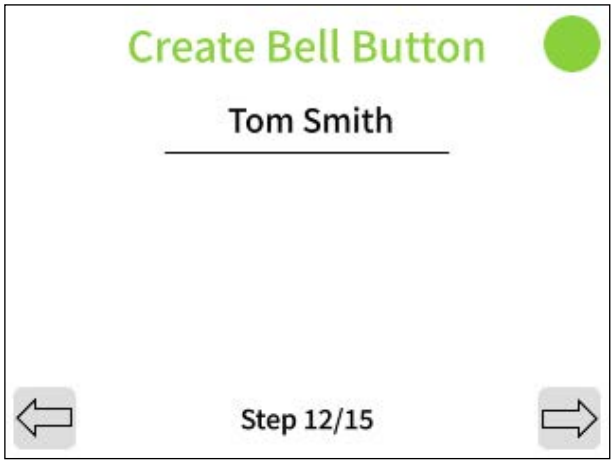

- Warten Sie auf die Bestätigungsmeldung, dass eine E-Mail an Ihre Adresse gesendet wurde.
- Überprüfen Sie Ihre E-Mails, klicken Sie auf den Link und loggen Sie sich dann mit Ihrem Benutzernamen und Passwort ein, um Ihr neues frogCloud-Konto zu aktivieren.
- Tippen Sie auf den „Weiter"-Pfeil ⇨ , um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

### 4.14. Startansicht und Erklärungen der Anzeigemodi

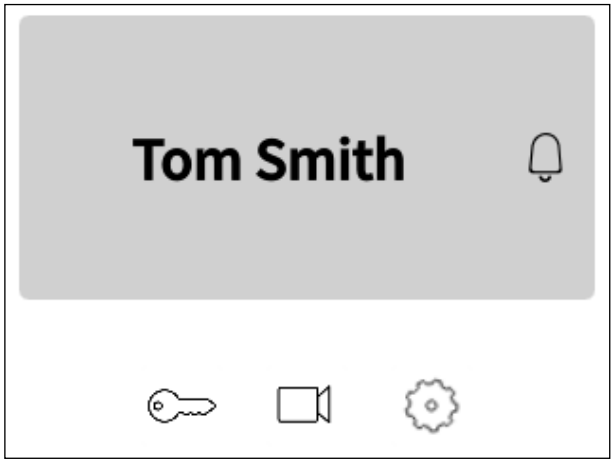
Die Startansicht erscheint, wenn das Terminal durch Annäherungserkennung oder Berührung aktiviert wird. Ansichten bestehen aus einem Hauptbereich und einer Symbolleiste. Das System unterstützt vier Anzeigemodi, wobei die Symbolleiste über den Webbrowser weiter angepasst werden kann.

**Symbolleisten-Tasten:**

- Ermöglicht die Eingabe von Funktions-PINs
- Öffnet den Kamera-Dialog. (Siehe Kapitel 8 „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.

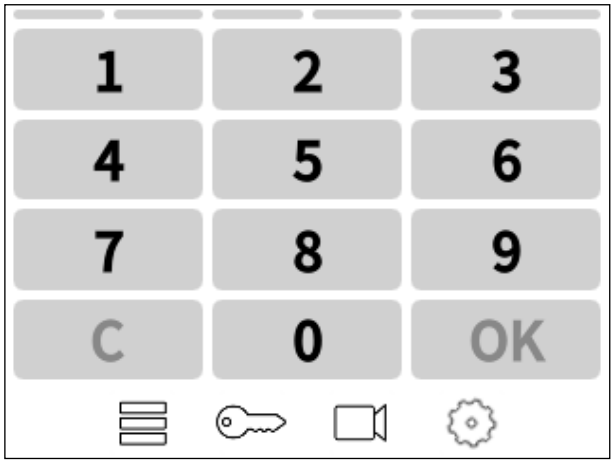
**Anzeigemodus 1: Klingeltasten („Bell Buttons“)**

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



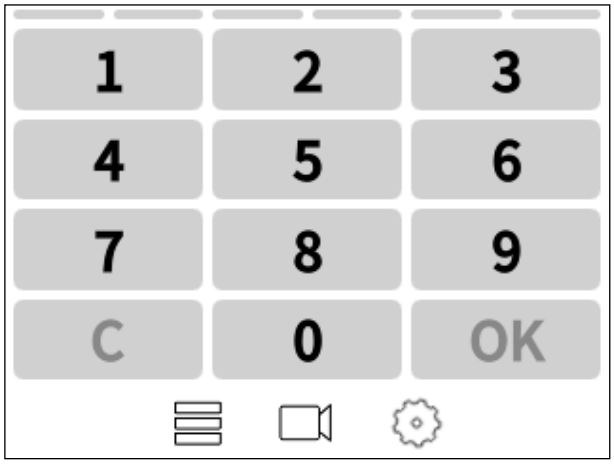
### Anzeigemodus 2: App + PINs

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



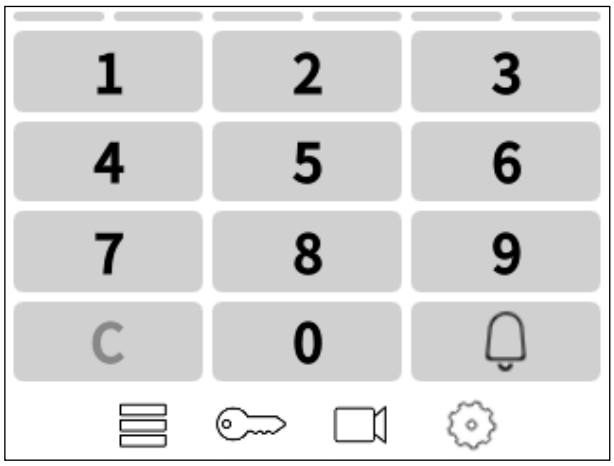

### Anzeigemodus 3: PINs

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

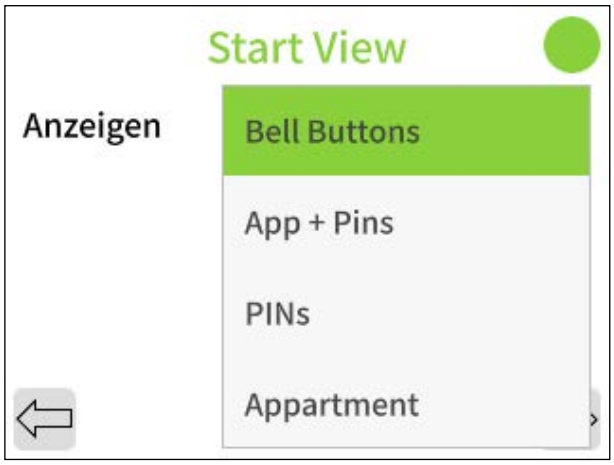



### Anzeigemodus 4: Apartment

Diese Ansicht ermöglicht die Eingabe von Wohnungs-/Einheitsnummern im Hauptbereich und zeigt 4 Symbolleisten-Schaltflächen an.



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

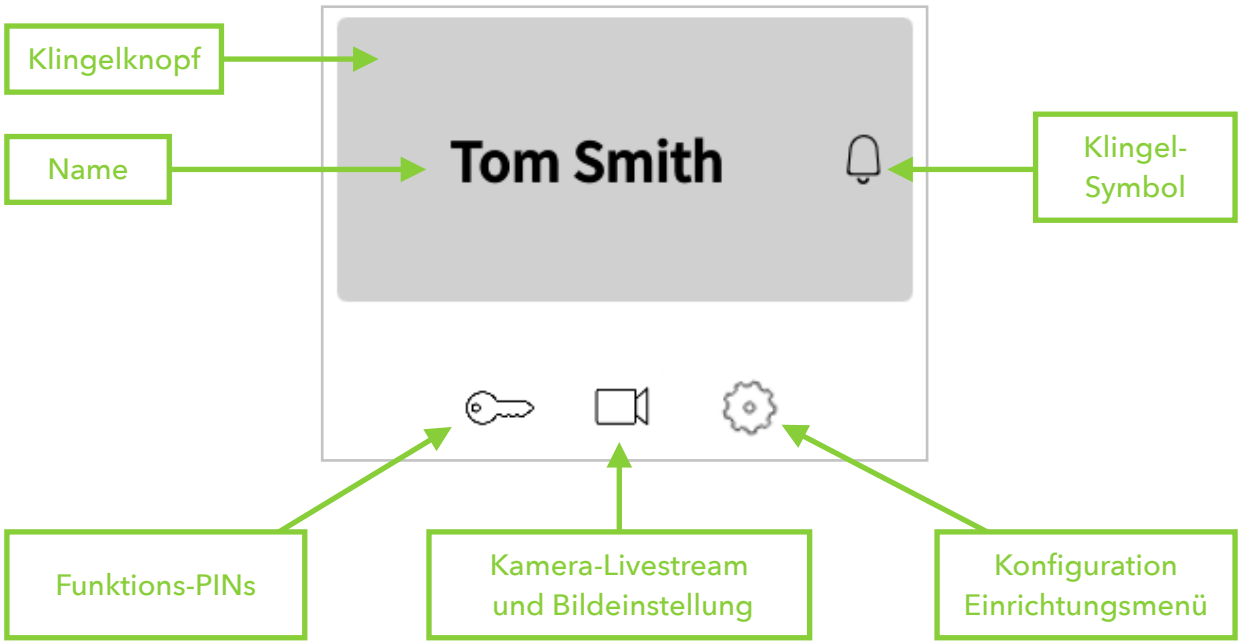



- Wählen Sie Ihre gewünschte Startansicht.
- Tippen Sie auf den "Weiter"-Pfeil ⇨, um fortzufahren.

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


- Fertig! Der Begrüßungsbildschirm erscheint und bestätigt den Abschluss des Assistenten.
- Tippen Sie auf den "Weiter"-Pfeil ⇨, 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.

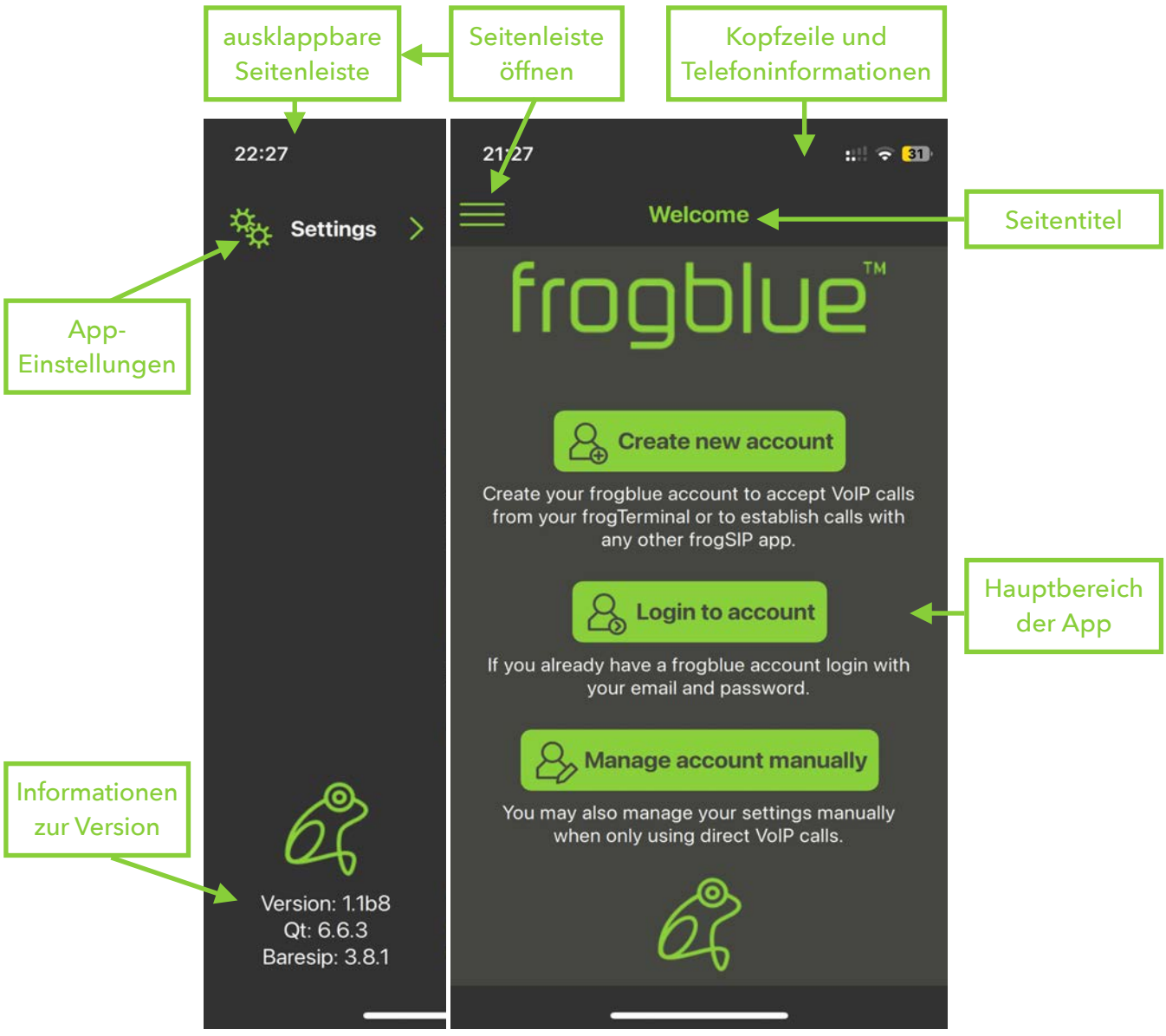
# 5. frogSIP App Benutzeroberfläche

## 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 Anrufhistorie.

## 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.

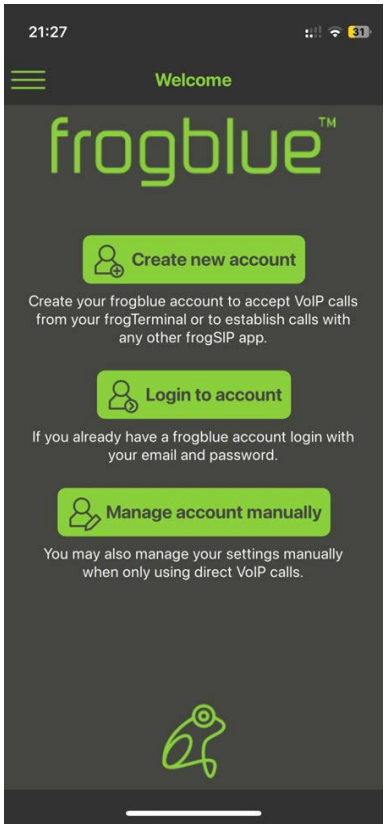



**Hinweis**: Zu Beginn werden wir die **Erstellung und Anmeldung von frogCloud-Konten** behandeln. **„Manage account manually"** wird für kundenspezifische SIP-Integrationen verwendet und in einem späteren Abschnitt behandelt.

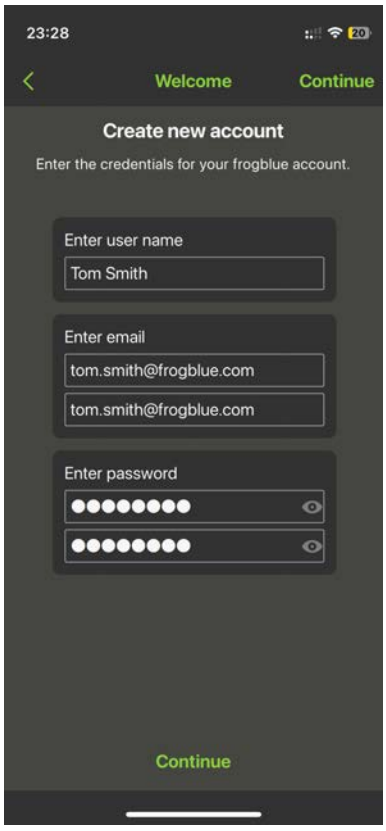
## 5.3. Neues frogCloud-Benutzerkonto über die frogSIP App erstellen

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**".

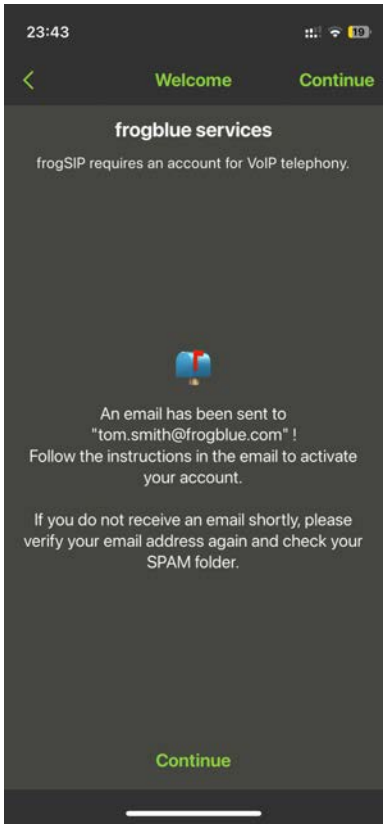



- Tippen Sie auf „**Create new account**"




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**“

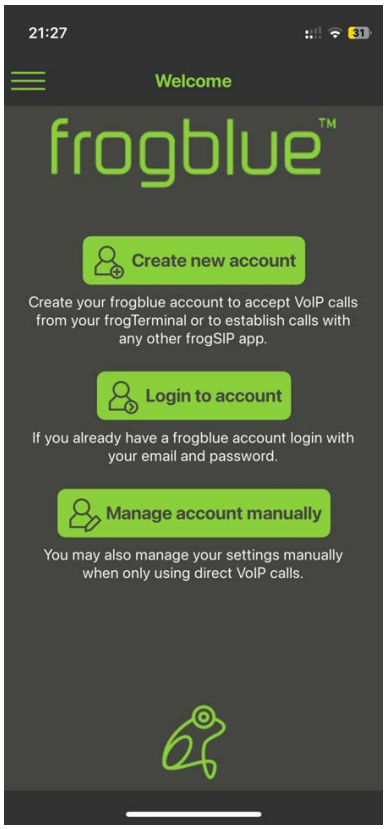

- Warten Sie auf die folgende Meldung, die bestätigt, dass Ihr neues Konto **aktiviert** ist.
- Tippen Sie auf „**Continue**“

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

1. Ihr **frogTerminal** auf die **neueste frogOS-Version aktualisiert** wurde, erhältlich unter frogblue.com.
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“**

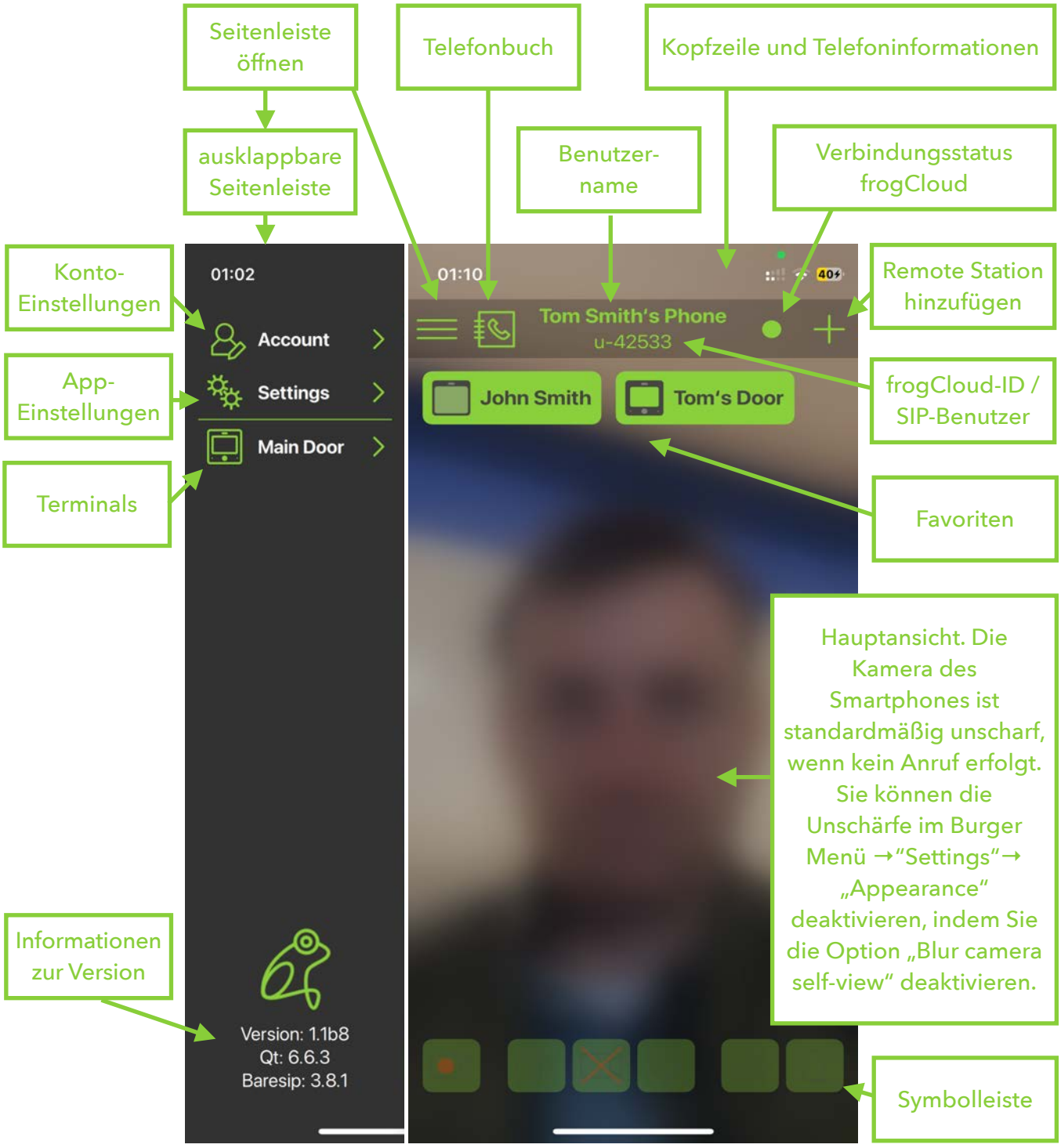

- Warten Sie auf die folgende Meldung, die bestätigt, dass Ihr Konto **aktiviert** wurde.
- Tippen Sie auf „**Continue**“

## 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:**

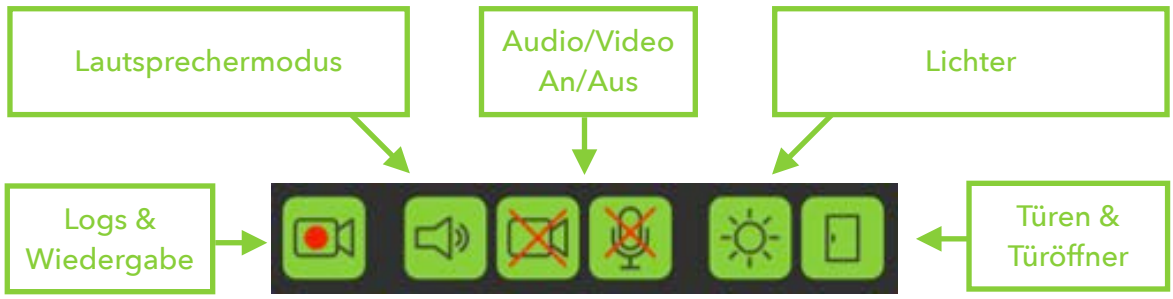
  ⚫ Undefined (undefiniert)

  🔴 No connection (keine Verbindung)

  🟢 Connected (verbunden)

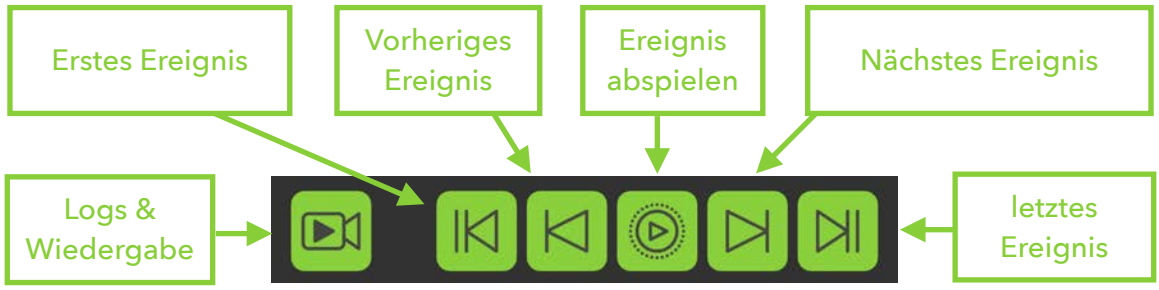
  Der Verbindungsstatus-Indikator zeigt die Verbindung zwischen der App und der frogCloud an. Ein grünes Licht bedeutet, dass die Verbindung aktiv ist, Rot weist auf eine fehlende Verbindung hin, und Grau zeigt an, dass die App nicht korrekt konfiguriert ist.
- **Remote Station oder Benutzer hinzufügen**: 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 → Darstellung und schalten Sie „Kamera-Selbstansicht unscharf" 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.
- **Lichter**: Steuern Sie das „Licht"-HomeObject des Terminals.
- **Türen & Türöffner**: Steuern Sie die Türöffner des Terminals oder von Relais (frogEntry).

### 5.5.2. Logs & Wiedergabe Symbolleiste

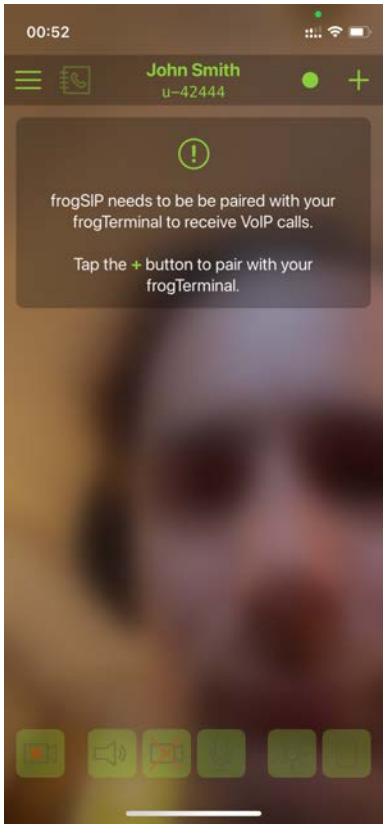



- **Logs & Wiedergabe**: Wechselt zwischen der Research-Player-Ansicht – verwendet für die Wiedergabe von Videoaufnahmen und die Überprüfung von Zutritts- oder Ereignisprotokollen – und der Live-Anruf-Ansicht.
- **Erstes Ereignis**: Springt zum frühesten aufgezeichneten Ereignis im System.
- **Ereignis 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.

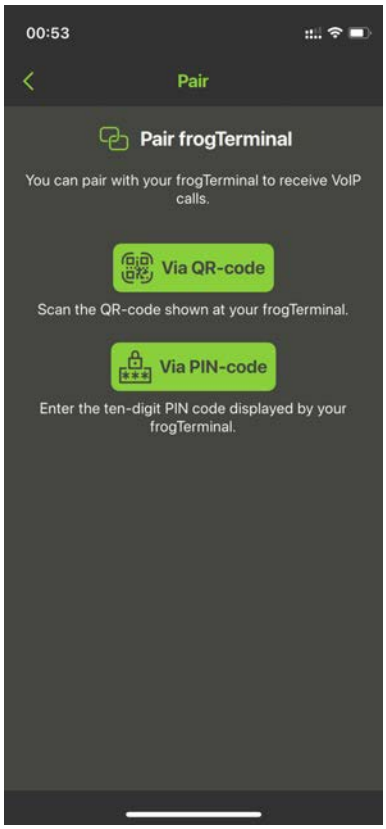

- Tippen Sie oben rechts auf das +-Symbol „**Add remote stations**“.


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.

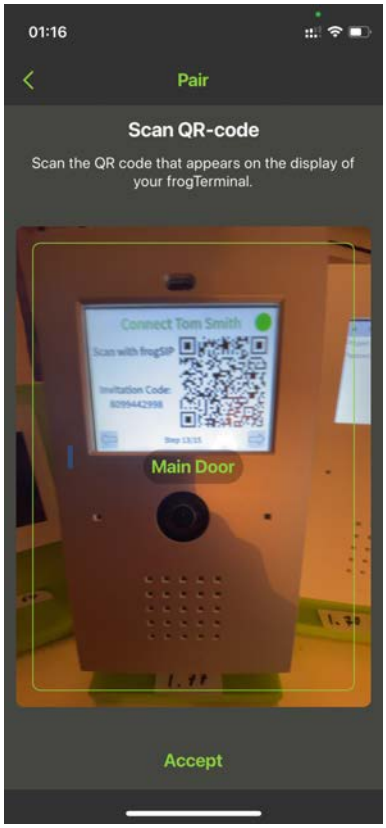
Benutzer können entweder über einen einfachen QR-Code oder über einen Einladungs-PIN-Code verbunden werden.

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




Das Terminal kann auf zwei bequeme Arten gekoppelt werden:

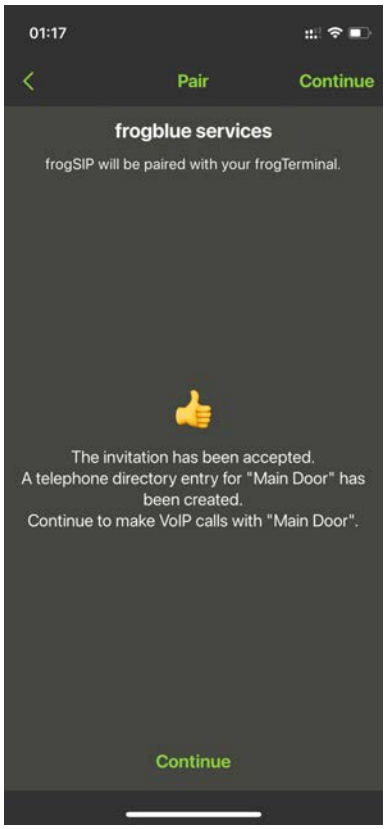
- „**Via QR-Code“**: Ideal für eine schnelle und einfache Kopplung, wenn sich das Smartphone, auf dem frogSIP läuft, während der Wizard-Einrichtung am selben Ort wie das Terminal befindet. .
- „**Via PIN-Code“**: Perfekt, wenn sich das Smartphone an einem anderen Ort befindet. Senden Sie einfach den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




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.
2. Ihre **frogSIP-App** wurde ebenfalls auf die neueste Version **aktualisiert**.

## 5.7. Anrufen, Wiedergabe und Verwaltung des frogTerminals mit frogSIP

Dieser Abschnitt beschreibt, wie Sie frogSIP mit Ihrem frogTerminal verwenden. Er behandelt das Initiieren von Anrufen, den Zugriff auf und die Überprüfung von Aufnahmen sowie die Verwaltung von Geräteeinstellungen.

### 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 7, „Telephony Call Destination Einrichtung". 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

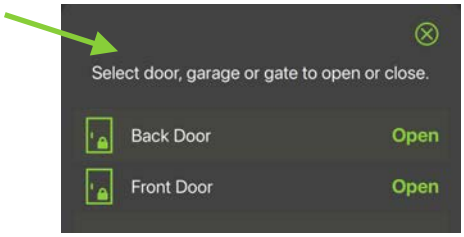
Damit das frogTerminal automatisch Anrufe von autorisierten Benutzern annimmt, stellen Sie sicher, dass das automatische Annehmen für Benutzer unter Web → Einstellungen → Allgemein auf „Automatische Anrufannahme" eingestellt ist. Zusätzlich können Benutzer auf reine Audio- oder volle Audio-/Video-Zugriffe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

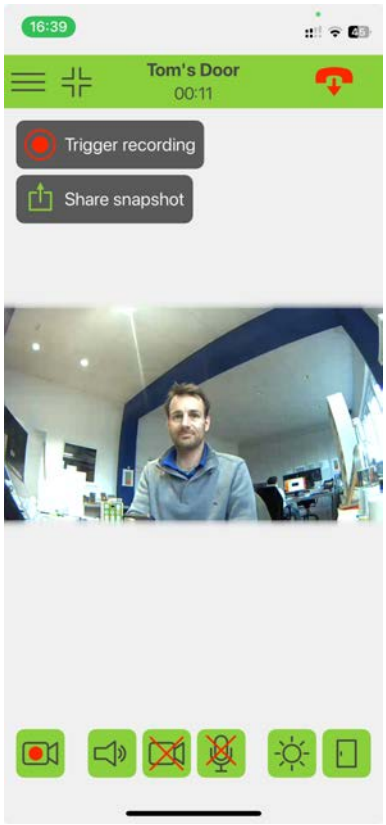
### 5.7.3. Anrufe initiieren


- 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.


- Blenden Sie die Symbolleiste aus, um mehr Platz für den Videoanruf zu schaffen.
- Lösen Sie eine manuelle Aufnahme während des Anrufs aus.
- Beenden Sie den Anruf.
- Öffnen Sie das Quick-Menü, um ein Bild aufzunehmen oder eine Aufnahme während eines Anrufs zu starten.
- Schalten Sie das Licht ein und aus.
- Öffnen Sie die Tür – wenn mehrere Türen konfiguriert sind, erscheint ein weiteres Dialogfeld, das es Ihnen ermöglicht, die Türzustände einzusehen und auszuwählen, welche Tür geöffnet werden soll.

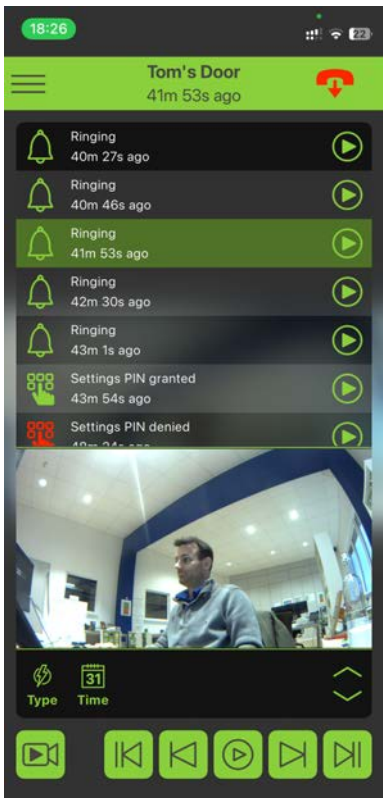



Um ein Bild aufzunehmen oder eine Aufnahme während eines Anrufs auszulösen, tippen Sie , um die folgenden Optionen zu sehen.

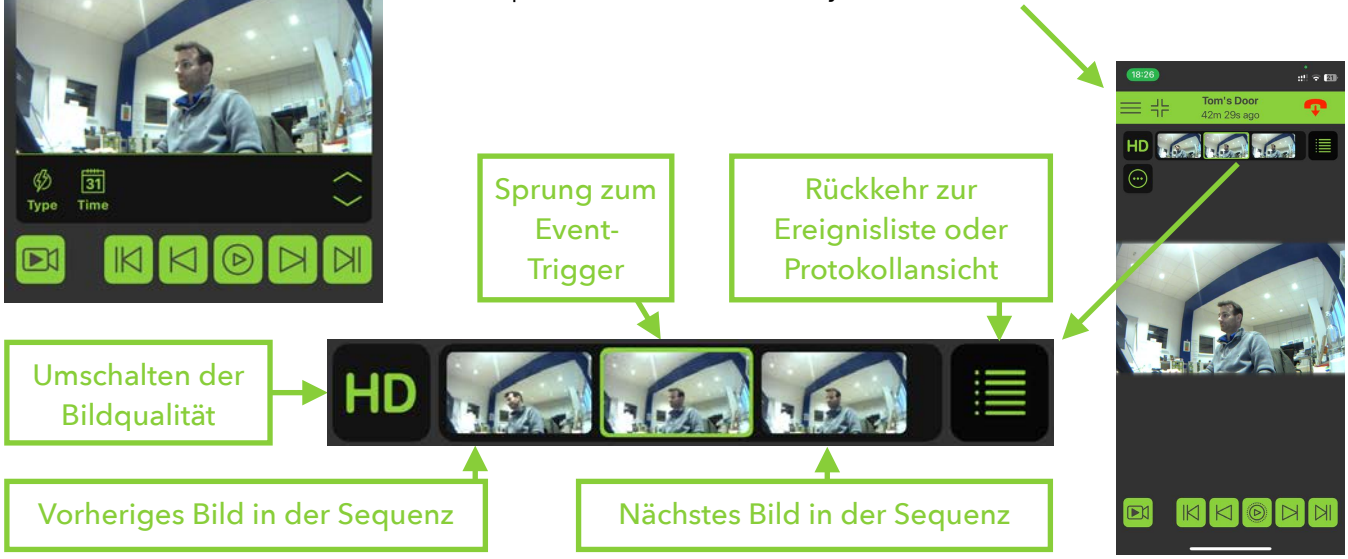
- „**Trigger recording**“: Löst eine Aufnahme über das Benutzerklick-Ereignis im frogTerminal aus. Startet manuell die Aufnahme eines Ereignisses. Gehen Sie zu „**Settings**“ → „**Recording**“, um die Aufnahmeeinstellungen zu prüfen und zu ändern.
- „**Share snapshot**“: Nehmen Sie ein aktuelles Standbild 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.



# 6. Zutrittskontrollkonfiguration

## 6.1. 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.

## 6.2. 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).

## 6.3. Grafisches Feedback für Zutrittsereignisse


- Ein erfolgreiches Zutrittsereignis


- Ein verweigertes Zutrittsereignis


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

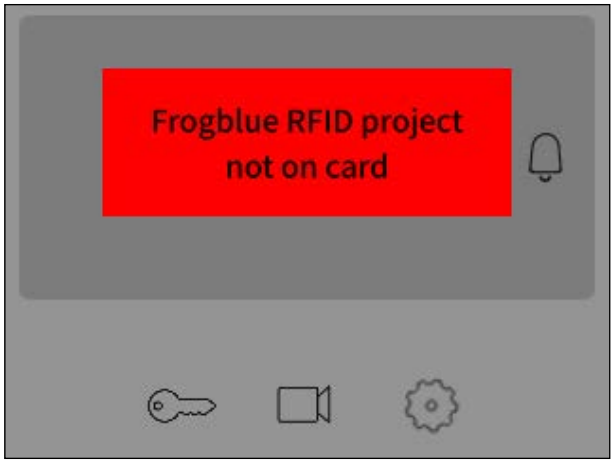

- Ein verweigertes Zutrittsereignis.
- Grund: Zeitplan-Ausnahme. Karte ist zu diesem Zeitpunkt nicht erlaubt.


- 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

## 6.4. 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.

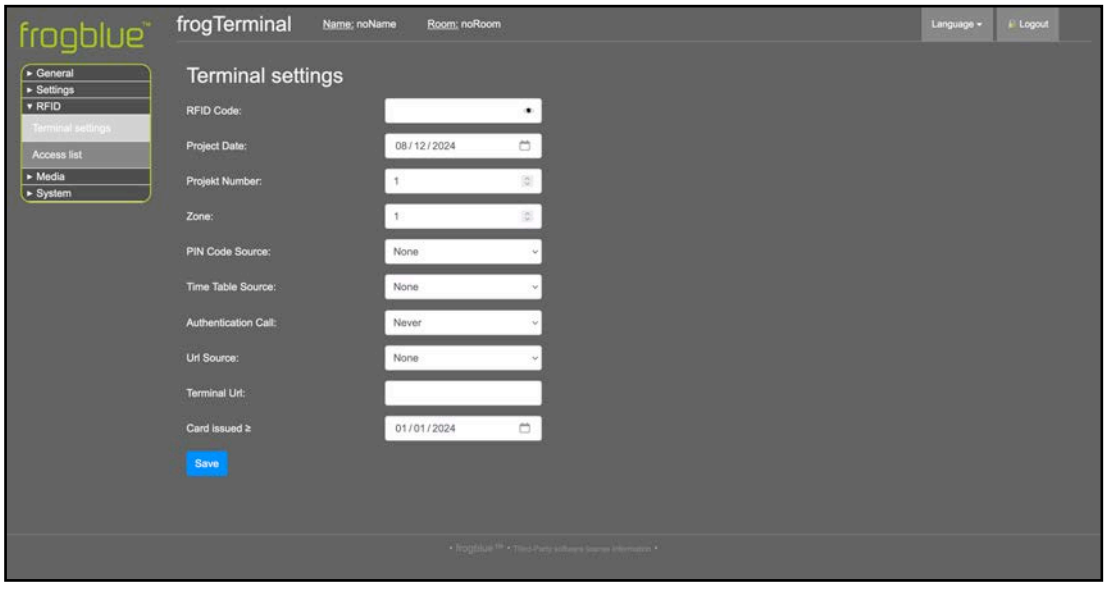
Zukünftige Erweiterungen: Anstehende Updates werden die Möglichkeit einführen, Benutzerdaten über das Netzwerk oder lokal via Bluetooth zu verwalten. Zusätzlich ist ein cloudbasiertes Zutrittsmanagementsystem mit Zeiterfassung geplant.

## 6.5. 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.



### 6.6. 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**).

### 6.7. 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.

### 6.8. RFID-Verschlüsselung und Zonen

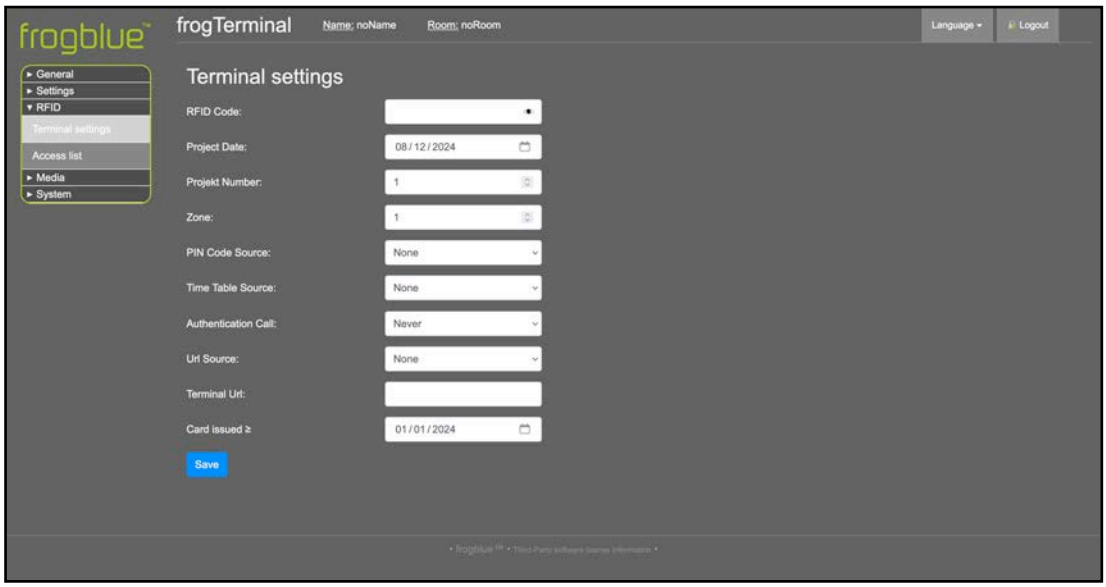
Richten Sie Zutrittskontrollparameter wie RFID-Verschlüsselung, Zonen und Projekteinstellungen ein.

**Schrittübersicht**:

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

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

**Menü: „Access Control“ → „Terminal Settings“**




- **„RFID Code“**: 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 Code, Datum und derselben Projektnummer in Betrieb genommen wurden, arbeiten als ein einheitliches System.
- **„Project Date“**: Der Zeitstempel, der als Sicherheits-Seed dient, typischerweise eingestellt auf das letzte Datum, an dem dieses Projekt in Betrieb genommen wurde.
- **„Project Number“**: 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 Source“**: Bestimmt die Quelle der gespeicherten PIN-Codes für die Zwei-Faktor-Authentifizierung, drei 3 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 der Terminal-Option erscheint ein zusätzliches Eingabefeld, in dem Sie eine sechsstellige PIN für den Zutritt an diesem Terminal festlegen können.*
- **„Time Table Source“**: Gibt an, aus welcher Quelle zeitbasierte Zutrittsregeln stammen, mit 3 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**: 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 6.9 „Hinzufügen und Sperren von Karten" zur Konfiguration von Zeitplänen.*

- **„Authentication Call"**:

  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. **Never**: Deaktiviert Authentifizierungsanrufe für alle Zutrittsereignisse an diesem Terminal.
  2. **Card Value**: Die Anrufeinstellungen (ob und wer angerufen wird) werden auf der Zutrittskarte definiert und gespeichert, was individualisierte Konfigurationen für Benutzer ermöglicht.
  3. **Only Exeption**: Anrufe werden nur in Ausnahmefällen getätigt, beispielsweise bei Zugriffsversuchen außerhalb der festgelegten Zeitpläne oder nach falschen PIN-Eingaben.
  4. **Always**: Bei jedem Zutrittsereignis wird ein Authentifizierungsanruf getätigt, unabhängig von Zeitplänen oder PIN-Korrektheit, um maximale Überwachung zu gewährleisten.

- **„URL Source"**: 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:

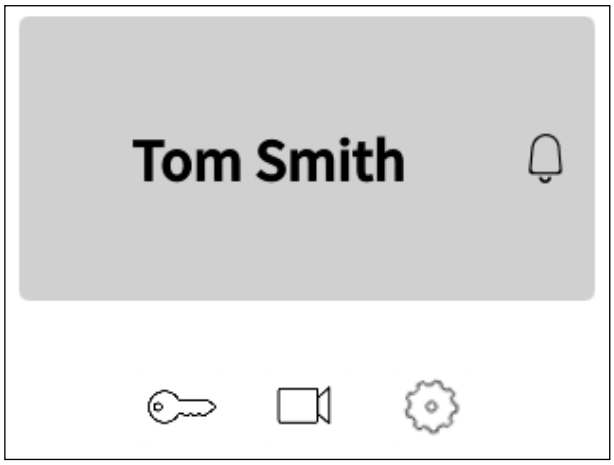
1. **None**: Deaktiviert das URL-Auslösen für Zutrittsereignisse an diesem Terminal.
2. **Card**: Die auszulösende URL wird auf der Zutrittskarte definiert und gespeichert, wodurch benutzerdefinierte Aktionen für einzelne Benutzer ermöglicht werden.
3. **Terminal**: Eine spezifische URL wird lokal am Terminal festgelegt und universell für alle Zutrittsereignisse an diesem Standort ausgelöst. Diese Einstellung eignet sich ideal für standardisierte Integrationen über mehrere Benutzer hinweg.

- **Terminal-URL**: Die URL, die ausgelöst wird, wenn die URL-Quelle als Terminal konfiguriert ist. Dadurch kann das Terminal standardisierte API-Aufrufe oder IP-Aktionen für alle Zutrittsereignisse initiieren.
- **Card Issued ≥**: 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.

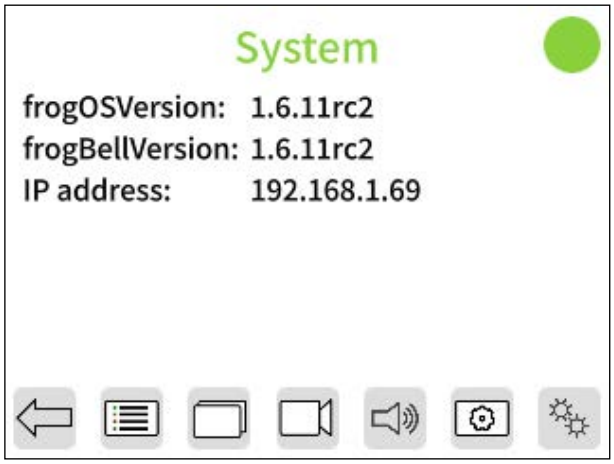
  Diese Einstellung stellt eine einfache Sicherheitsmaßnahme dar, falls es zu einem möglichen Sicherheitsverstoß (z. B. verlorene Zutrittsschlüssel) kommt – setzen Sie dieses Datum einfach auf den aktuellen Tag, alle älteren Karten werden sofort gesperrt, alle Personen müssen nun ihre Schlüssel zur Neuschreibung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

Button speichert die aktualisierten Zutrittseinstellungen am Terminal..

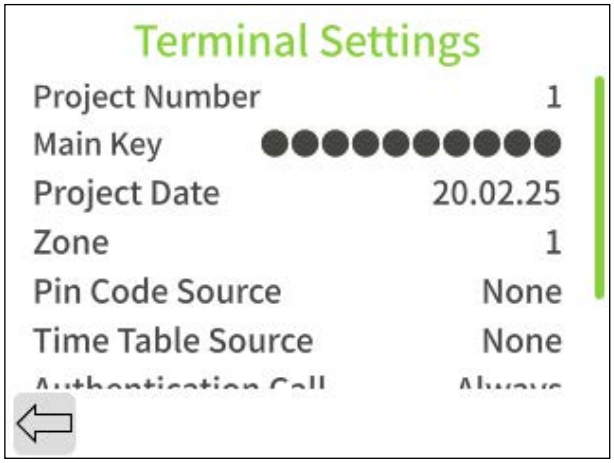
### 6.8.2. RFID-Verschlüsselung und Zonen über den On-Device-Touchscreen.




- Tippen Sie auf ⚙ und geben Sie Ihren 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 6.8.2 „RFID-Verschlüsselung und Zonen über den On-Device-Touchscreen“ beschrieben werden.

## 6.9. Hinzufügen und Sperren von Karten

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

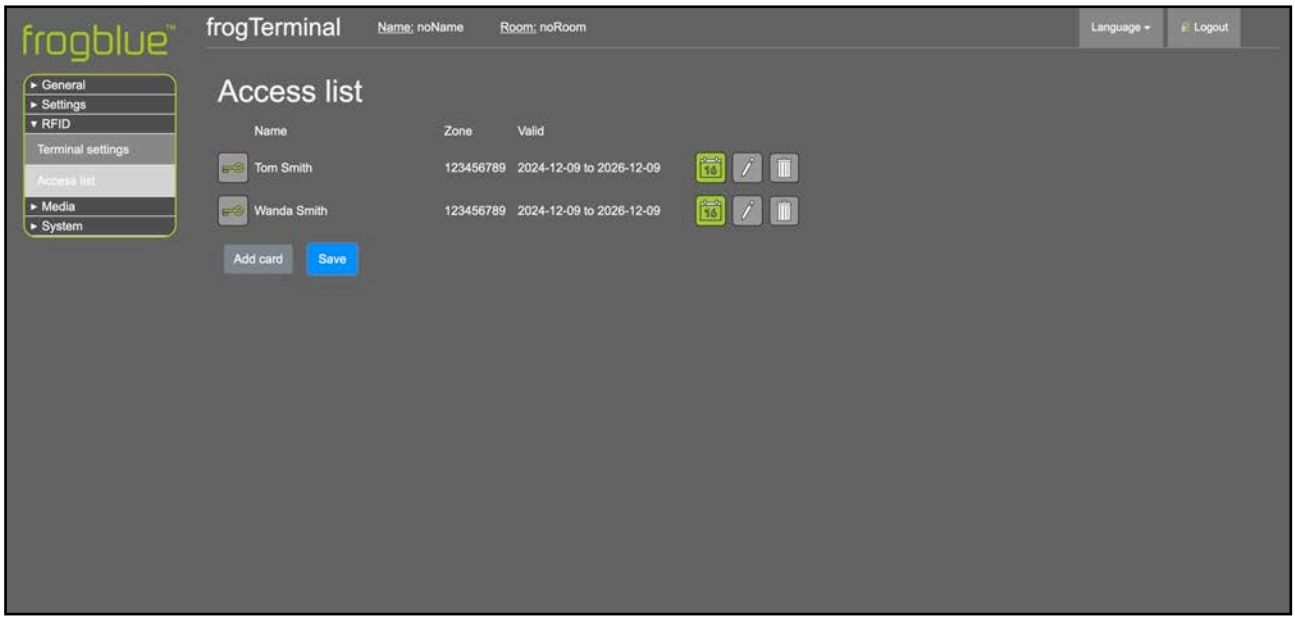
**Schrittübersicht**:

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

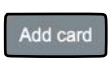
### 6.9.1. Hinzufügen und Sperren von Karten über den Webbrowser

**Menu: Access Control → Access Rules**

*Noch nicht vollständig funktionsfähig. Volle RFID-Konfiguration über den Webbrowser folgt in einem Software-Update.*



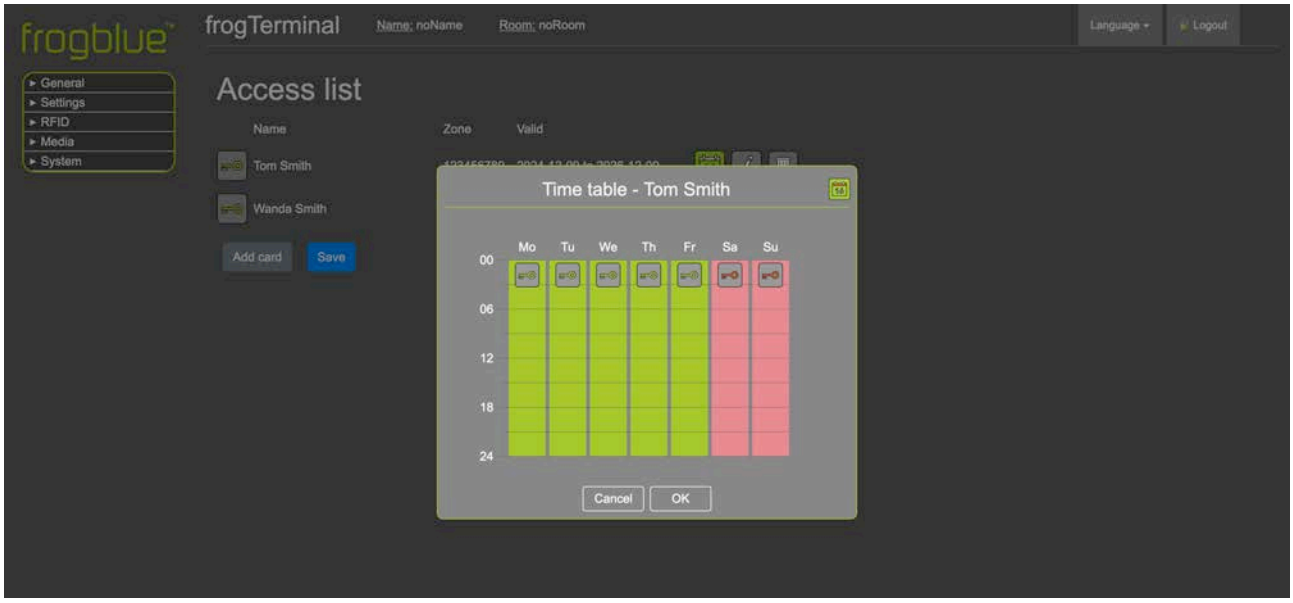

**Zutrittsliste**

- 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 „Time Table Setup“ in der nächsten Sektion.
- Der  Button öffnet die Karteneinstellungen zur Anpassung. Weitere Informationen finden Sie im Abschnitt „Edit Card Dialog“.
- 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.



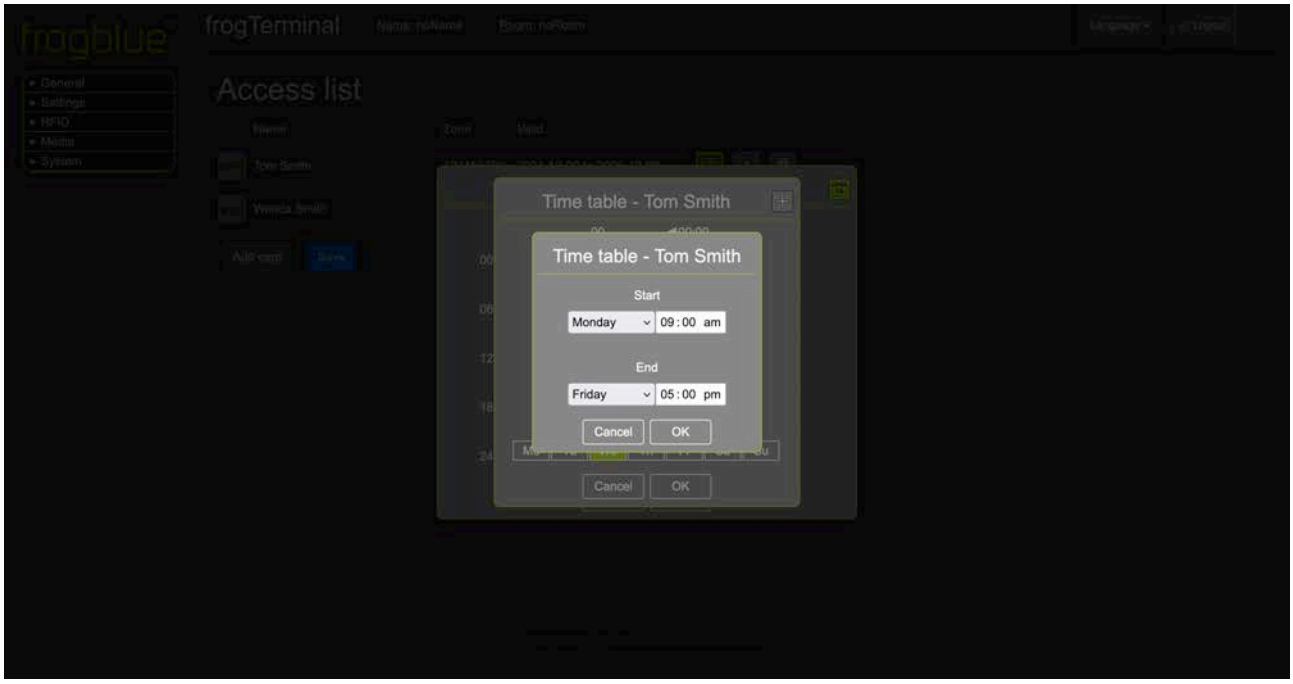

### Time Table Setup

- 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 So 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 „**Time Table Day Setup**“ für den ausgewählten Tag.
- Tagesteile können auch per Drag & Drop verschoben werden, um Zeiteinstellungen von einem Tag auf andere zu kopieren.


### Time Table Day Setup Dialog

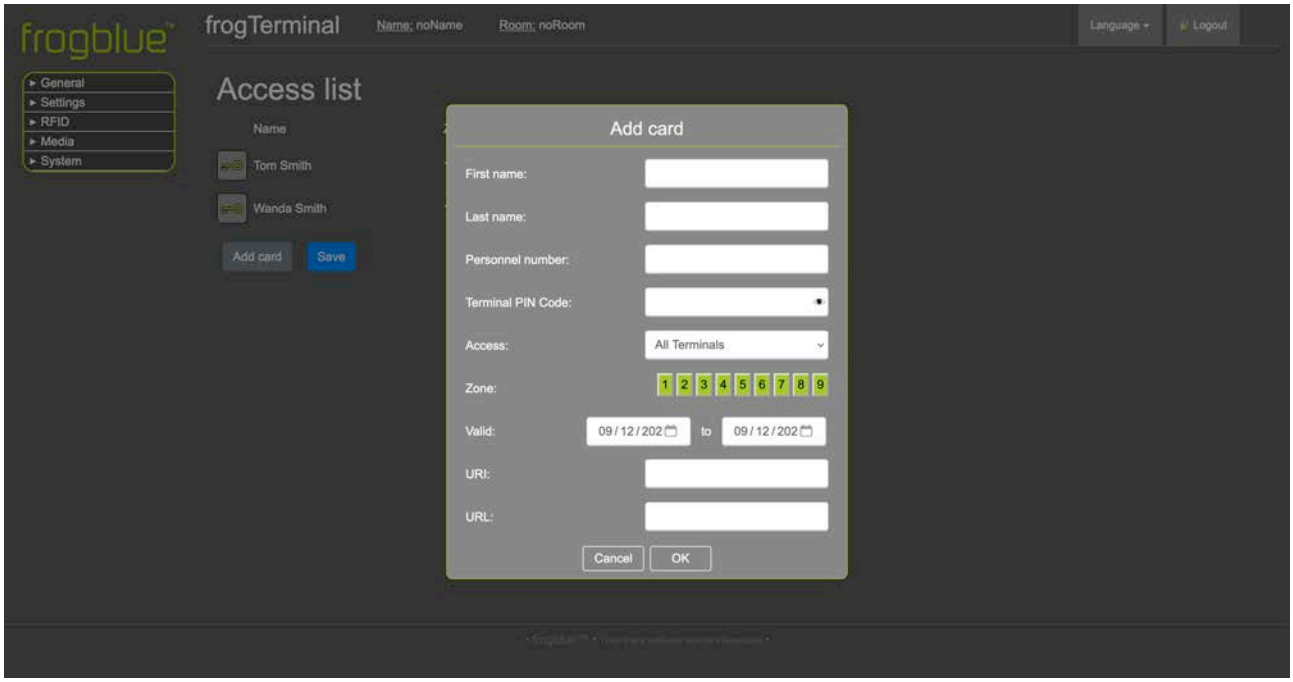
Der  Button schaltet den Zutritt für den entsprechenden Zeitraum um. Ein grünes Symbol zeigt an, dass der Zutritt erlaubt ist, Rot zeigt an, dass er verweigert wird.

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 Arbeitszeiten verweigert, aber von 9 bis 17 Uhr während der Arbeitszeit erlaubt wird.




### Time Table Day Dropdown Dialog

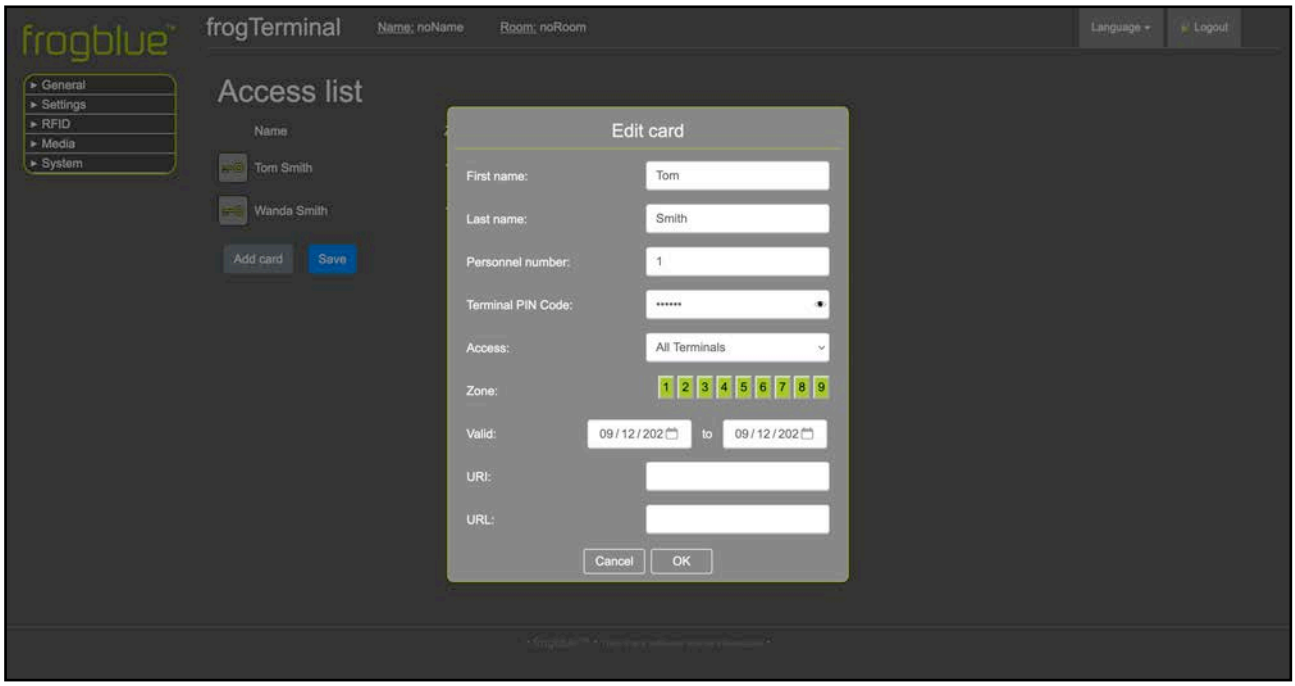
- In diesem Dialog können Sie benutzerdefinierte Zeiträume für Ihren Zeitplan konfigurieren, z. B. 9 bis 17 Uhr.
- Zeitabschnitte können auch mehrere Tage umfassen, wie z. B. Montag bis Freitag, 9 bis 17 Uhr, was Flexibilität für wiederkehrende Zeitpläne bietet.




### Add Card Dialog

- **„First name“**: Der Vorname der Person, die mit dieser Karte verknüpft ist.
- **„Last name“**: Der Nachname der Person, die mit dieser Karte verknüpft ist.
- **„Personnel number“**: Eine eindeutige Nummer oder Kennung für die Person, die mit dieser Karte verknüpft ist.

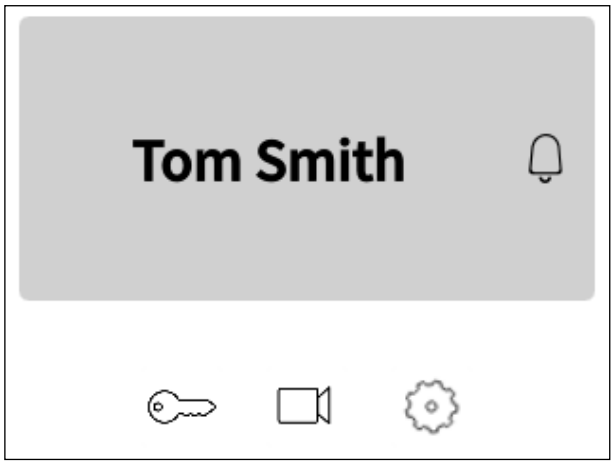
- „**Terminal PIN Code**“: Der eindeutige Zutritts-PIN-Code für die Person, die mit dieser Karte verknüpft ist. Dieser Code ist erforderlich, wenn bei den Terminaleinstellungen → „**PIN-Code-Source**“ „**Card**“ eingestellt ist.
- „**Access**“: Gibt an, ob dieser Eintrag nur für dieses Terminal oder 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 _ _ 9 Zutritt nur zu den Zonen 3, 6 und 9.
- „**Valid**“: Der Datumsbereich, in dem dieser Zutrittseintrag gültig ist.
- „**URI**“: Die URL, die im Ausnahmefall, wie z. B. bei einem Zutrittsverweigerungsereignis, ausgelöst wird.
- „**URL**“: Die URL, die bei erfolgreichem Zutritt ausgelöst wird.



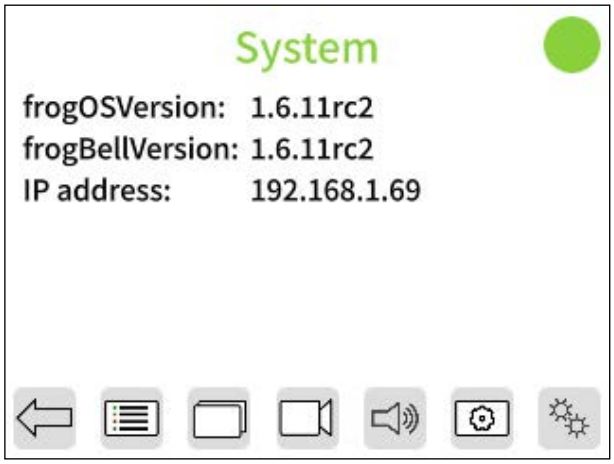

### Edit Card Dialog

Dieser Dialog spiegelt die Einstellungen des „**Add Card Dialog**“ wider, dient jedoch zur Bearbeitung der Konfiguration für den ausgewählten Eintrag.

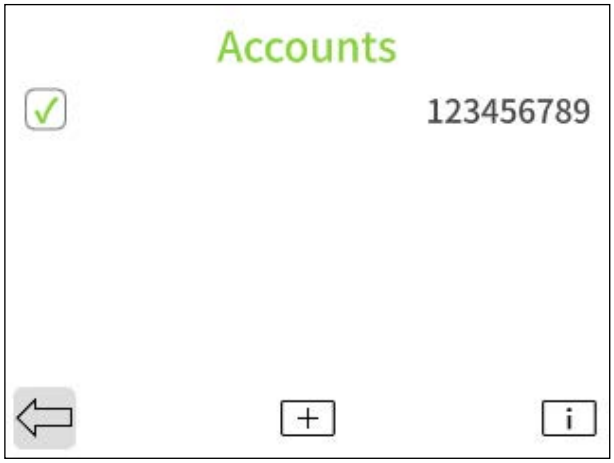
### 6.9.2. Hinzufügen und Sperren von Schlüsseln/Karten über den On-Device-Touchscreen




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

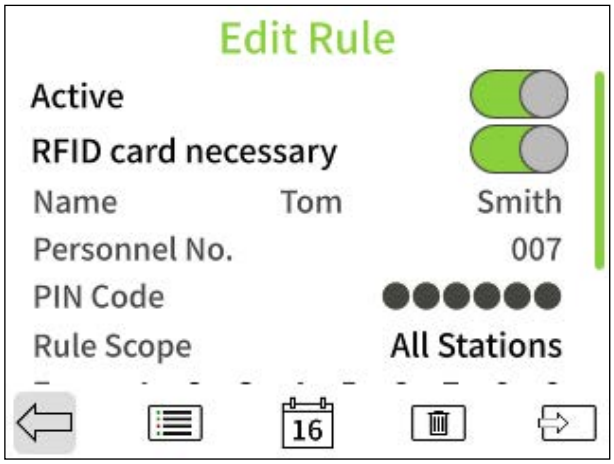



- Tippen Sie ▭, um auf die Zutrittsregel-Einstellungen zuzugreifen.

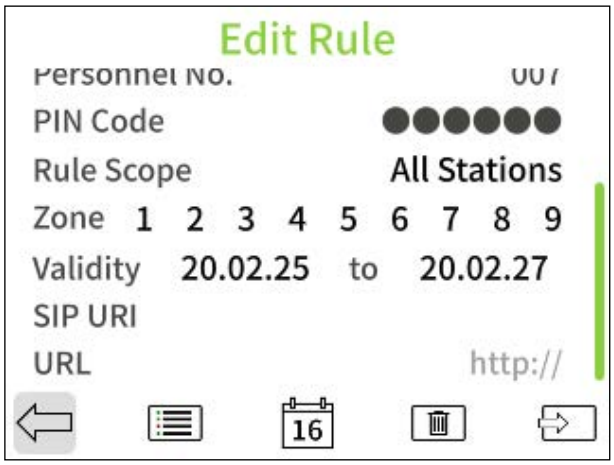



- Tippen Sie ⊞, um einen Zutrittseintrag hinzuzufügen.

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




- „**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.




- „**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.

### 6.9.3. Lesen & Formatieren von Schlüsseln/Karten

Wie Sie RFID-Karten oder Schlüsselanhänger für den Benutzerzutritt hinzufügen und bei Bedarf sperren.

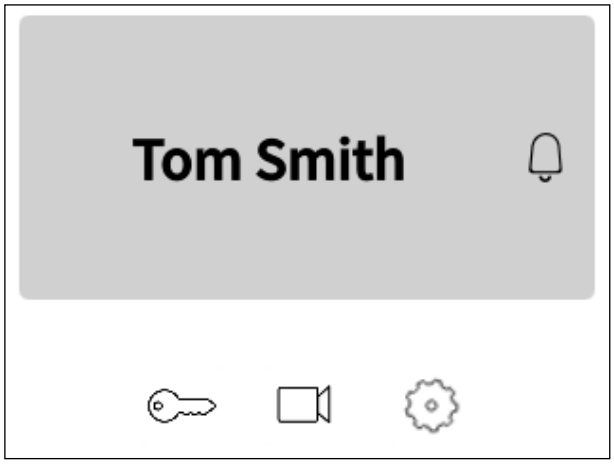
**Schrittübersicht**:

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

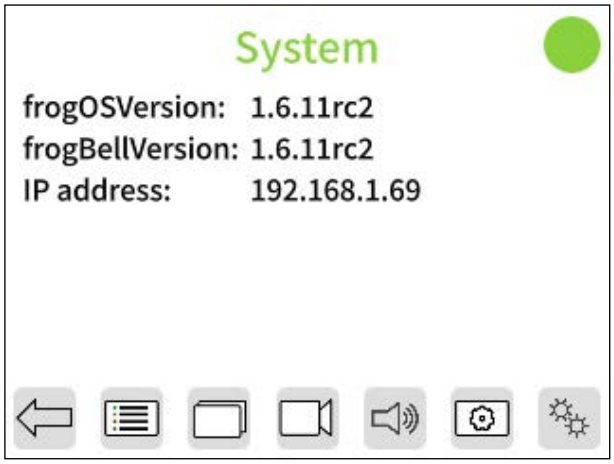
### 6.9.4. Über den Webbrowser (RFID → ZutrittsListe)

*Noch nicht vollständig funktionsfähig. Volle RFID-Konfiguration über den Webbrowser folgt in einem Software-Update.*

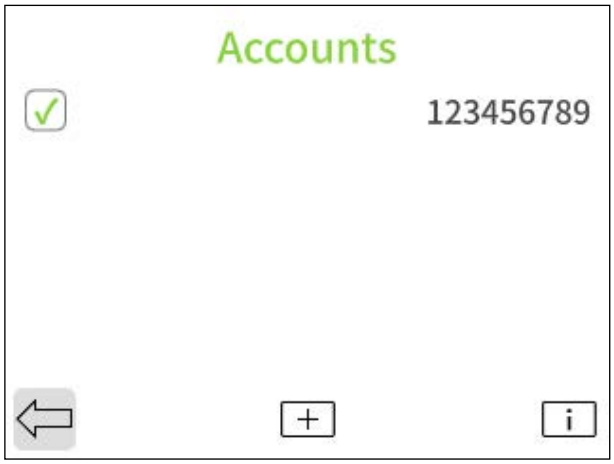
### 6.9.5. Über den On-Device-Touchscreen



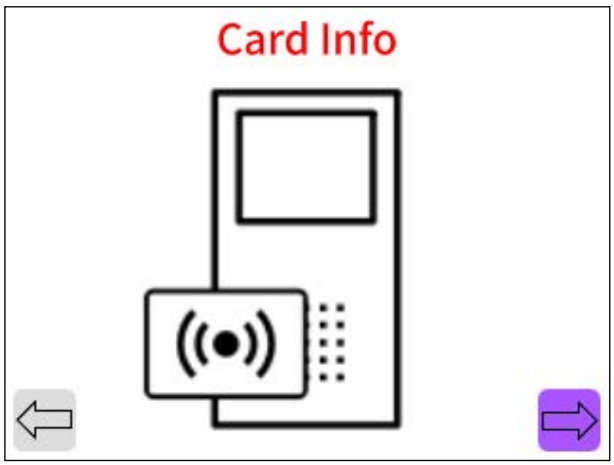

- Tippen Sie ⚙ und geben Sie Ihre sechsstellige Admin-PIN ein, um den Konfigurationsmodus zu betreten.




- Tippen Sie ▭, um auf die RFID-Schlüsseleinstellungen zuzugreifen.

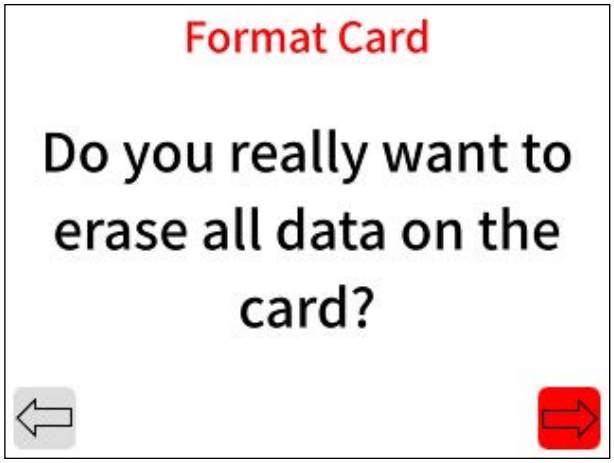



- Tippen Sie [i], um den Dialog „RFID Card Info“ zu öffnen.

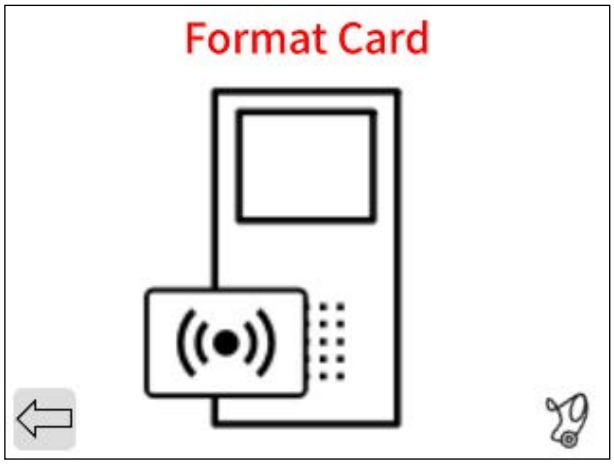



- Halten Sie Ihre RFID-Karte oder Ihren Transponder vor den RFID-Sensor des Terminals – direkt etwas links neben dem Lautsprecher.


- 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.

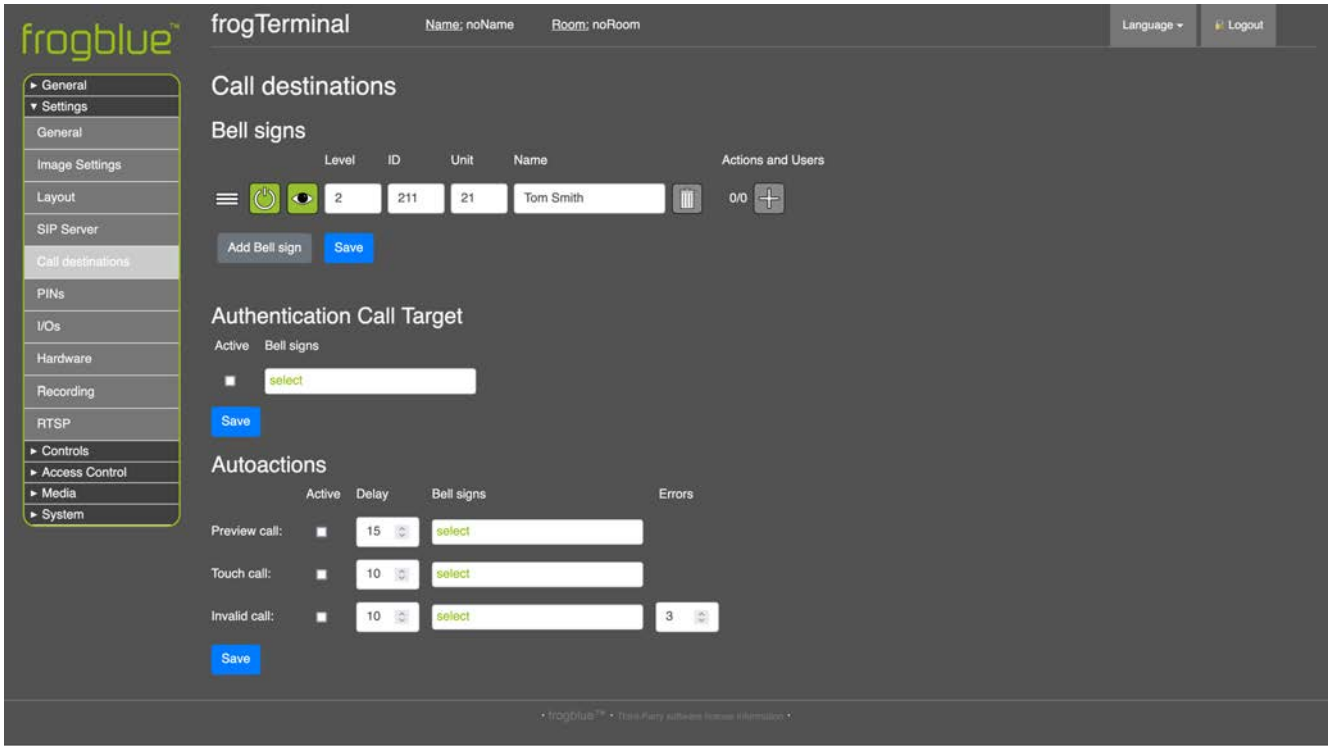



- Halten Sie den Key/die Karte vor das Terminal, warten Sie auf das Bestätigungssignal (Piepton) und Ihre Karte wird auf die Werkseinstellungen zurückgesetzt.

# 7. Telephony Call Destination Einrichtung

## 7.1. Klingelsignale / Ruftasten

Über den Webbrowser im Menü: Einstellungen → „Call destinations“
Hier richten wir die Klingelsignale, „Ring“- oder „Call“-Buttons ein, die auf dem Touchscreen des Terminals erscheinen, wenn dieses einen Input wahrnimmt, z. B. durch Berührung oder den Näherungssensor.




- Klicken Sie auf „**Add Bell sign**“, um eine neue Ruftaste zu erstellen. Ein neuer Eintrag erscheint in der Liste der Klingelsignale.
- 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.
- 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.

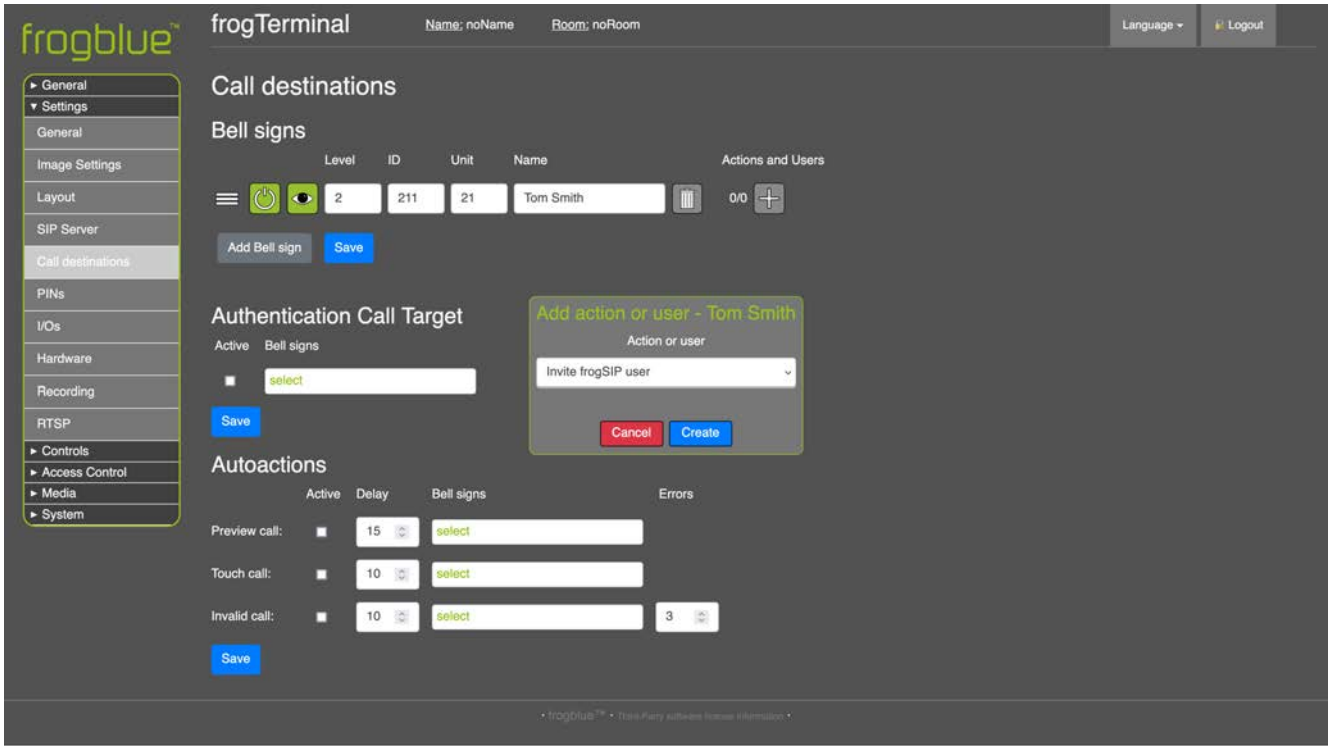
- Wählen Sie, ob dieser Eintrag auf dem Touchscreen des Terminals ausgeblendet oder angezeigt werden soll. Ausgeblendete Einträge können dennoch programmgesteuert (z. B. über APIs) oder für Authentifizierungsanrufe verwendet werden.
- „**Level" (Optional)**: Das Stockwerk, in dem sich der Eintrag befindet (z. B. „2").
- „**ID" (Optional)**: Eine Kennung für diesen Eintrag (z. B. könnte „211" Stockwerk 2, Einheit 21, Person 1 repräsentieren).
- „**Unit" (Optional)**: Gibt die Wohnungs- oder Einheitsnummer an (z. B. „21").
- „**Name"**: Der Anzeigename für den Eintrag auf der Touchscreen-Ruftaste (z. B. „Tom Smith").
- Löscht den Klingelsignal-Eintrag.
- „**Actions and Users"**: Definiert die Aktionen, die ausgelöst werden, wenn eine Klingeltaste gedrückt oder aktiviert wird. Verwenden Sie den Button, 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.

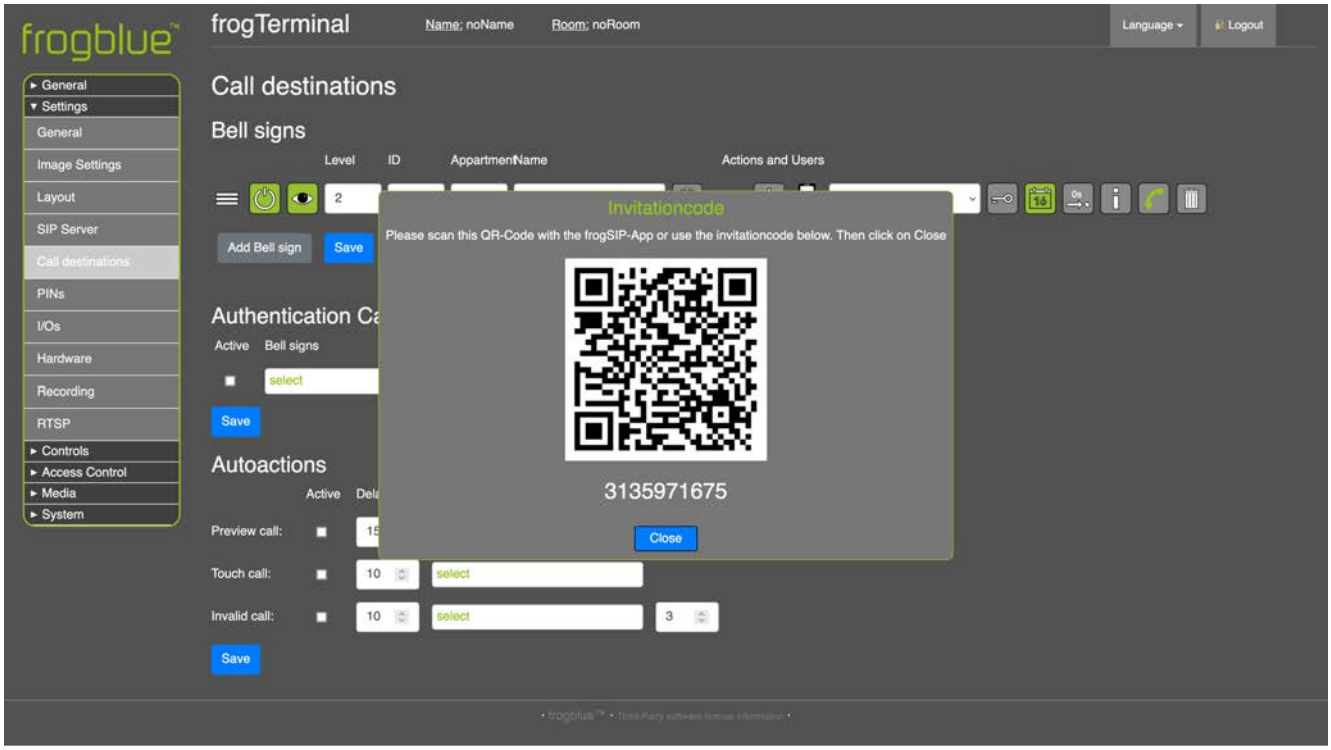
Durch Drücken des Buttons öffnet sich ein Dialog, in dem Sie aus einer Anzahl von Aktionstypen über das Dropdown-Menü wählen können:

### 7.1.1. Klingelaktionen: frogSIP-Benutzer einladen

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



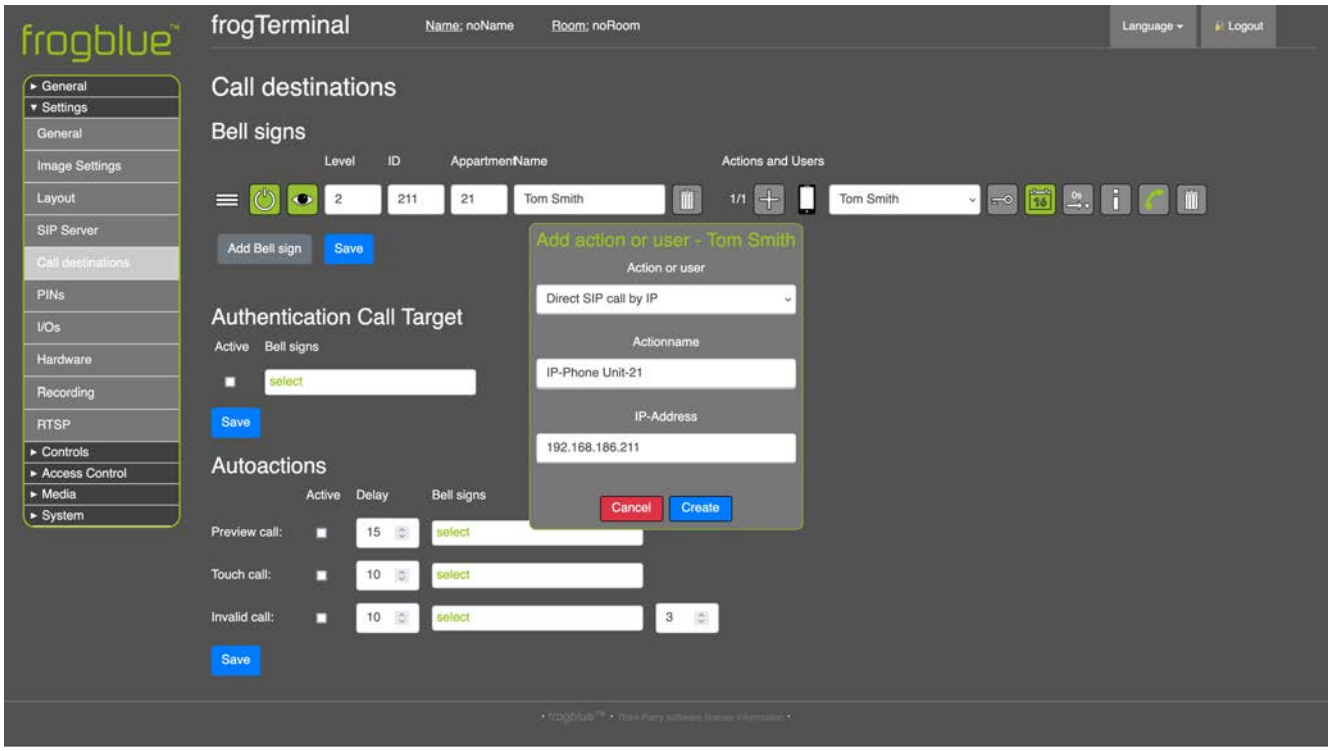

- Wählen Sie „ **Invite frogSIP user** " aus dem Dropdown-Menü
- Klicken Sie auf „**Create**", um eine neue Kopplungseinladung für eine frogSIP App-Verbindung zu erstellen.




- Scannen Sie den QR-Code oder geben Sie den Einladungscode in der **frogSIP App** ein. Siehe Abschnitt **5.6 „Koppeln des Terminals mit der frogSIP App“**.

### 7.1.2. Klingelaktionen: Direkte SIP-Anrufe per IP

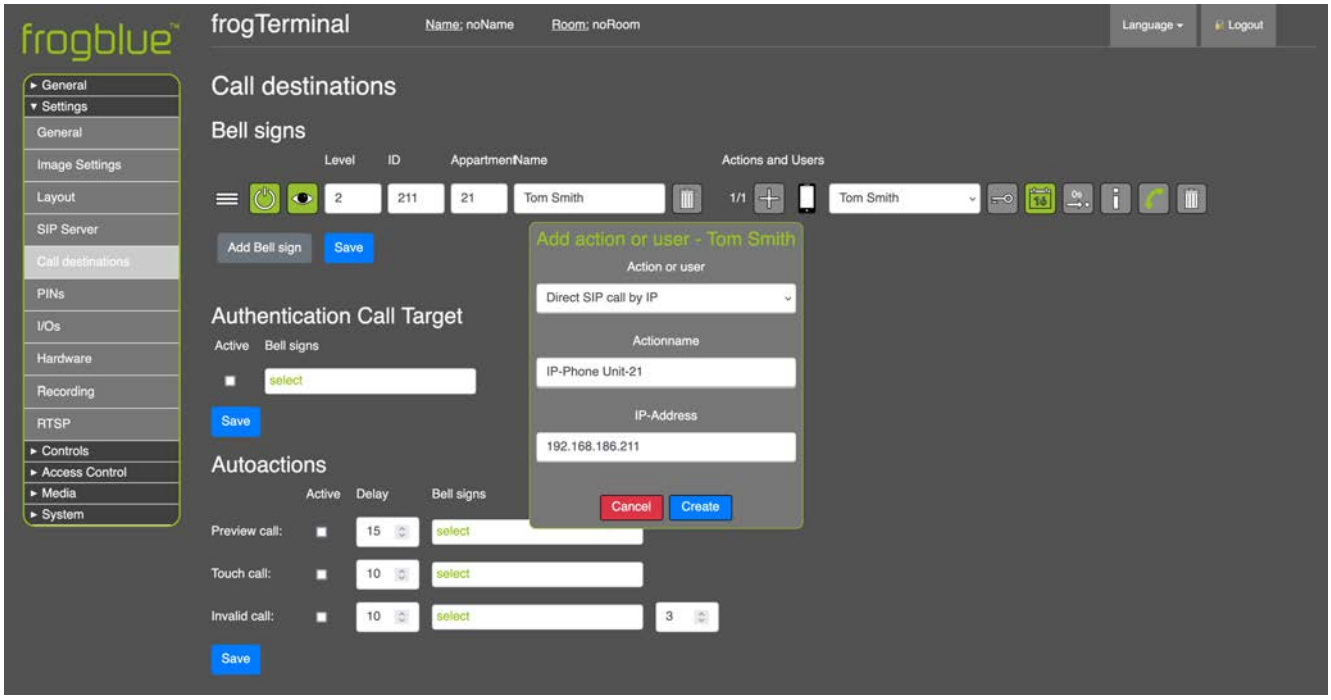
Zum direkten Anrufen von SIP-Telefondiensten via IP.




- Wählen Sie „ **Direct SIP call by IP** “ aus dem Dropdown-Menü.
- „**Actionname**“: Geben Sie einen Namen für die Aktion ein, z. B. „**IP-Phone Unit 21**“.
- „**IP-Address**“: Die IP-Adresse des SIP-Telefondienstes, den Sie anrufen möchten.
- Klicken Sie auf „**Create**“, um eine neue Aktion für direkte SIP-Anrufe per IP zu erstellen.

### 7.1.3. Klingelaktionen: SIP-Anrufe über SIP-Server

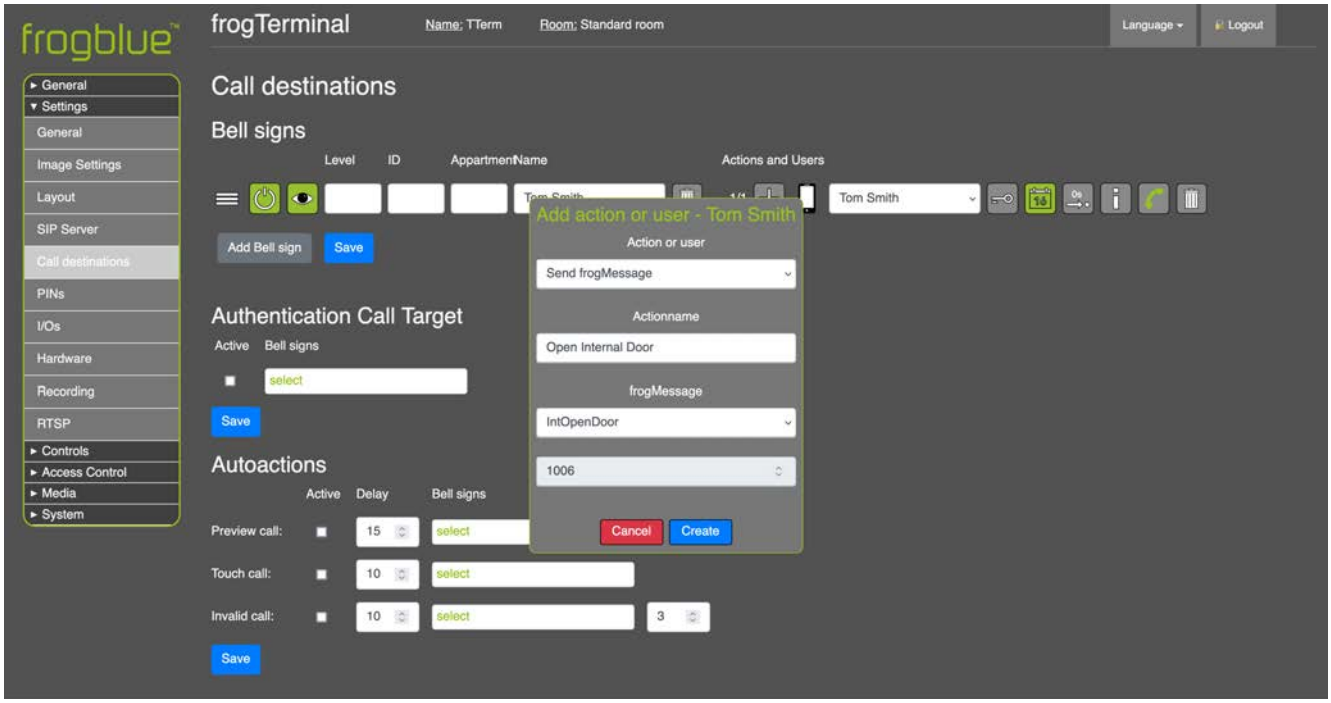
Wenn ein SIP-Server konfiguriert ist, können Anrufe an jedes Telefon im System getätigt werden. Der SIP-Server muss zuerst konfiguriert werden – s. Abschnitt 17.2 „SIP-Server-Registrierung“ für Details.




- Wählen Sie „ **Direct SIP call by IP** “ aus dem Dropdown-Menü.
- „**Actionname**“: Geben Sie einen Namen für die Aktion ein, z. B. „**IP-Phone Unit 21**“.
- „**IP-Address**“: Die IP-Adresse des SIP-Telefondienstes, den Sie anrufen möchten.
- Klicken Sie auf „**Create**“, um eine neue Aktion für direkte SIP-Anrufe per IP zu erstellen.

### 7.1.4. Klingelaktionen: frogMessage senden

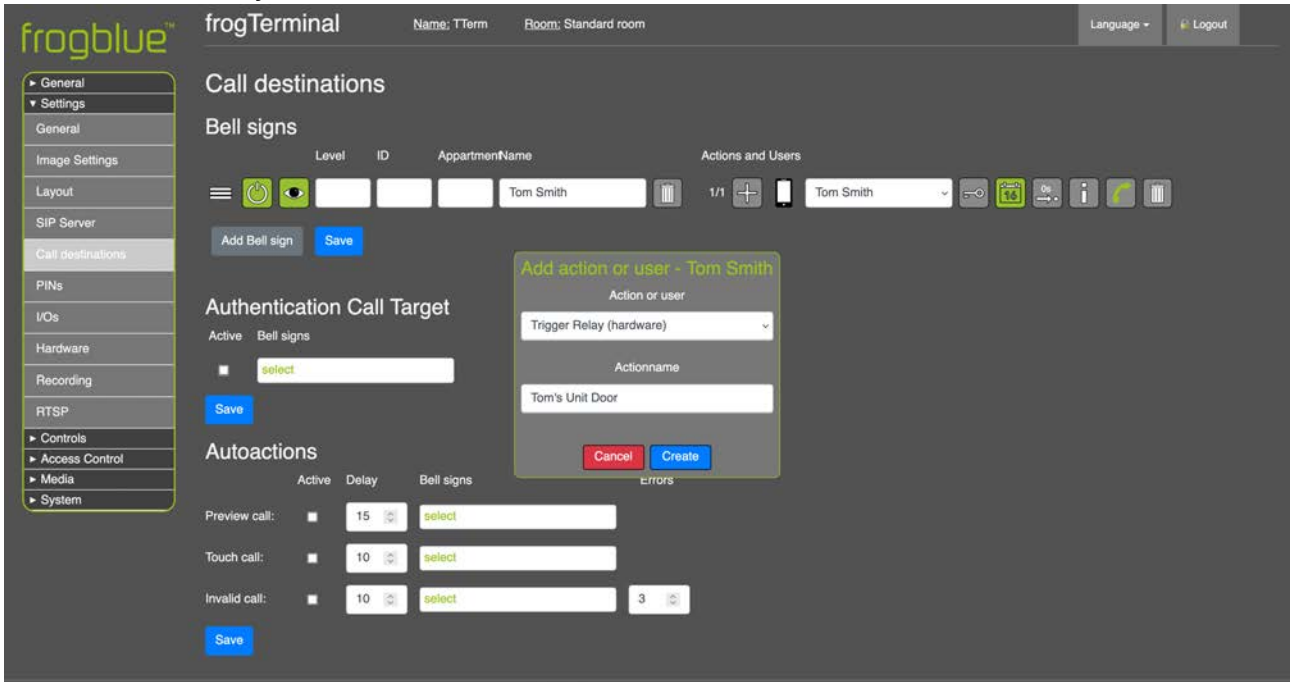
Diese Funktion ermöglicht die nahtlose Integration in frogblues Smart-Automationsnetz, wodurch eine automatisierte Steuerung von Lichtern, Türen und Rollläden möglich ist. Dafür muss Ihr frogTerminal für die frogMesh-Integration vorbereitet werden – siehe Abschnitt 16.



- „**Action or user**“: Wählen Sie „**Send frogMessage**“ aus dem Dropdown-Menü.
- „**Action name**“: Geben Sie einen Namen für die Aktion ein, z. B. „**Open Internal Door**“.
- „**frogMessage**“: Wählen Sie die frogMessage, die Sie senden möchten, aus dem Dropdown-Menü aus.

### 7.1.5. Klingelaktionen: Hardware-Relais auslösen

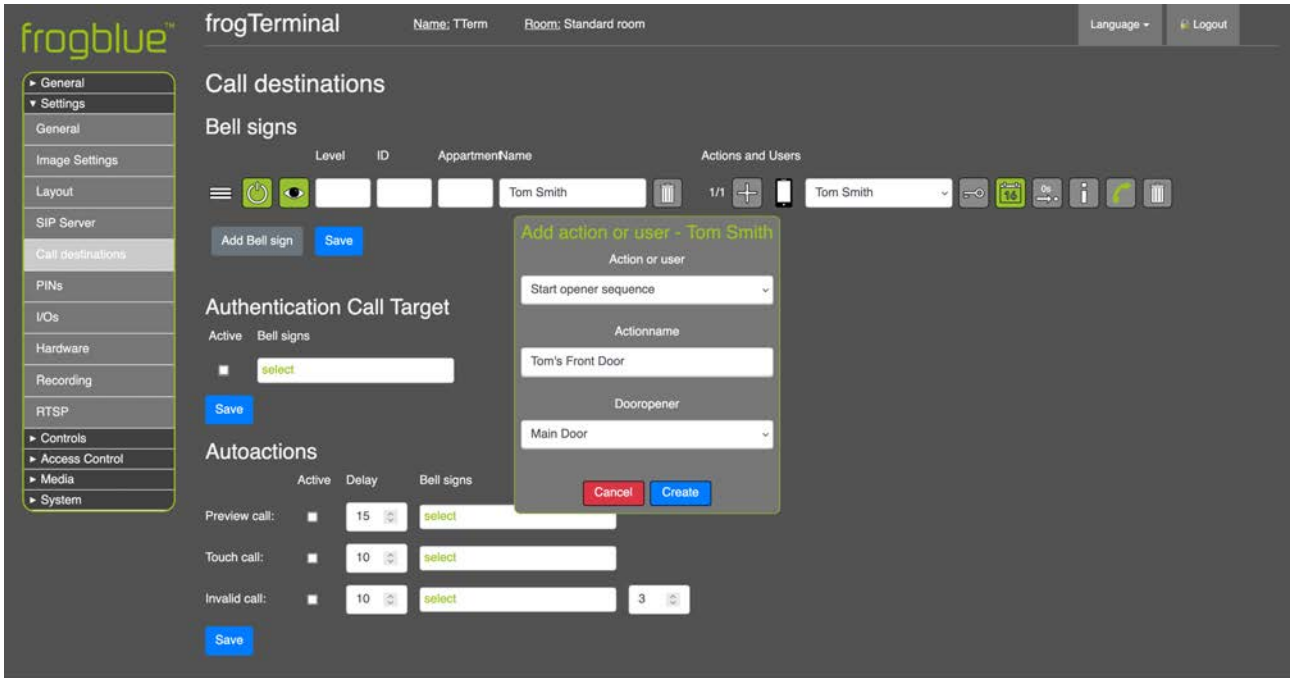
Diese Funktion ermöglicht es Ihnen, das integrierte Hardware-Relais des frogTerminals direkt auszulösen. Beispielsweise kann eine Klingeltaste so konfiguriert werden, dass sie ein externes Licht oder ein anderes System über das Relais aktiviert.




- „**Action or user**“: Wählen Sie „ **Trigger Relay (hardware)** “ aus dem Dropdown-Menü.
- „**Action name**“: Geben Sie einen Namen für die Aktion ein, z. B. „**Tom's Unit Door**“.

### 7.1.6. Klingelaktionen: Öffner-Sequenz starten

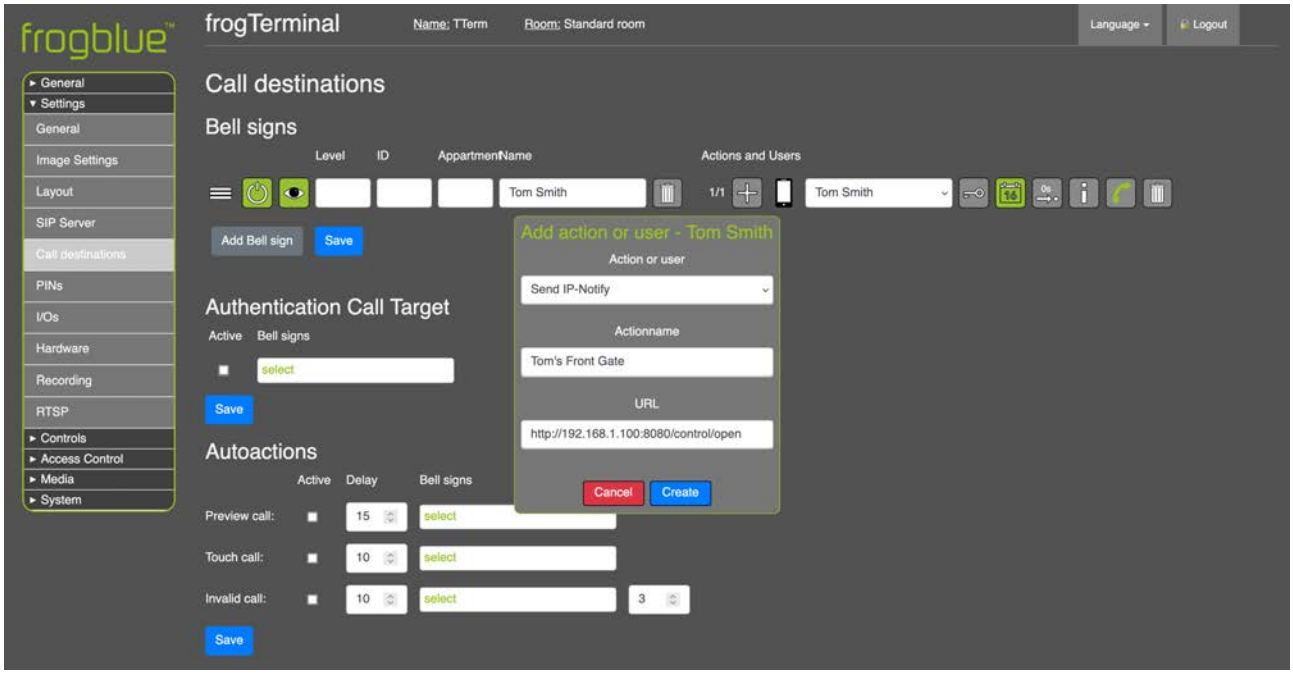
Diese Funktion ermöglicht es, vordefinierte Öffner-Sequenzen oder HomeObjects auszulösen, was eine fortschrittliche Steuerung mehrerer Zutrittspunkte ermöglicht. Beispielsweise können Sie das System so konfigurieren, dass zuerst ein Tor geöffnet und nach einer festgelegten Verzögerung (z. B. 20 Sekunden) automatisch eine Garagentür geöffnet wird. Diese Funktionalität verbessert die Automatisierung, indem sie sequentielle Zutrittsereignisse optimiert.




- „**Action or user**“: Wählen Sie „**Start opener sequence**“ aus dem Dropdown-Menü.
- „**Action name**“: Geben Sie einen Namen für die Aktion ein, z. B. „**Tom's Front Door**“.
- „**frogMessage**“: Die IP-Adresse des SIP-Telefondienstes, den Sie anrufen möchten.

### 7.1.7. Klingelaktionen: IP-Notify senden

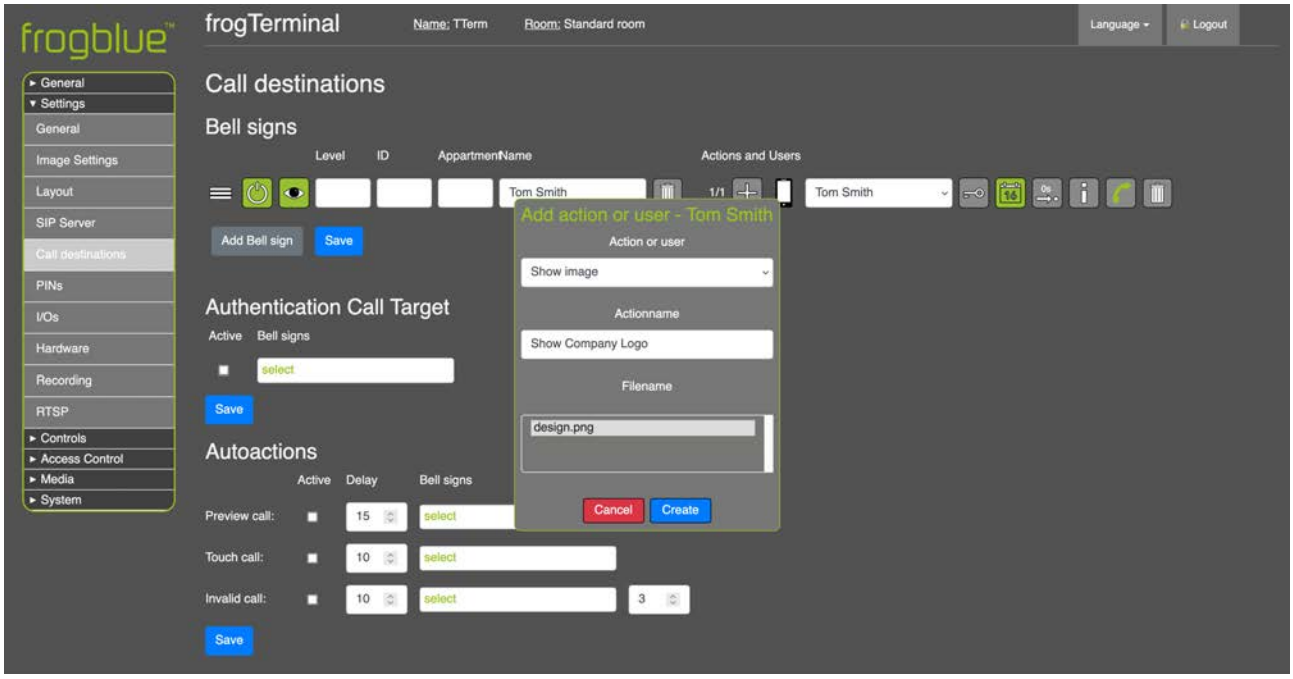
Dies ermöglicht die nahtlose Integration mit IP-Geräten von Drittanbietern, sodass eine Klingeltaste Netzwerkbenachrichtigungen senden kann, die externe Systeme wie z.B.einen IP-Toröffner per IP-Notify auslösen.




- „**Action or user**“: Wählen Sie „ **Send IP-Notify** “ aus dem Dropdown-Menü.
- „**Action name**“: Geben Sie einen Namen für die Aktion ein, z. B. „**Tom's Front Gate**“.
- „**URL**“: Die URL, die für diese Aktion ausgelöst werden soll, wobei die IP-Adresse Ihres Toröffners, Port 8080 und der Befehl „control/open“ erwartet werden, um das Tor zu öffnen.

### 7.1.8. Klingelaktionen: Bild 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.




- „**Action or user**“ Wählen Sie „ **Show image** “ aus dem Dropdown-Menü.
- „**Action name**“: Geben Sie einen Namen für die Aktion ein, z. B. „**Show Company Logo**“.
- „**Filename**“: Wählen Sie eine Bilddatei aus, die auf das Terminal hochgeladen wurde. Weitere Details finden Sie im Abschnitt 15 „Onboard-Medieneinstellungen“.

## 7.2. Authentifizierungs-Anrufziel

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

## 7.3. Automatische Aktionen

Definieren Sie die Anrufziele für Ereignisse oder Fehler am Terminal:

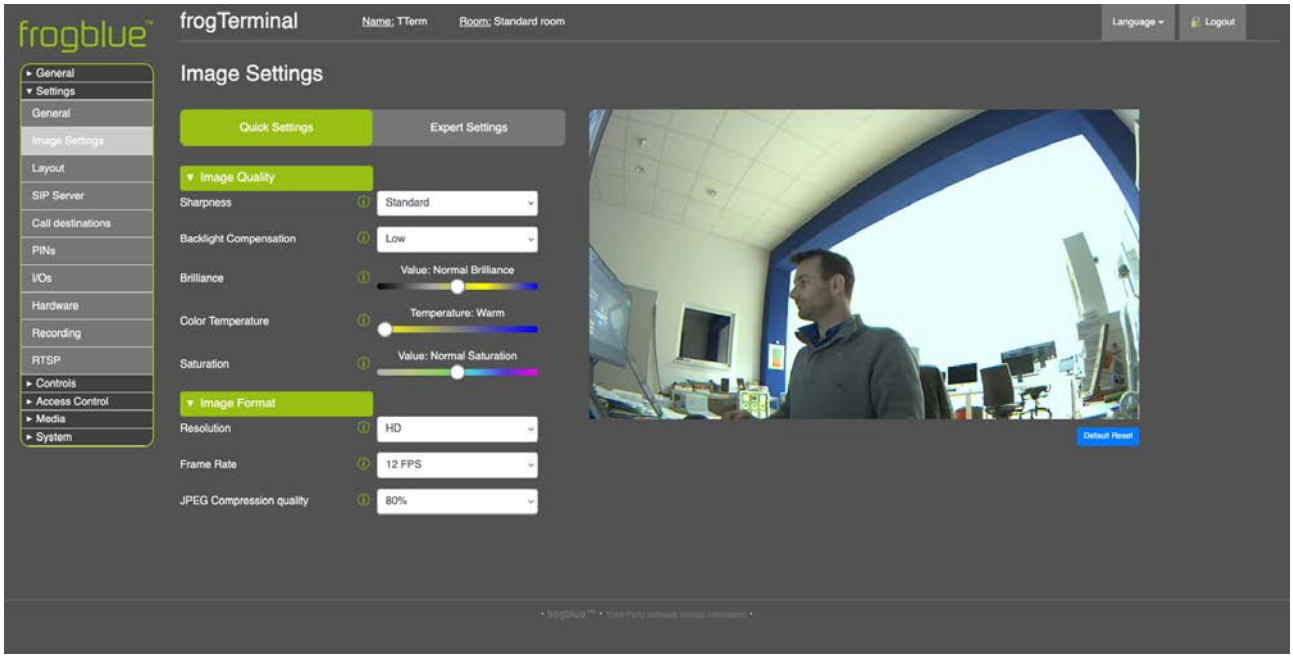
- Vorschauanruf: Wird initiiert, wenn die Näherungs- oder Bewegungssensoren für den angegebenen Verzögerungszeitraum ausgelöst werden und keine Aktion erfolgt, z. B. wenn eine Person eine gewisse Zeit untätig vor dem Terminal steht.
- Touch-Anruf: Wird initiiert, wenn der Touchscreen für den angegebenen 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.

# 8. Kameraeinstellungen und Aufnahmeverwaltung

## 8.1. 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.

## 8.2. 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.

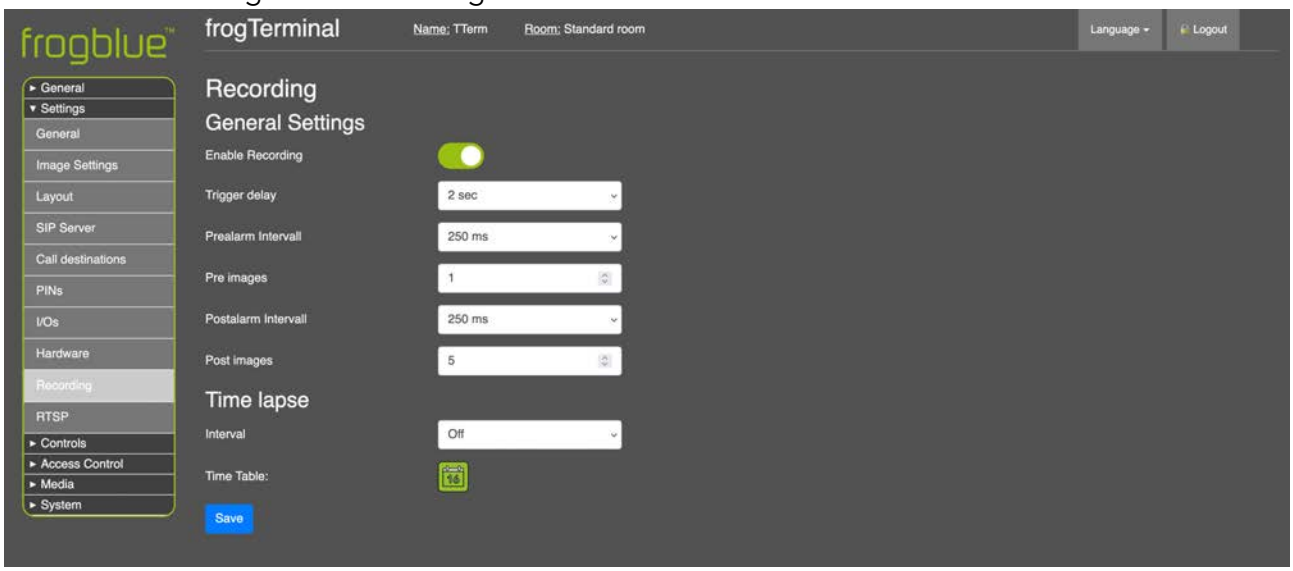
## 8.3. Ereignis-Aufnahmeeinstellungen

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.




- „**Enable Recording**“: Schaltet die Ereignisaufnahme für die integrierte SD-Karte ein oder aus.
- „**Trigger Delay**“: 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, nicht eine störende Hand abbilden, die einen wesentlichen Teil des Bildes verdeckt.
- „ **Pre-alarm Interval:**“: 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.
- „**Pre Images**“: Geben Sie an, wie viele Bilder oder Frames vor dem Auslösen des Ereignisses aufgenommen werden sollen.

- „**Post-alarm Interval**“ Legen Sie die Dauer der Aufnahme nach dem Auslösen des Ereignisses fest.
- „**Post Images**“: Definieren Sie die Anzahl der Bilder oder Frames, die nach dem Auslösen des Ereignisses aufgenommen werden sollen.
- „**Maximum retention period**“: Legen Sie die maximale Dauer fest, in der Aufnahmen und Protokolle gespeichert werden, bevor ältere Daten automatisch mithilfe eines Ringpuffer-Mechanismus gelöscht werden.

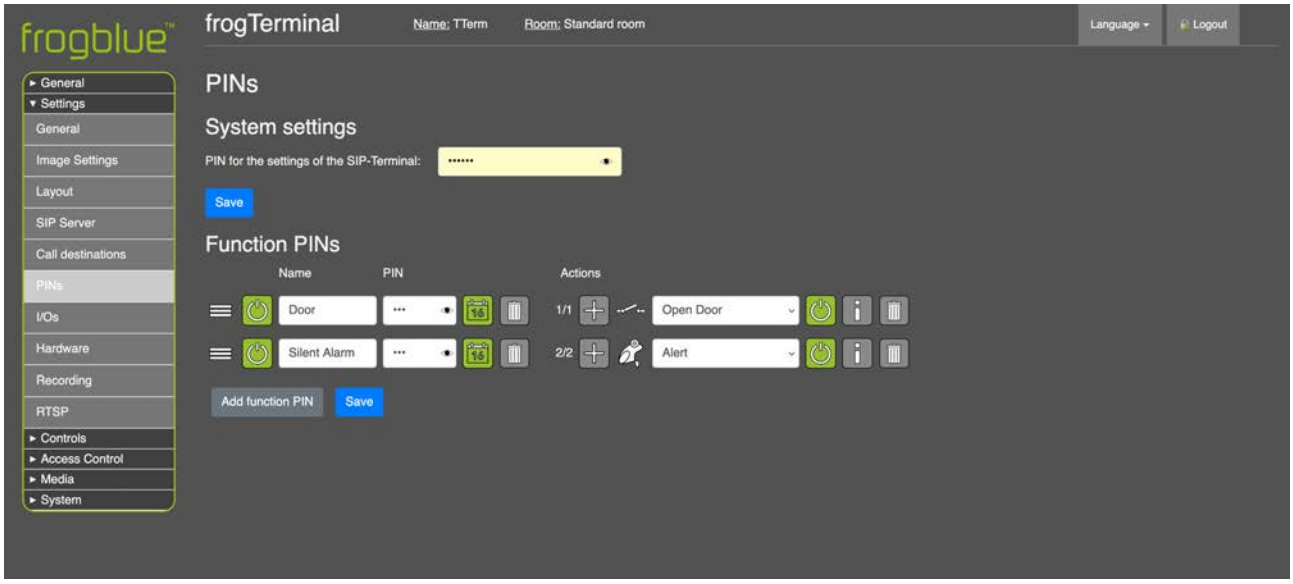
**Zeitraffer**

- „**Interval**“: Legen Sie das Intervall zwischen Zeitraffer-Aufnahmen fest, um periodische Schnappschüsse zu erfassen.
- „**Time Table**“: Geben Sie den Zeitplan für die Zeitraffer-Aufnahme an – beispielsweise Aufzeichnung nur während der Tageslichtstunden, um eine optimale Bildaufnahme sicherzustellen.

## 9. Admin-PIN & Funktions-PINs

Über den Webbrowser im Menü: Einstellungen → 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.




„**System settings**“: Legen Sie eine exakt sechsstellige PIN fest, welche zur Verwaltung des frogTerminals über den On-Device-Touchsreen verwendet wird, um Zugriff auf die lokalen Systemeinstellungen zu erhalten.

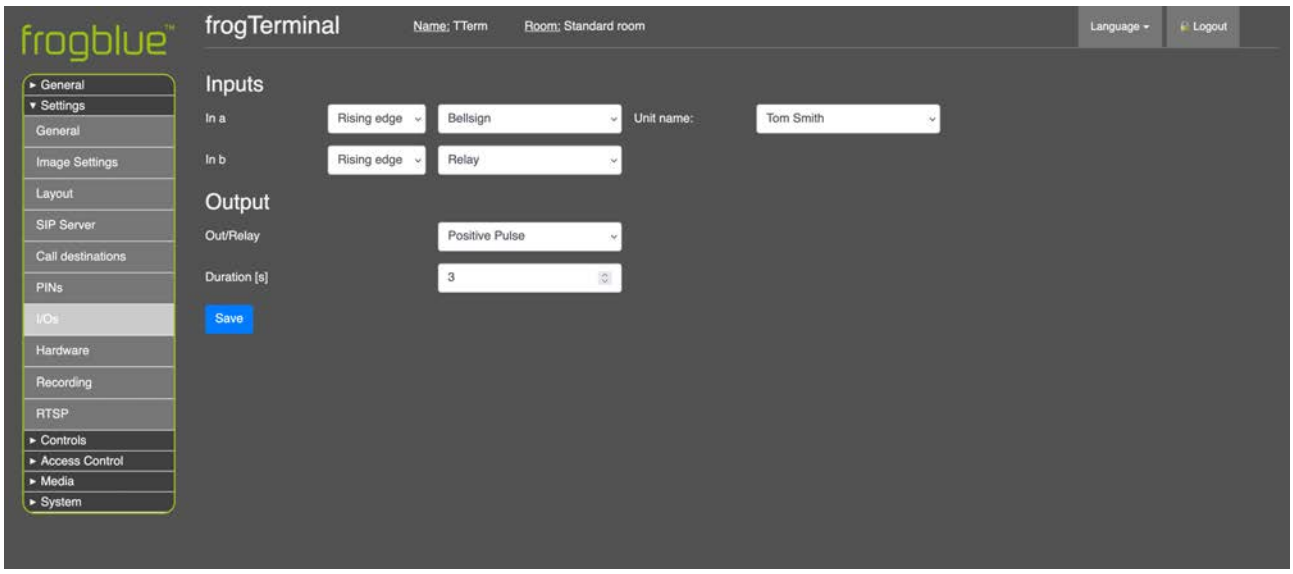
„**Function PINs**“: Ein Funktions-PIN muss eins bis sechs Nummern enthalten, die Länge des PINs ist frei wählbar. Funktion PINs lösen hinterlegte Funktionen, wie das lokale Relais aus, oder versenden Nachrichten über IP & Bluethooth.

**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.

# 10. Ein- / Ausgabe-Einstellungen

Über den Webbrowser im Menü: Einstellungen → I/Os

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




**Eingangskonfiguration (In a / In b)**: Konfigurieren Sie die physischen Eingänge A und B, um Aktionen basierend auf Zustandsänderungen auszulösen

- „**Rising edge**“: Wird aktiviert, wenn der Eingang von niedrig nach hoch wechselt.
- „**Falling edge**“: Wird aktiviert, wenn der Eingang von hoch nach niedrig wechselt.

- **Wählen Sie die Aktion für den Eingang:**
  - „**Bellsign**“: Wählen Sie den Klingel-Eintrag aus, der einen Anruf auslösen soll, wenn dieser Eingang aktiviert wird.
  - „**BT-Message**“: Senden Sie eine Bluetooth-Nachricht über frogMesh.
  - „**Relay**“: Aktivieren Sie das Hardware-Relais.
  - „**IP Notify**“: Senden Sie eine IP-Nachricht oder HTTP-Anfrage an eine bestimmte URL.
  - „**Play Sound“**: Wählen Sie eine Audiodatei (z. B. einen Klingelton) aus, die abgespielt wird, wenn der Eingang aktiviert wird.

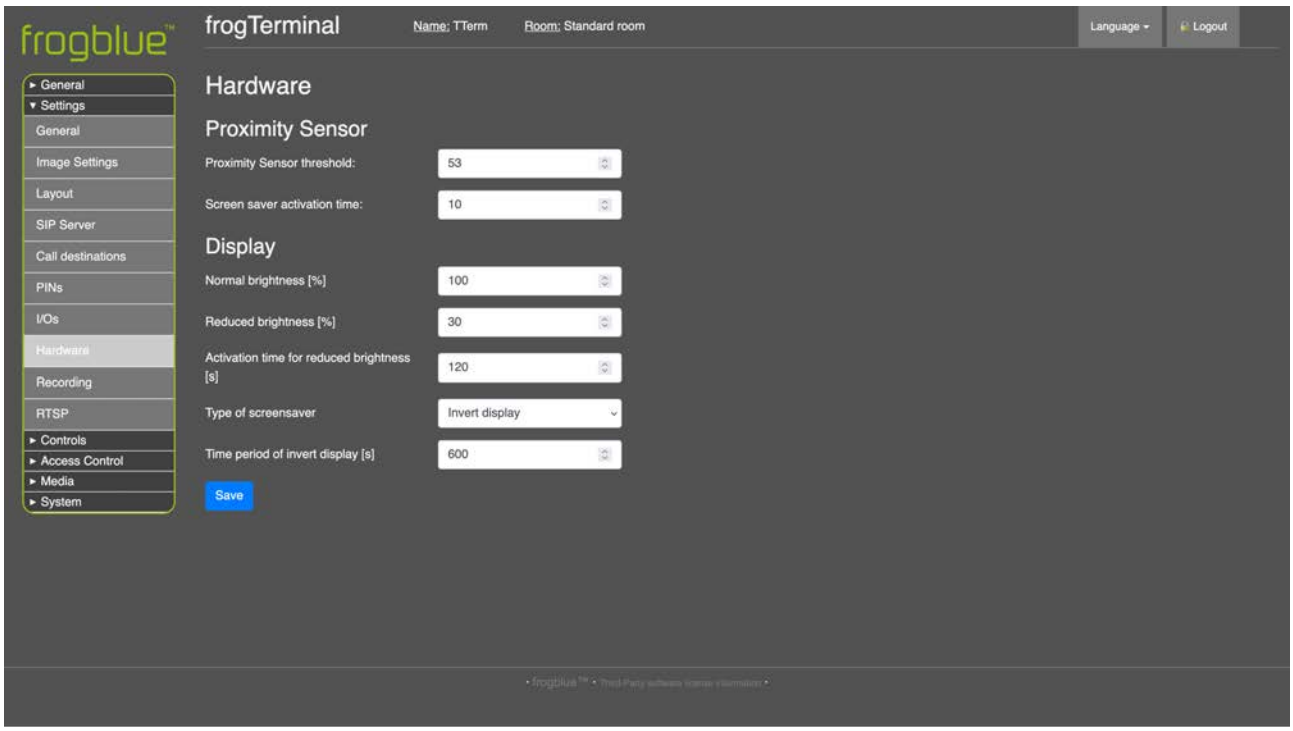
**„Output“**: Legen Sie die physischen Relais-Ausgangseinstellungen fest:

- „**Out/Relay“:** Wählen Sie zwischen einem positiven oder negativen Impuls.
- **„Duration (s)“**: Definieren Sie die Dauer in Sekunden, in der das Relais ausgelöst wird.

# 11. Hardware-Einstellungen: Näherungssensor & Touchscreen-Display

Über den Webbrowser im Menü: Einstellungen → Hardware

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




**„ Proximity Sensor“**

- **„Proximity Sensor Threshold“**: Diese Einstellung bestimmt die Empfindlichkeit des Näherungssensors, niedrigere Werte bedeuten höhere Empfindlichkeit.
- Um den aktuellen Erkennungswert zu visualisieren, navigieren Sie über die Bildschirmmenüs des Gerätes ( → → ) zu einer Live-Grafik der Näherungssensorwerte.
- **„Screen saver activation time“**: Zeit in Sekunden ohne Aktivität, nach der das Terminal automatisch in den Bildschirmschoner oder den Startbildschirm wechselt.

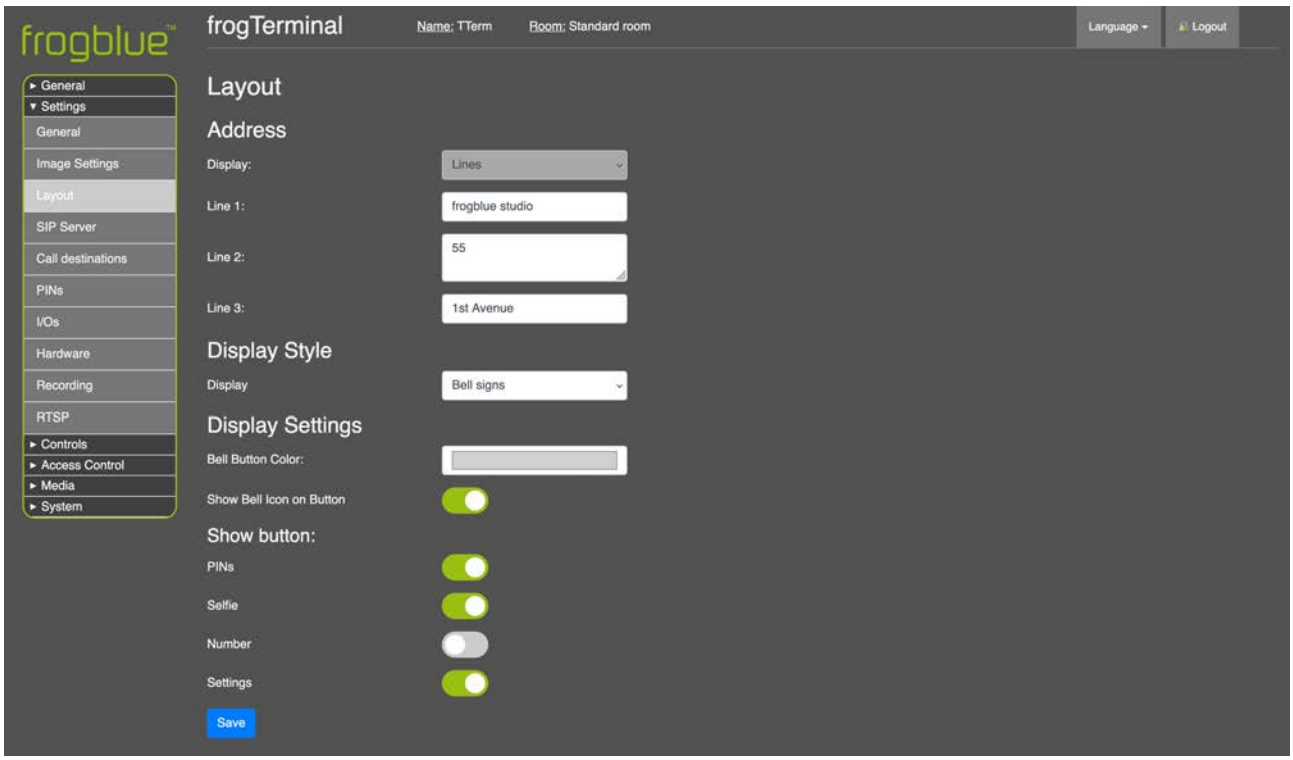
**„Display“**

- **„Normal brightness [%]“**: Diese Einstellung bestimmt die Helligkeit des Terminaldisplays bei Aktivierung, z. B. durch Berührung oder Näherung.
- **„Reduced brightness [%]“**: Diese Einstellung bestimmt die Helligkeit des Terminaldisplays im Standby-Modus.
- **„Activation time for reduced brightness [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. Touchscreen-Display-Layout

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

Konfigurieren Sie das Home Screen Layout für die Terminals auf dem Gerätetouchscreen.

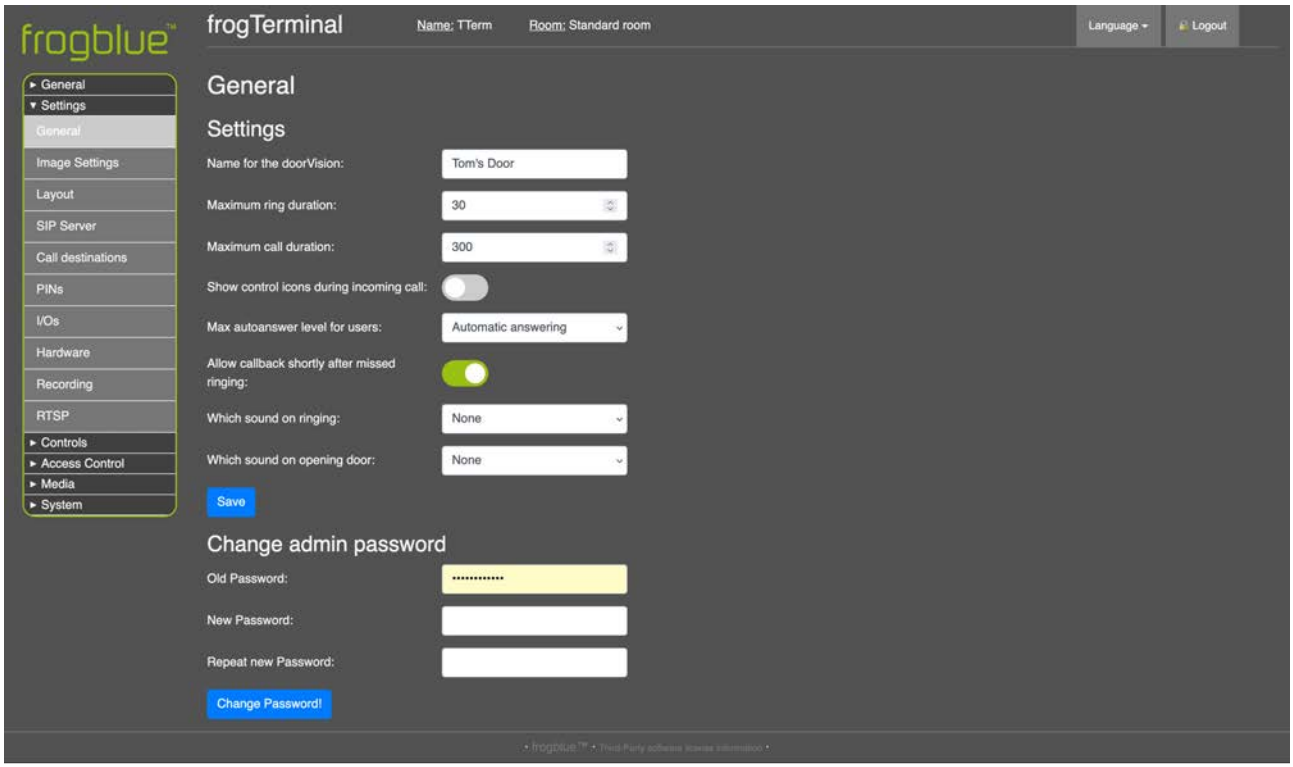



- „**Address**“: Die Einstellungen für das Layout des Standby-Bildschirms.
- „**Display**“: Die Einstellungen für den Startbildschirm.

# 13. Allgemeine Terminal-Einstellungen

Über den Webbrowser im Menü: Einstellungen → Allgemein

Konfigurieren Sie allgemeine Einstellungen wie den Namen, die Standard-Klingeleinstellungen und das Web-Admin-Passwort.




### Einstellungen

- **„Name for the doorVision“**: Geben Sie den Namen für Ihr frogTerminal ein, z. B. „Toms Tür“, um das Gerät in Ihrem System zu identifizieren.
- **„Maximum ring duration“**: Legen Sie die maximale Zeit fest, die das Terminal versucht, bei einem Angerufenen zu klingeln, bevor es aufgibt.
- **„ Maximum call duration“**: Legen Sie die maximale Anrufdauer fest, nach der das Terminal automatisch auflegt.
- **„ Show control icons during incoming call“**: Blendet die Symbolleiste automatisch ein, wenn ein Anruf eingeht (z. B. um Video ein- oder auszuschalten).
- **„ Max autoanswer level for users:“**: Legen Sie das zulässige Level für die automatische Anrufbeantwortung fest:
  - **„Decline“**: Alle eingehenden Anrufe automatisch ablehnen.
  - **„No“**: Eingehende Anrufe nicht zulassen; keine SIP-Verbindungen werden akzeptiert.
  - **„Automatic answering“**: Automatische Anrufbeantwortung aktivieren. Beachten Sie, dass individuelle Benutzerberechtigungen weiterhin im Menü der Anrufzielaktionen konfiguriert werden müssen (klicken Sie auf den „i“-Button neben dem Aktionseintrag eines Benutzers, um die Anrufbeantwortung am Terminal für diesen Benutzer zuzulassen).
- **„Allow callback shortly after missed ringing“**: 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.

- **„Ring sound“**: Der Ton, der am Terminal abgespielt wird, wenn ein Anruf erfolgt.
- **„Open door sound“**: 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.

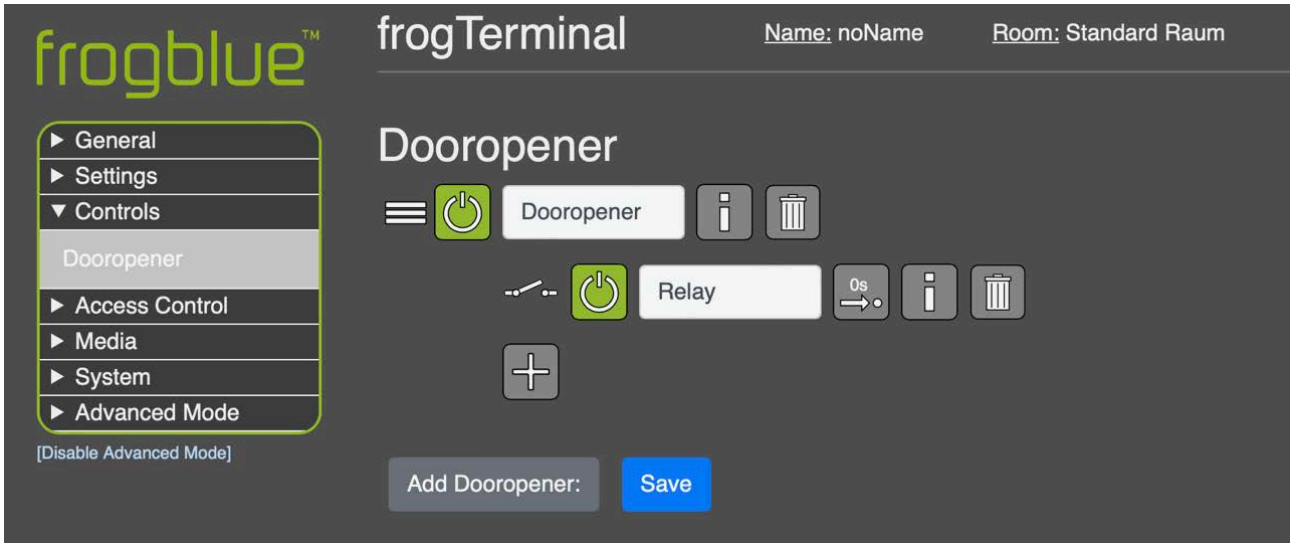
**„Change admin password“**

- **„Web-Admin-Passwort“**: 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 „**Change password**“ klicken!

## 14. Türsteuerungseinstellungen

Über den Webbrowser im Menü: Steuerung → Türöffner

Konfigurieren sie den lokalen Türöffner, “Homeobjects” und die Steuerungsmöglichkeiten der frogSip-App.



# 15. Onboard-Medieneinstellungen

Über den Webbrowser im Menü „Medien“

Konfigurieren sie die Einstellungen der visuellen und akustischen Bereiche und verwalten Sie die Aufzeichnungen von lokalen Events.

## 15.1. Audio-Dateien

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

## 15.2. Bilddateien

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


## 15.3. Video-Dateien

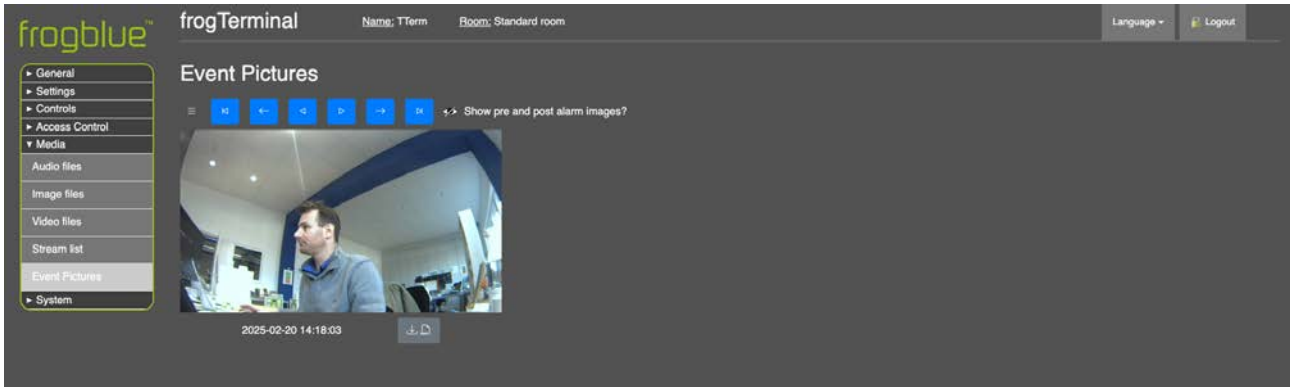
Ermöglicht die Verwaltung und das Hochladen benutzerdefinierter Videodateien, die im frogTerminal verwendet werden können, z. B. für Lieferhinweise oder automatisierte Standort-Einweisungen.


## 15.4. Streamliste

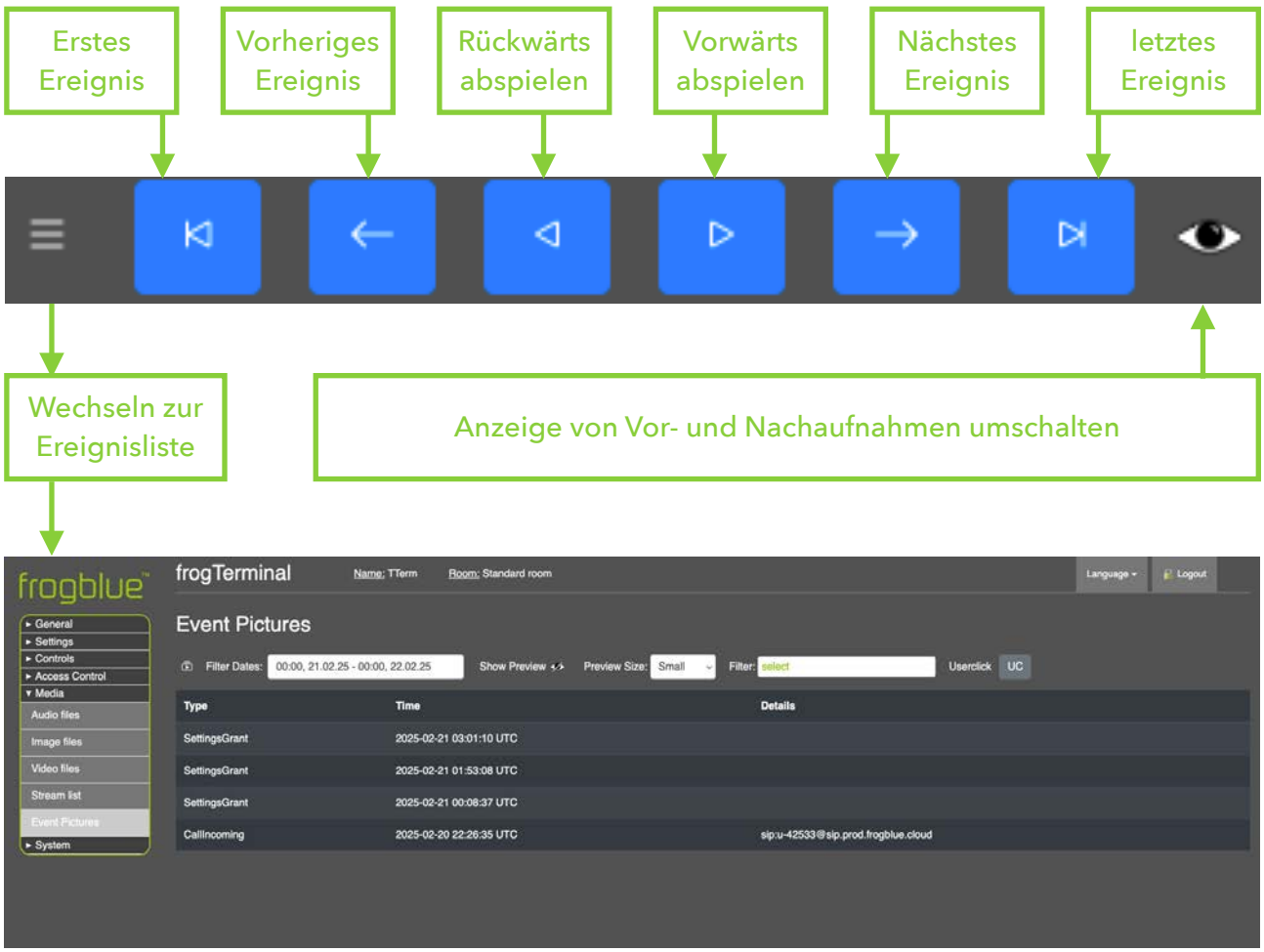
*Funktion noch nicht vollständig implementiert – Unterstützung für externe Streams folgt.*

## 15.5. 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.
- UC Löst eine manuelle Aufnahme aus.

# 16. 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. Kapitel 4.4).

Wenn Sie die Benutzeroberfläche offen gelassen haben, fahren Sie fort. Falls Sie die Benutzeroberfläche gesperrt haben, siehe Abschnitt 20 „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.

# 17. Netzwerkkonfiguration

## 17.1. 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.

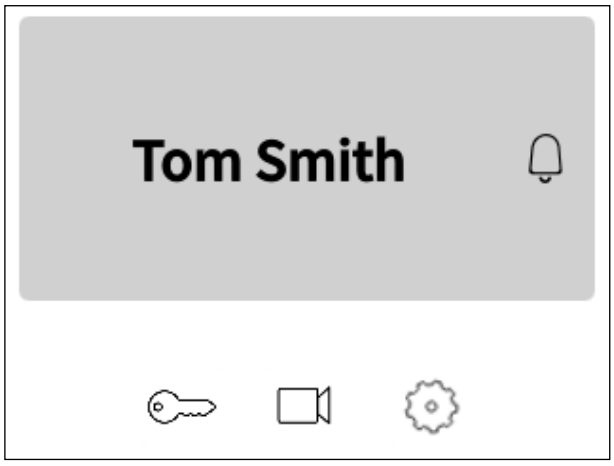
### 17.1.1. Netzwerkkonfiguration über den Webbrowser.

Menü: System → Netzwerk

*Noch nicht vollständig funktionsfähig. Volle Netzwerkeinrichtung über den Webbrowser folgt in einem Software-Update.*

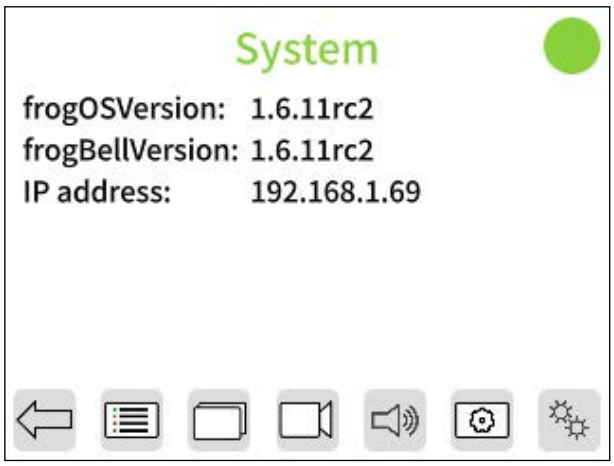

- Schalten Sie frogCast über das Kontrollkästchen ein oder aus.

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




- Tippen Sie ⚙, um in den Konfigurationsmodus zu gelangen.

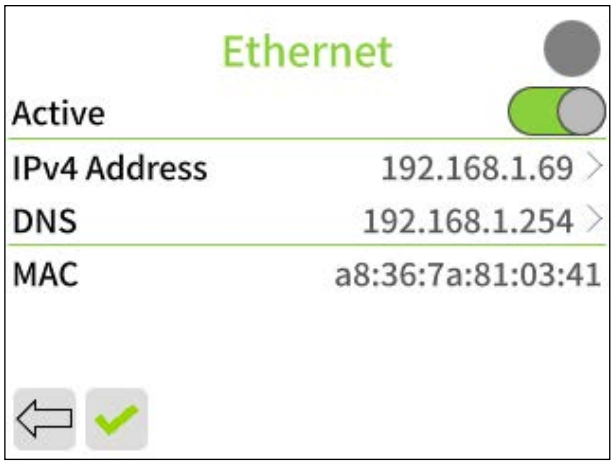

- Geben Sie Ihre sechsstellige Admin-PIN ein und tippen Sie **OK**




- Tippen Sie , um auf die zusätzlichen Einstellungseiten zuzugreifen.

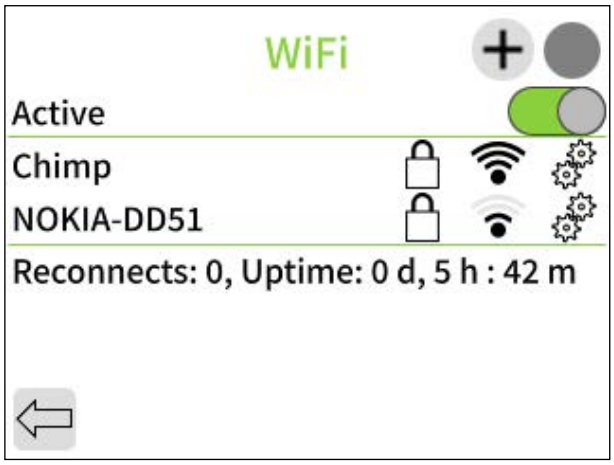

- Tippen Sie , um die Ethernet-Einstellungen zu konfigurieren → Springen Sie zu Abschnitt 4.1.7.
- Tippen Sie um die WLAN-Einstellungen zu konfigurieren → Springen Sie zu Abschnitt 4.1.7.

### 17.1.3. 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.

### 17.1.4. 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**".

### 17.1.5. 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.

### 17.2. SIP-Server-Registrierung

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

**Schrittübersicht**:

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

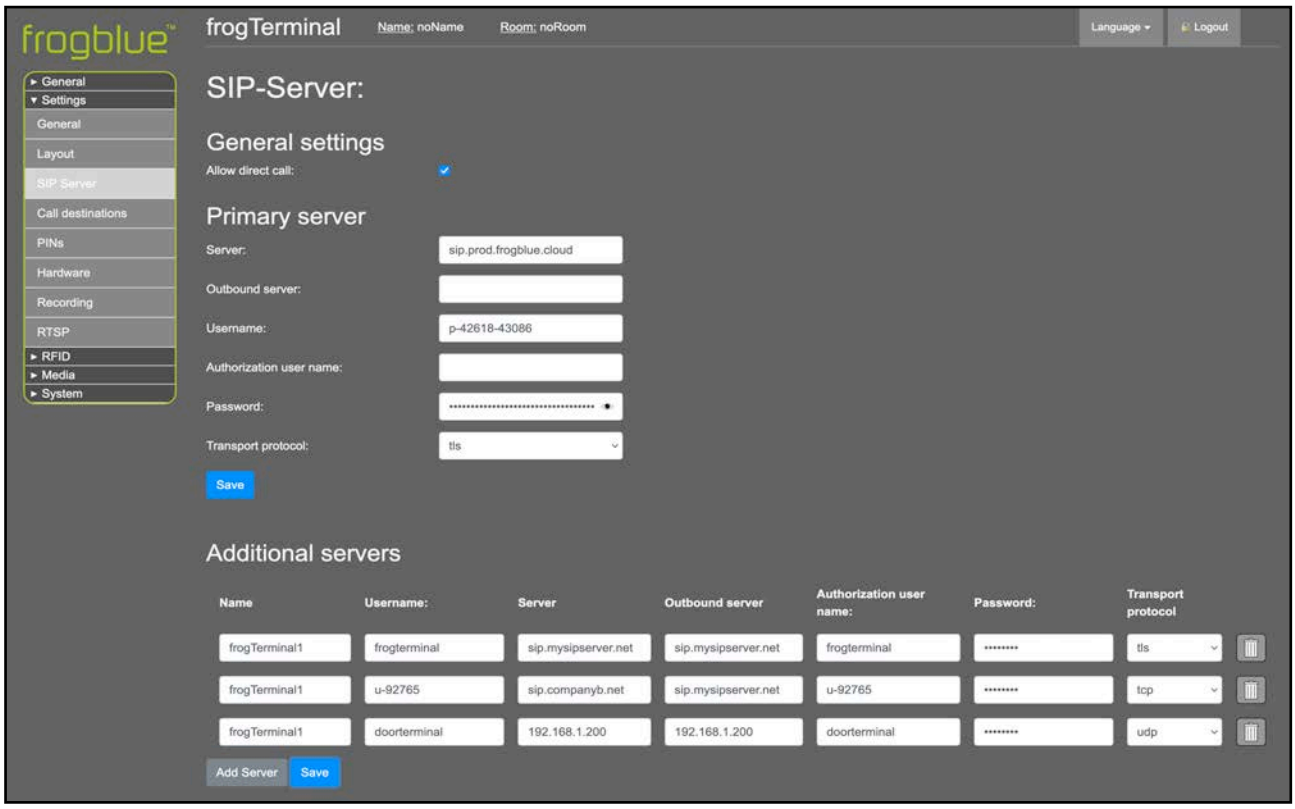
#### 17.2.1. SIP-Grundlagen

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, bei der sich das Terminal registriert.
- „**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 separaten Autorisierungsbenutzernamen für die Anmeldung, der von der SIP-Erweiterung abweichen kann.
- **„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.

### 17.2.2. SIP-Einrichtung über den Webbrowser

Menü: Einstellungen → SIP-Server




**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 sechsstellige PIN für den Zutritt an diesem Terminal festlegen können.*
- **„Time Table Source“**: Gibt an, aus welcher Quelle zeitbasierte Zutrittsregeln stammen, mit drei Optionen:
  - **Keine**: 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).

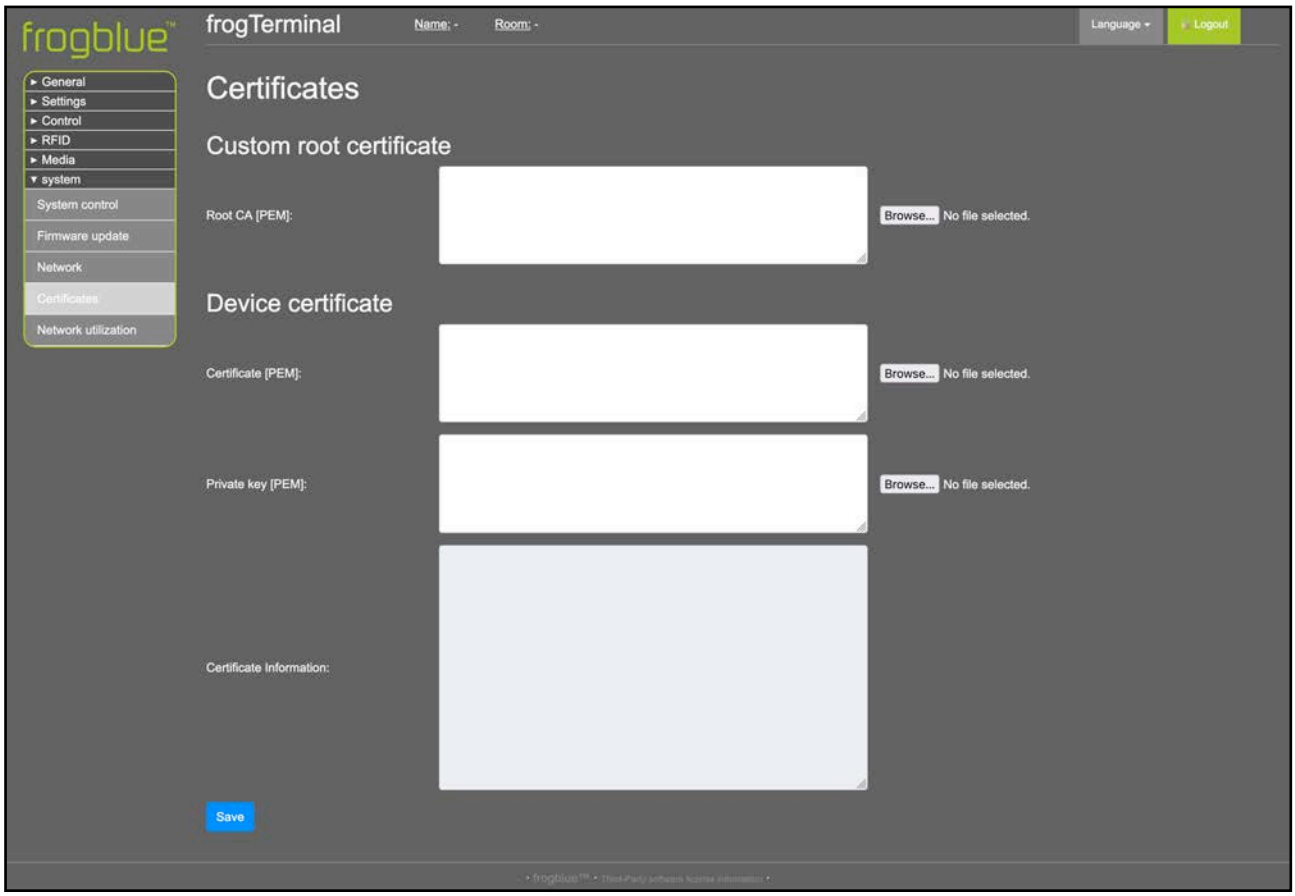
- **Terminal**: Die Zeitregeln werden lokal auf dem Terminal gespeichert. So kann jedes Terminal einen individuellen Zeitplan als Quelle für Zeitregeln haben. Vorhandene Zeitpläne auf einer Zutrittskarte werden auf diesem Terminal ignoriert.

## 17.3. 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 ode 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 cetificate“:**

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 **„ 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.

# 18. Integration mit Drittanbieter-Videosystemen

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

## 18.1. 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

## 18.2. 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.

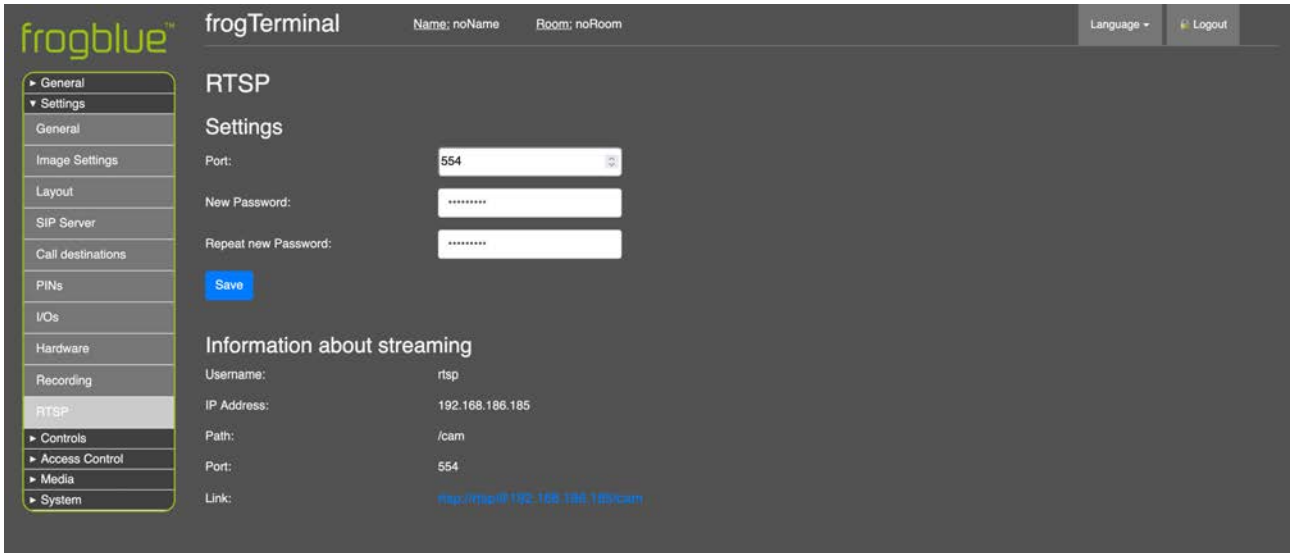
- Die **On-board-Aufnahme** für optimale Leistung **deaktiviert** ist. Stattdessen verwenden Sie ein **VMS**-System zur Videoaufzeichnung.

**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.

## 18.3. 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:

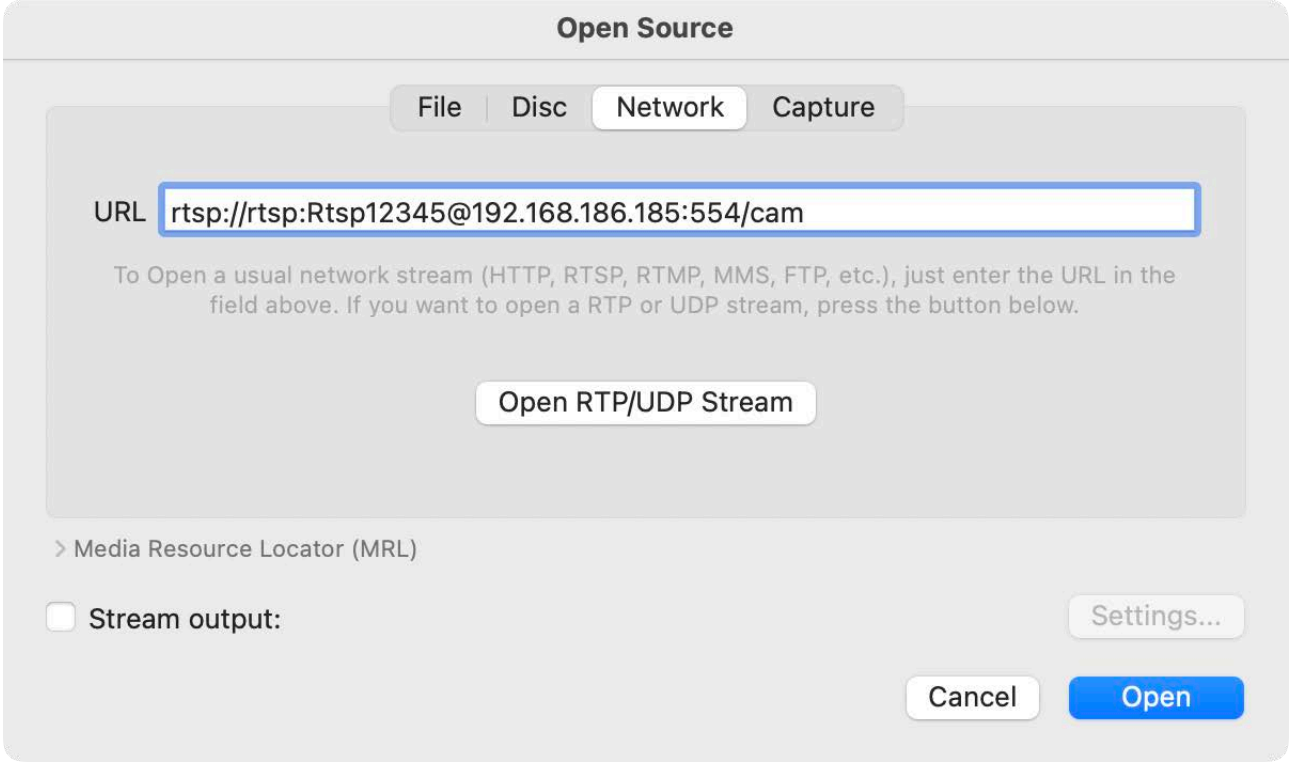
- RTSP auf dem frogTerminal aktiviert ist.
- Die korrekte RTSP-URL verwendet wird:

### RTSP-Integration mit VLC Media Player

**VLC Media Player** ist ein Open-Source-Videoplayer, 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.

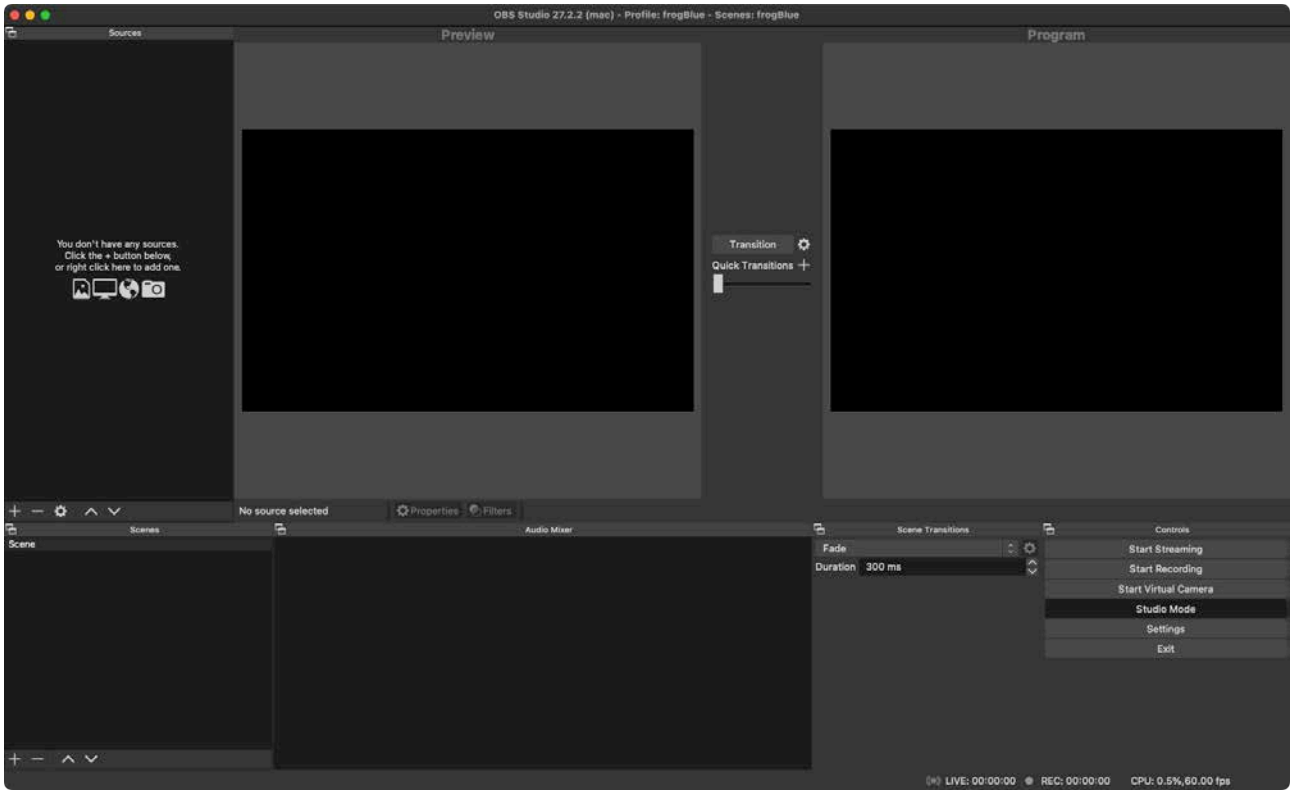

Der Kamerastream sollte nun im VLC-Hauptfenster erscheinen. Standardmäßig puffert VLC den Stream, was zu einer Verzögerung von mehreren Sekunden führen kann.

**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.

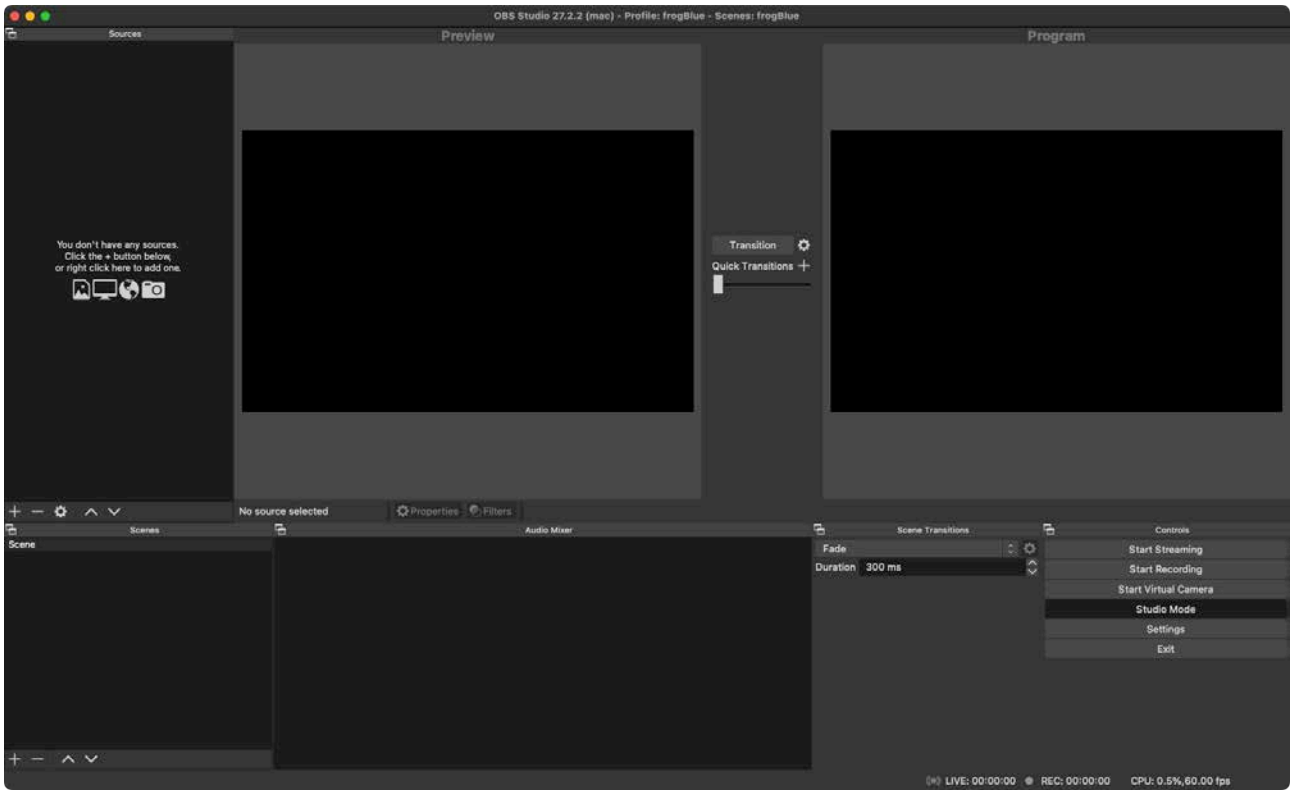
### RTSP-Integration mit OBS Studio

**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:

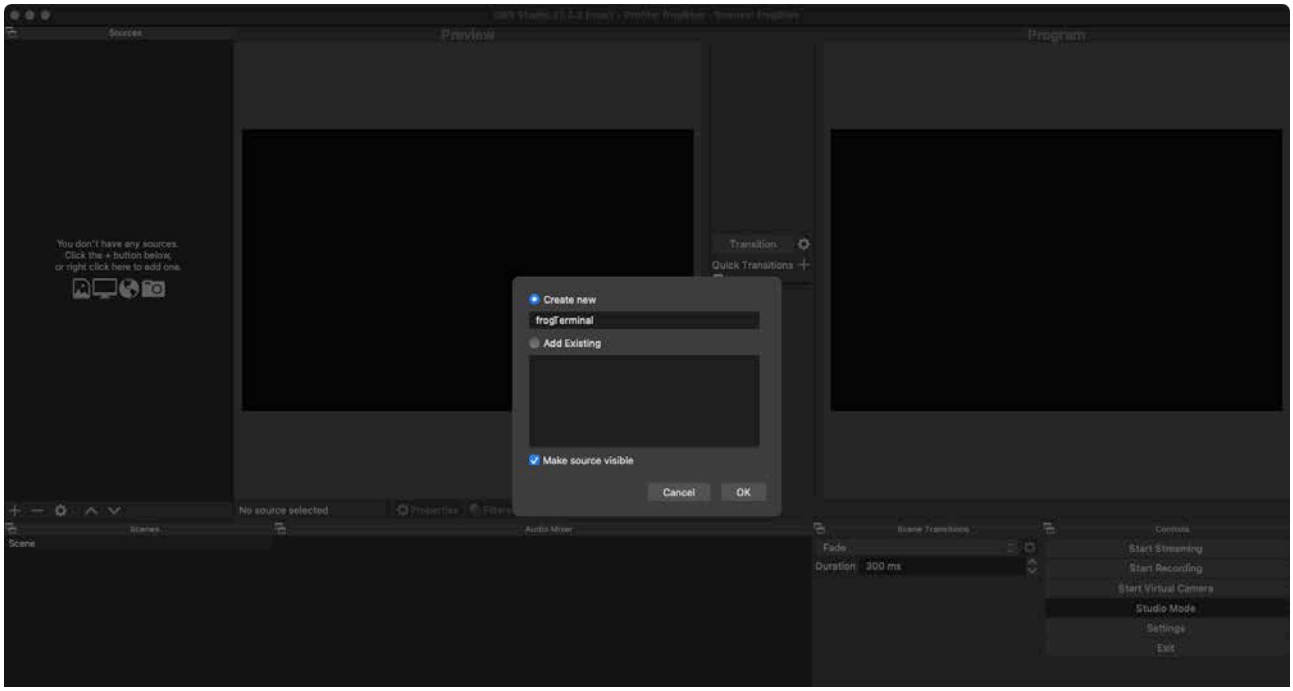
- Öffnen Sie **OBS Studio**.



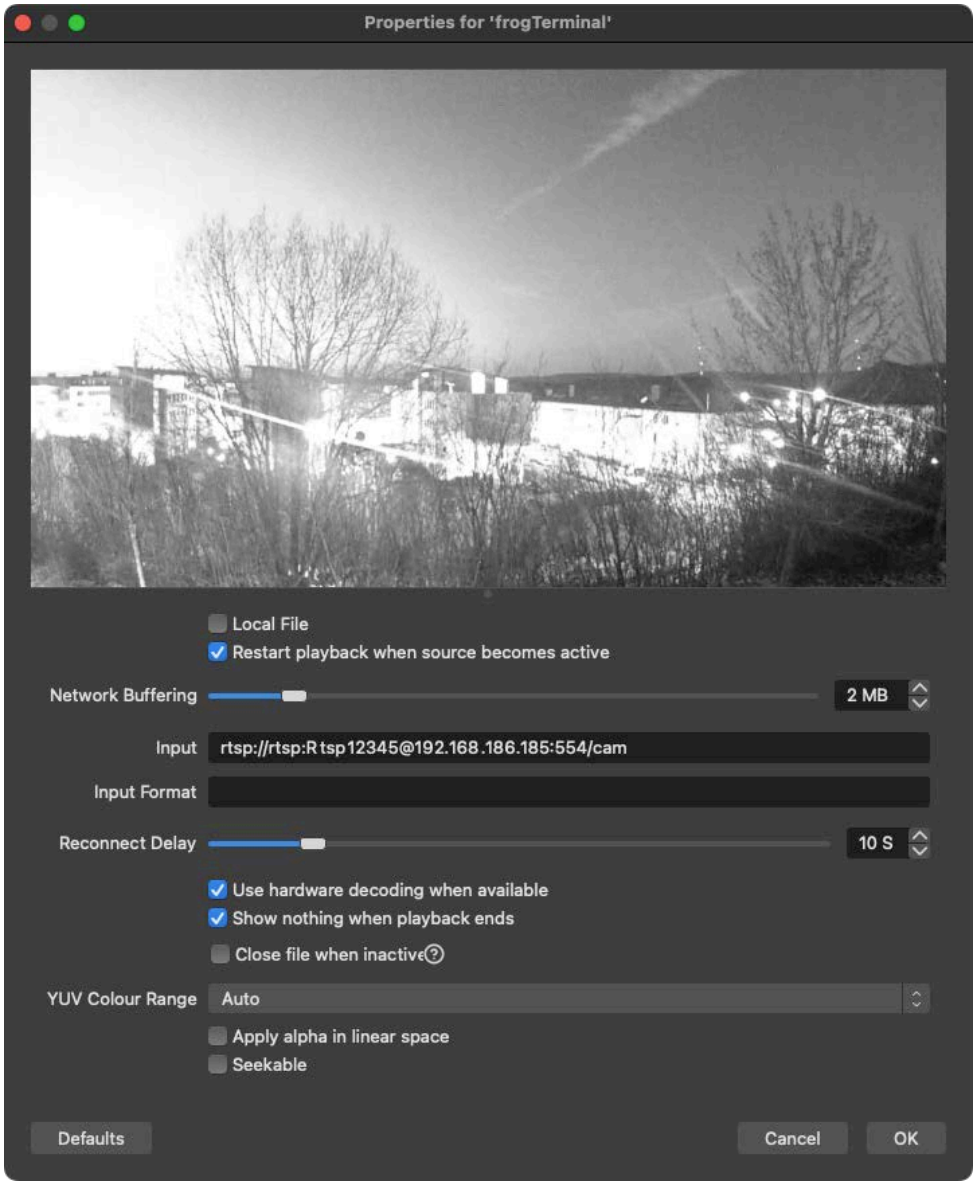

- Klicken Sie unter „**Sources**“ auf das Pluszeichen (+), um eine neue Videoquelle hinzuzufügen.



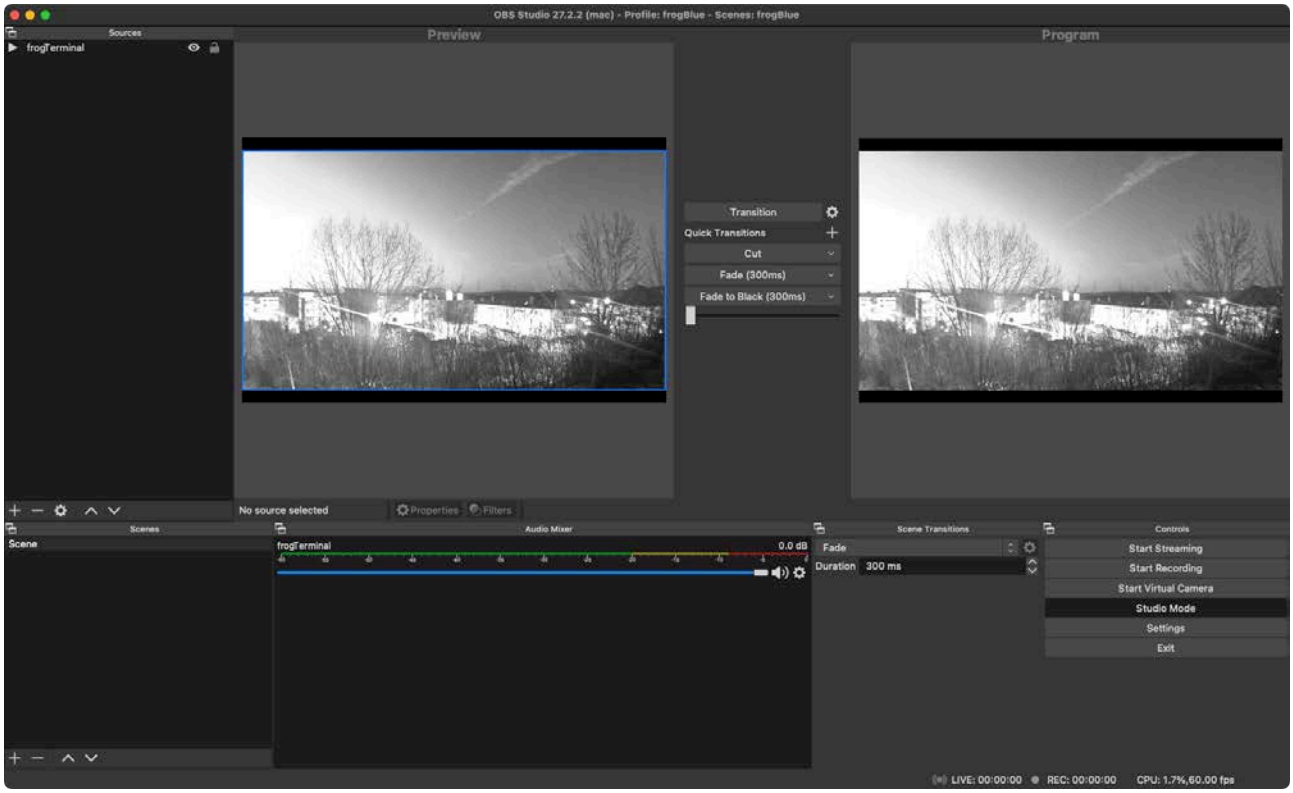

- Wählen Sie „**Media Source**“.




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



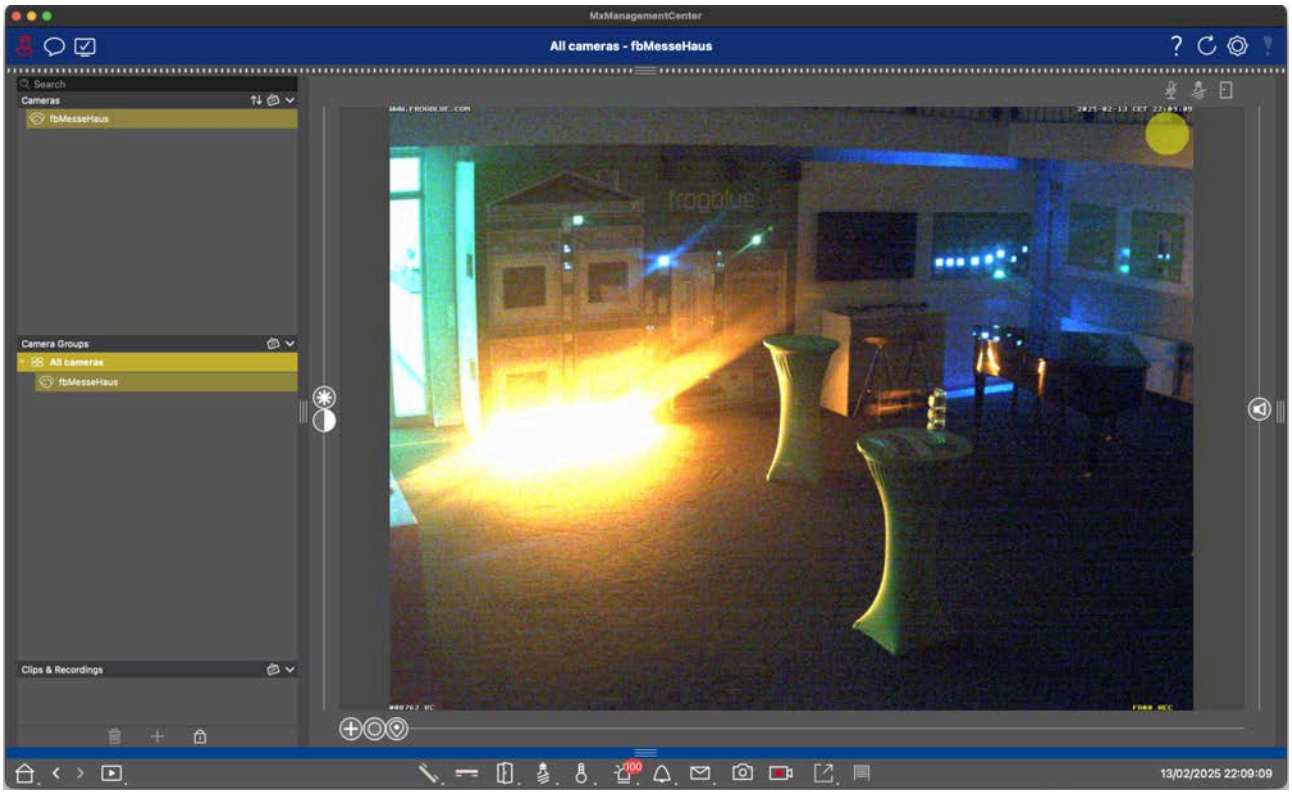
- Entfernen Sie das Häkchen bei „**Local File**“.
- Geben Sie die **RTSP-URL** ein. Der Benutzername und das Passwort können im HTTP-Format übermittelt oder im nächsten Schritt eingegeben werden.
- Setzen Sie ein Häkchen bei „**Use hardware decoding when available**“.
- Klicken Sie auf **OK**.



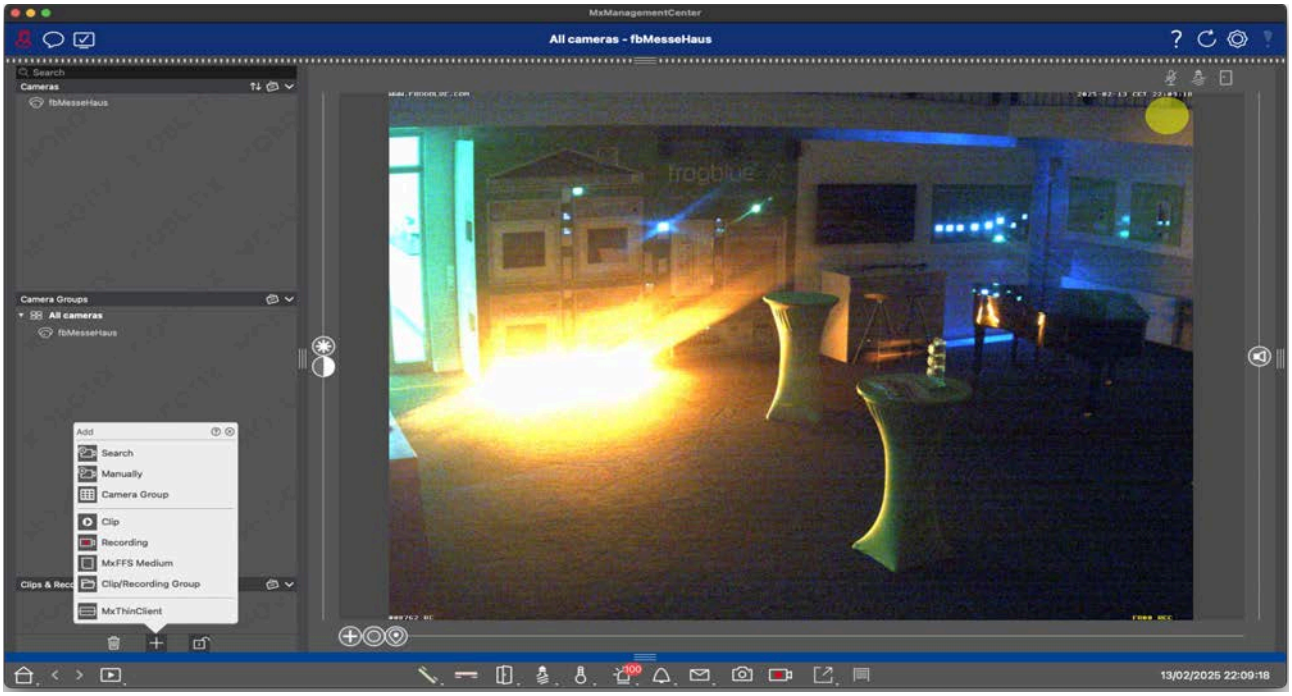

Der Livestream der frogTerminal-Kamera sollte nun in OBS Studio sichtbar sein.

**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.**

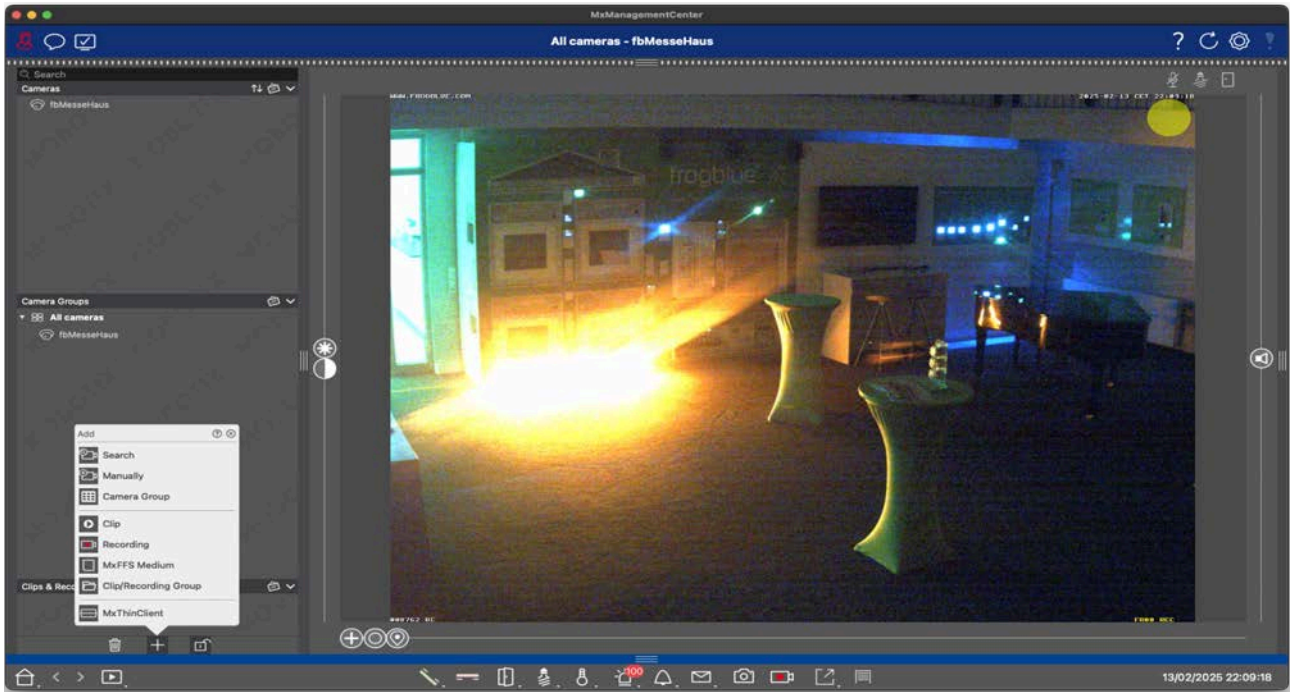
## 18.4. Integration mit MOBOTIX MxManagementCenter



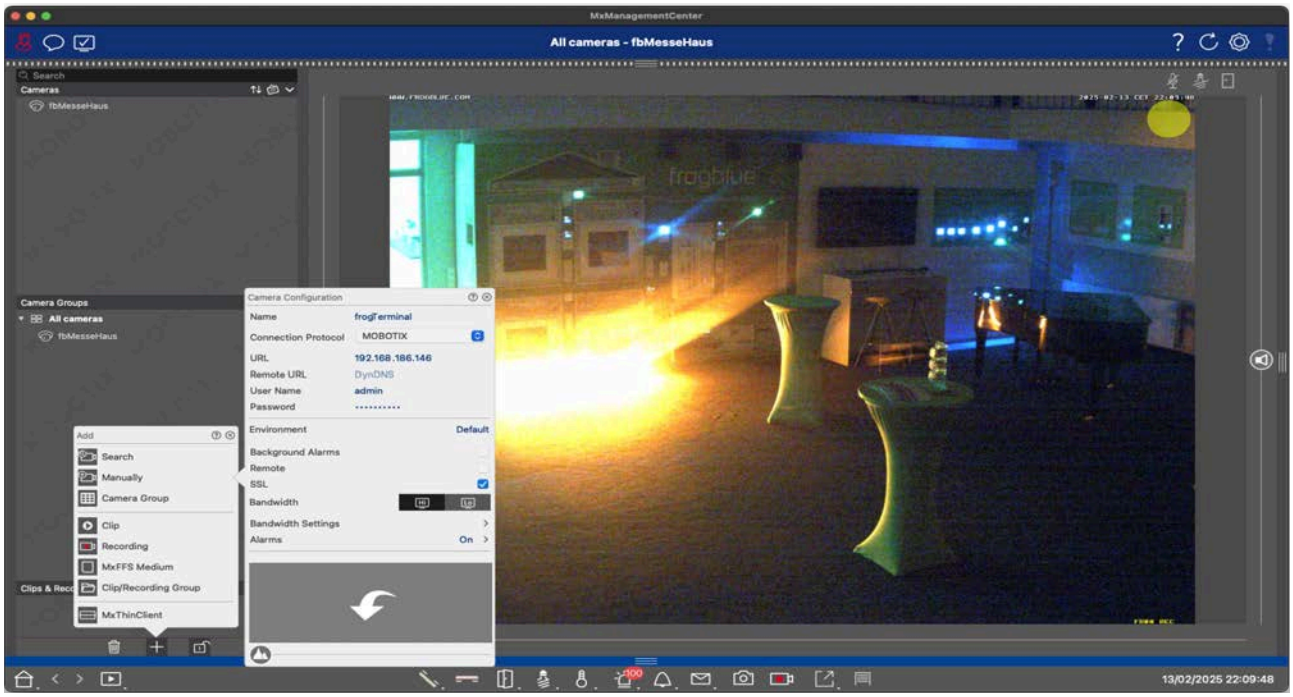

- Klicken Sie auf das Schloss-Symbol unten in der linken Seitenleiste, um die Oberfläche zu entsperren.



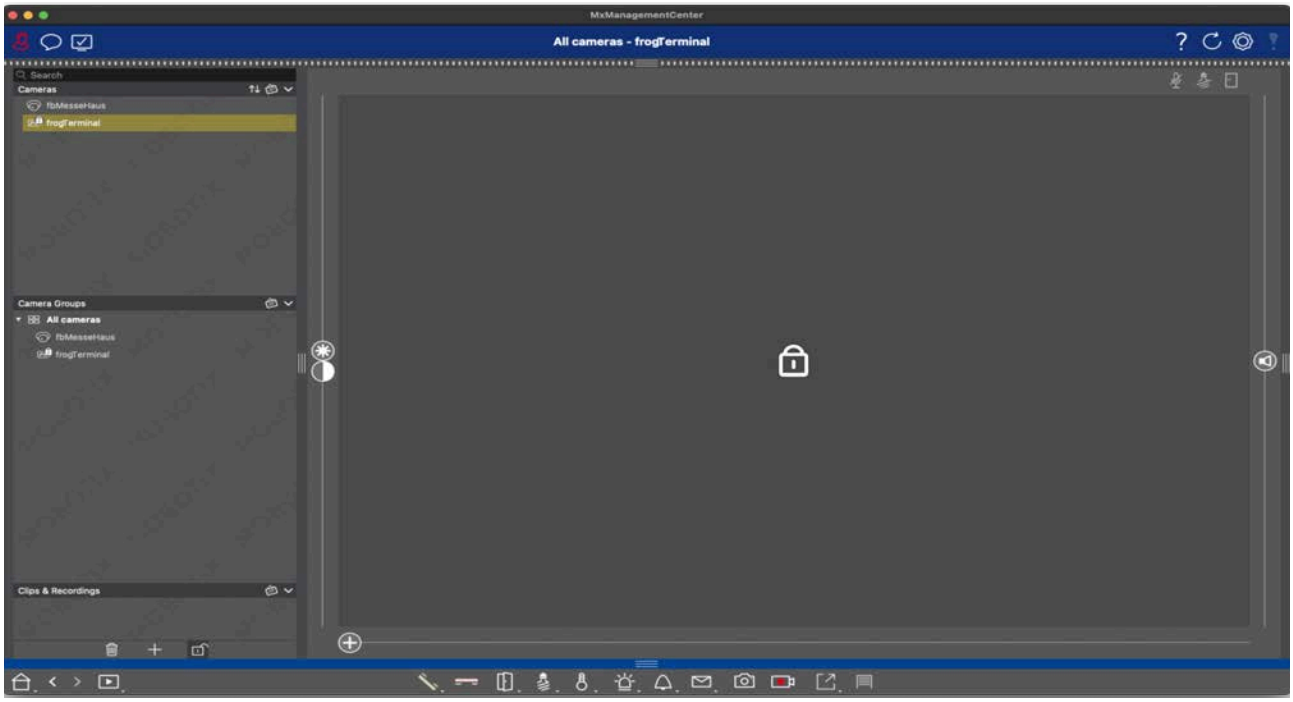

- Klicken Sie auf das „+“-Symbol unten in der linken Seitenleiste, um ein neues Element hinzuzufügen.



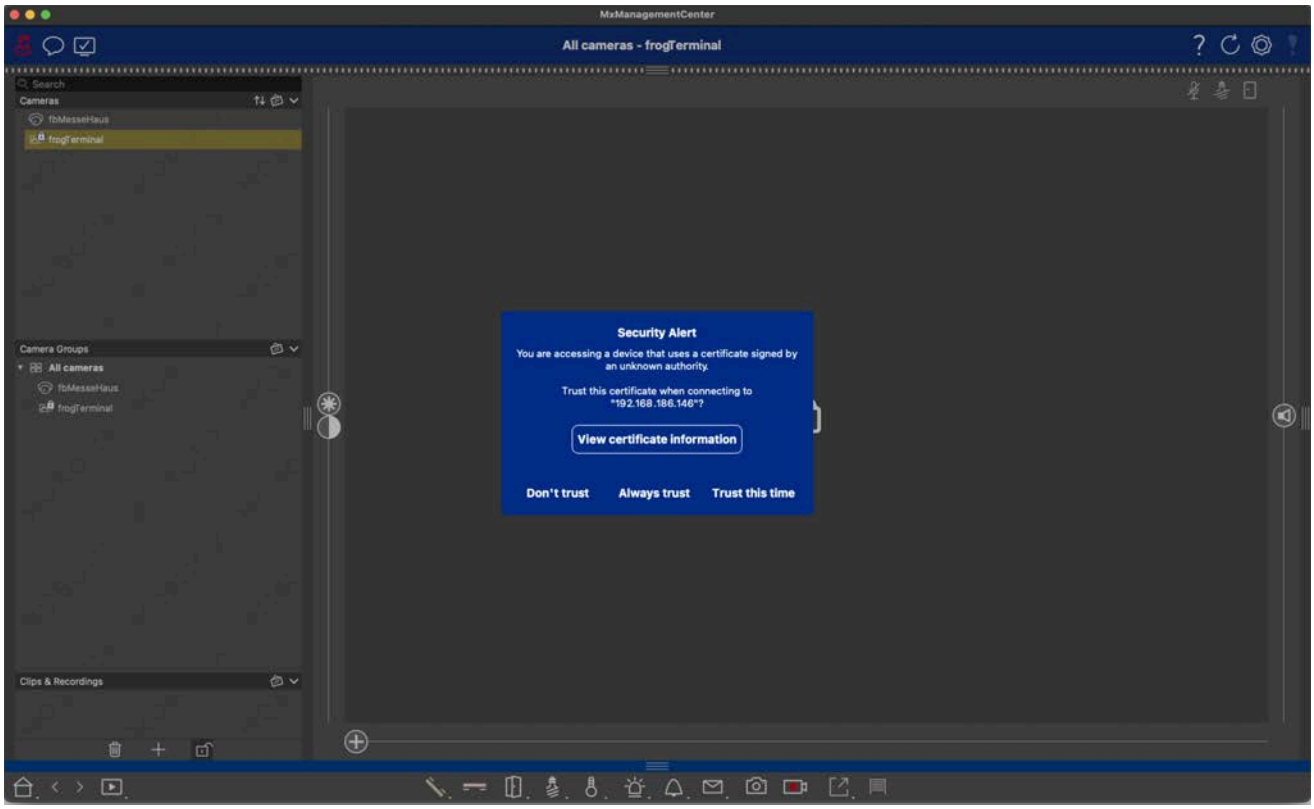

- Klicken Sie auf das Symbol „**Manually**“, um eine neue Kameraquelle hinzuzufügen.



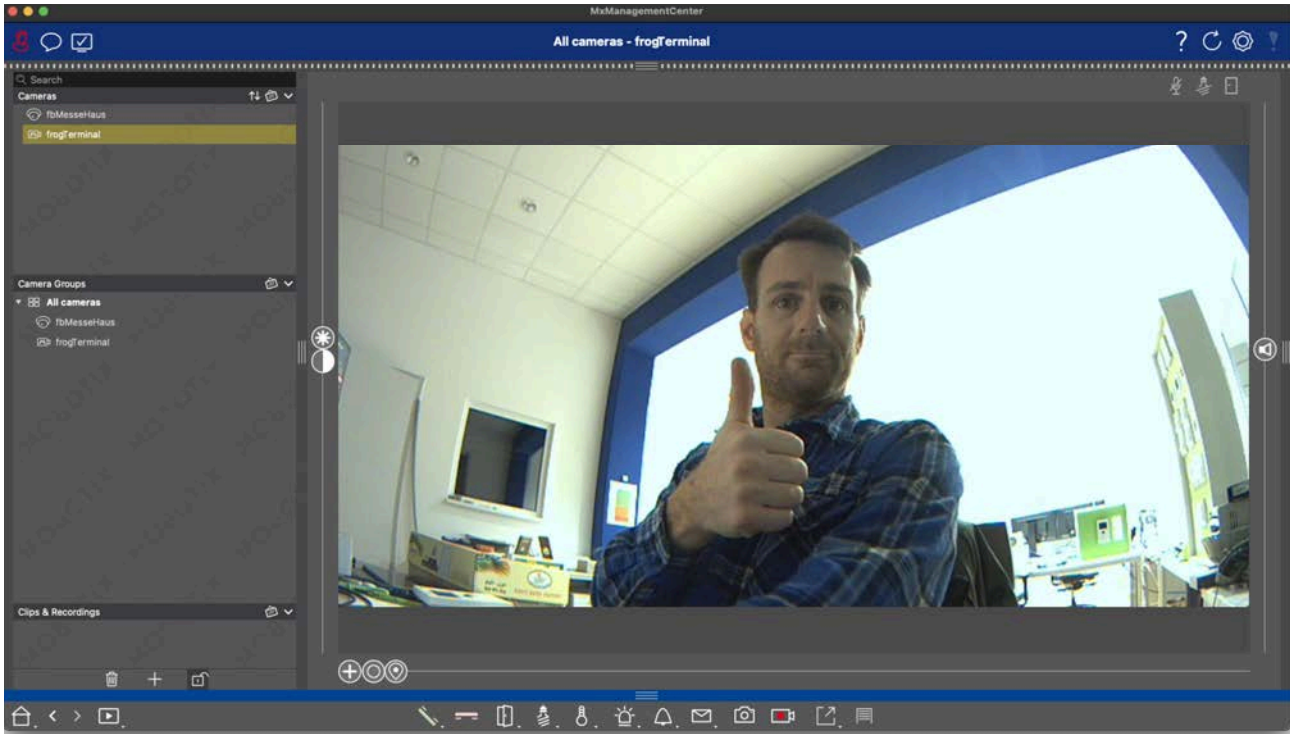

- „**Name**“: Geben Sie einen Namen für Ihr frogTerminal in MxCC ein.
- „**Connection Protocol**“: Wählen Sie „MOBOTIX“.
- „**URL**“: Geben Sie die IP-Adresse Ihres frogTerminals ein.
- „**User name**“: Geben Sie den Web-Benutzernamen für Ihr frogTerminal ein.
- „**Password**“: Geben Sie das Web-Passwort für Ihr frogTerminal ein.
- „**SSL**“: Aktivieren Sie das Kästchen, um eine gesicherte Verbindung zum frogTerminal zu ermöglichen (erforderlich).
- Klicken Sie außerhalb des Einstellungsbereichs, z.B. im grauen Bereich der linken Seitenleiste.




- Klicken Sie auf das Aktualisierungs-Pfeilsymbol oben rechts in der Oberfläche.




- Klicken Sie auf „Always Trust“ oder „Trust this Time“, um die Verbindung zu akzeptieren.




- Der Videostream des frogTerminals sollte in MxMC erscheinen.

# 19. Erweiterte Integration und API-Funktionen

**Hinweis: Spezialfunktionen! Sprechen Sie mit Ihrem frogblue-Partner oder dem lokalen frogblue-Kompetenzzentrum für Details.**

## 19.1. 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.

## 19.2. 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 Anwesenheits-protokolle 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, um.

# 20. Wartung und Fehlersuche

## 20.1. Firmware-Updates

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

## 20.2. Systemsteuerung – Konfigurationsdateien, Neustart und Werkseinstellungen

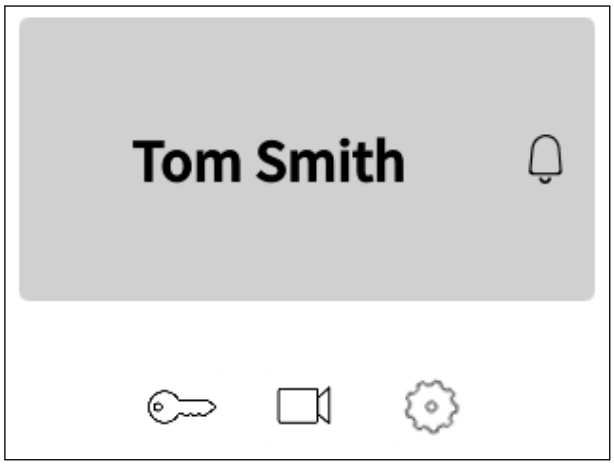
Dieser Abschnitt beschreibt, wie die gesamte Konfiguration herunter- oder hochgeladen, das System neu gestartet oder das Gerät auf Werkseinstellungen zurückgesetzt wird.

### Terminal über das Webinterface auf Werkseinstellungen zurücksetzen

**Menü: System → Systemsteuerung**

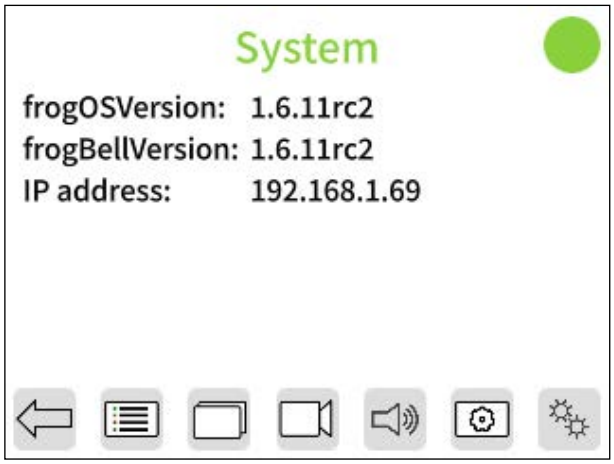
Um einen Werksreset durchzuführen, klicken Sie auf „Auf Werkseinstellungen zurücksetzen“ und dann auf „Ja“ zur Bestätigung. Warten Sie, bis im Browser die Meldung „Done“ erscheint und der Terminalbildschirm zum Begrüßungsbildschirm mit der Option „Start Wizard“ zurückkehrt. Bitte beachten Sie, dass der 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



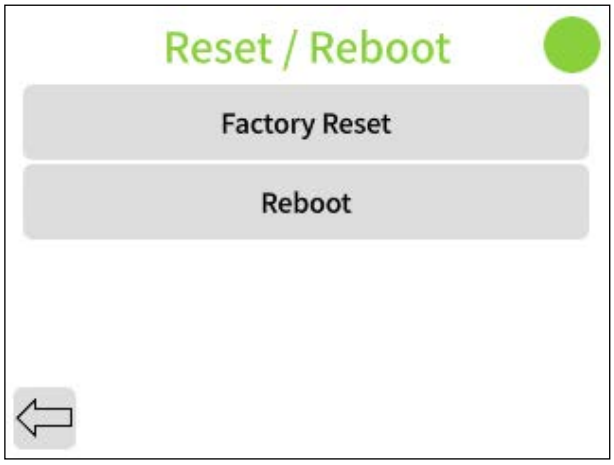

- Tippen Sie , um in den Konfigurationsmodus zu gelangen.


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

frogblue™

SMART BUILDING TECHNOLOGY GERMANY

Wir verknüpfen drahtlos via **Bluetooth®** 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® 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!



**Die Spezialisten für smarte Technologie und energieeffiziente Gebäudetechnik aus der Pfalz**