

HANDBUCH VESTA ALARMANLAGEN



Für Kunden von



Version 1.0, Stand 06.09.2024

Inhalt

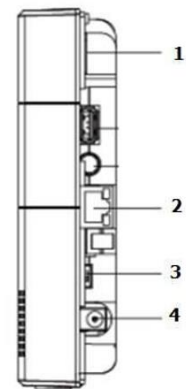
HANDBUCH	1
VESTA ALARMANLAGEN	1
1. VESTA HSGW Zentralen	3
Inbetriebnahme	3
Eigenschaften Alarm-Zentrale:	4
2. VESTA hybride Alarmzentralen (Funk und Kabel)	4
Merkmale Alarmzentrale:	4
3. Installation SmartHomeSec App	6
4. Alarm-Zentrale registrieren	6
5. Alarmzentrale programmieren	10
6. Bereich Sicherheit	12
7. Bereich Ereignis	13
8. Geräte hinzufügen / anlernen	14
8.1 Gerät / Sensor konfigurieren	15
8.2 Konfiguration der Zone. Interne Einstellungen	17
8.3 Gehtest	18
9. Geofencing einrichten	19
9.1 Geofencing Bereich festlegen	19
9.2 Szenario zum Scharfschalten der Alarmanlage erstellen	20
9.3 Szenario zum Unscharf-Schalten der Alarmanlage erstellen	22
9.4 Szenarien in der SmartHomeSec-App aktivieren	23
10. Einstellungen Zentrale	28
10.1 Sicherheit	29
10.2 Zentrale	31
10.3 Code	32
10.4 Datum und Uhrzeit	34
10.5 Werksrückstellung	35
10.6 FW-Aktualisierung	35
10.7 Konventionelle verdrahtete Zonen	37
10.8 NETZWERK-Einstellungen: GSM	39
10.9 NETZWERK-Einstellungen: GPRS	40
10.10 NETZWERK-Einstellungen: LORA	41
10.11 ARC-Verbindungseinstellungen: Ereignisse	42
10.12 ARC-Verbindungseinstellungen: Bilder	43

1. VESTA HSGW Zentralen



Inbetriebnahme

1. Legen Sie eine SIM-Karte (2G, 3G oder 4G) ein (1).
2. Verbinden Sie den Netzwerkport mit dem beiliegendem Netzkabel mit Ihrem Router oder einem Switch mit Internetzugriff (2).
3. Schalten Sie den Batterieschalter auf die Position ON (3).
4. Schließen Sie die Zentrale über das mitgelieferte Netzteil an (4).
5. Alle LEDs leuchten auf und nach 10-15 Sekunden ist das Gateway bereit.



Vista Lateral

Eigenschaften Alarm-Zentrale:

- IP (Ethernet) und 2G oder 4G
- 160 / 320 Zonen – 2 / 8 Bereiche - 240 Benutzer/Partition
- RF 868 MHz (2 km Reichweite) und Z-Wave (100- 200 m), Über Dongle optional auch ZigBee
- 100 Automatisierungsregeln
- 50 Szenen
- USB-Erweiterungssteckplatz: Zig-Bee, Wi-Fi, 3G / LTE, LoraWAN
- Eingebaute Sirene und Batteriepufferung
- EN-50131 Klasse 2
- Betriebsbedingungen: -10°C bis 45°C (14°F bis 113°F) Bis zu 85% nicht kondensierend

2. VESTA hybride Alarmzentralen (Funk und Kabel)



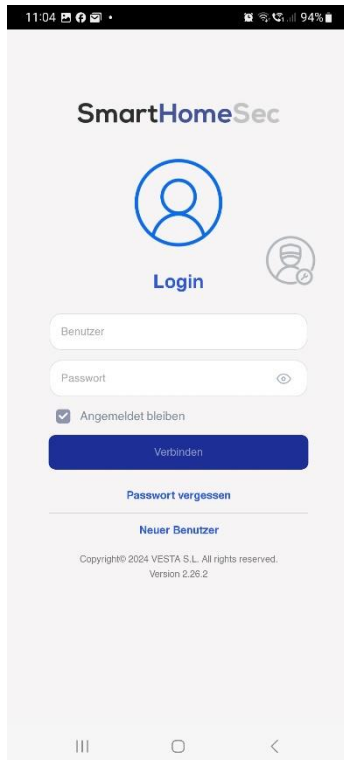
Merkmale Alarmzentrale:

- IP (Ethernet) und 2G oder 4G
- 640 Zonen - 8 Bereiche - 240 Benutzer/Partition
- RF 868 MHz (2 km Reichweite) und Z-Wave/ZigBee (100- 200 m)

- 100 Automatisierungsregeln
- 50 Szenarien
- ZigBee + Z-Wave integriert (VESTA-113N-SF1)
- USB-Erweiterungssteckplatz: Wi-Fi, LoraWAN
- RS485 BUS-Anschluss
 - Tastaturanschluss (Touch und/oder LCD)
 - Konventionelle Zonenexpander EOL, DEOL, 3EOL
 - BUS V-Max Volumetrics
 - PIR CAM BUS V-Max
 - Sirenen im BUS V-Max
 - V-Max BUS-Relaismodule
 - V-Max BUS-Isolatoren
 - V-Max BUS-Verstärker
 - Etc...
- Sirenen-Ausgang und PG-Ausgang
- Backup-Batterie (ist im Gehäuse zu verbauen, liegt Lieferung bei Alarmanlagen.PRO bei)
- EN-50131 Grad 3

3. Installation SmartHomeSec App

Über die SmartHomeSec App können Sie Ihre neue VESTA Alarmzentrale auf Ihrem Smartphone (iOS oder Android) einrichten und steuern. Die App bietet Ihnen viele Vorteile zur Steuerung Ihrer smarten VESTA Alarmzentrale.



Installation:

1. Rufen Sie den App-Store auf Ihrem iPhone oder Android-Smartphone auf.
2. Suchen Sie die App "SmartHomeSec"
3. Klicken Sie auf "installieren"
4. Starten Sie die App und geben sie ihr alle angeforderten Berechtigungen

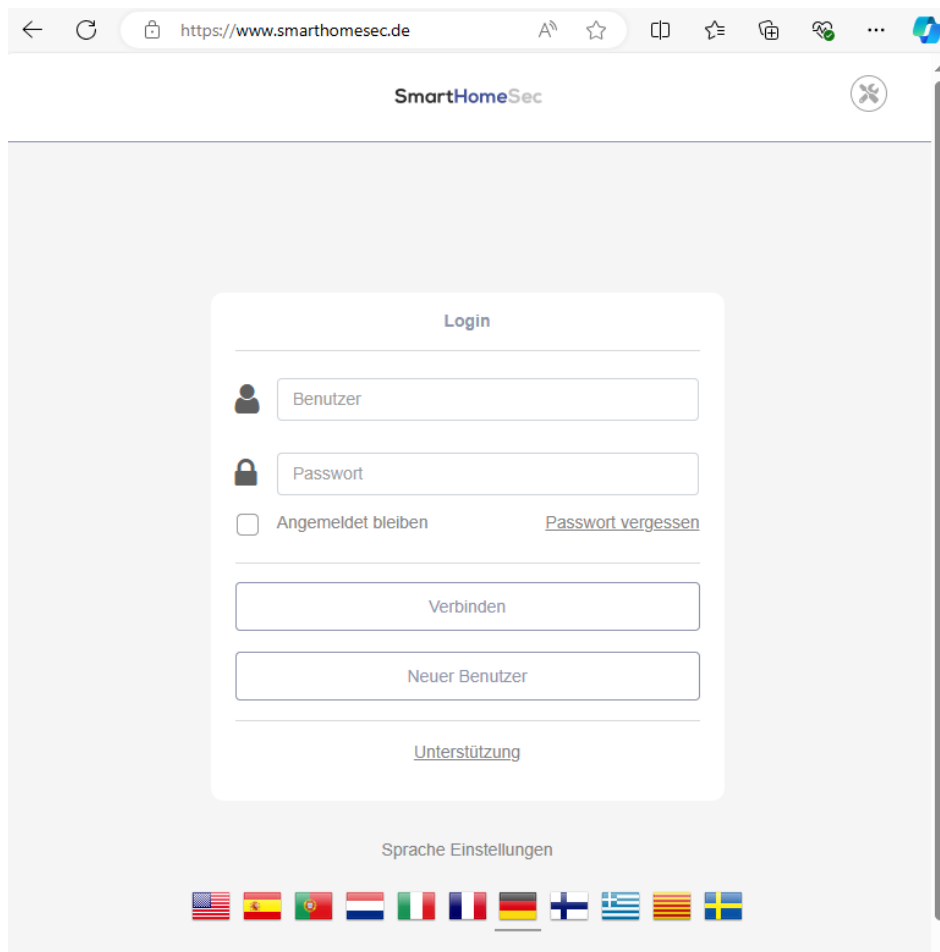
4. Alarm-Zentrale registrieren

In diesem Schritt beschreiben wir, wie Sie Ihr neues Alarmsystem in der SmartHomeSec-Verwaltung registrieren. Die SmartHomeSec ist die Schnittstelle zwischen Ihrer Alarmanlage und dem Internet. Über die Plattform können Sie immer auf Ihre Alarmanlage zugreifen. Sie benötigen dafür nur Zugriff aufs Internet.

SmartHomeSec

Rufen Sie die Plattform SmarHomeSec auf.

<https://www.smarthomesec.de>



Tip: Im unteren Bereich der Website können Sie die Sprache ändern. Klicken Sie auf die deutsche Landesfahne, um sich die Website in deutscher Sprache anzeigen zu lassen!

Haben Sie bereits einen Nutzer für Smarthomesec und wollen Sie die Zentrale als zweites System nutzen, können Sie sich jetzt mit Ihrem bestehenden Nutzeraccount anmelden.

Haben Sie noch keinen Benutzer für Smarthomesec, beschreiben wir in den folgenden Schritten wie Sie einen Nutzeraccount auf Smarthomesec erstellen..

Ersten Benutzer anlegen

1. Klicken Sie auf "First Time Registration" / "Neuer Benutzer"
2. Stellen Sie sicher, dass Ihre Alarmanlage eingeschaltet ist und Zugriff auf das Internet hat. Bestätigen Sie den entsprechenden Hinweis durch einen Klick auf "Next" / "Weiter"

3. Geben Sie im kommenden Schritt Ihre Kontaktdaten an. Die mit einem roten Stern versehenen Felder sind Pflichtangaben. Stimmen Sie den Nutzungsbestimmungen zu und klicken Sie auf "Next" / "Weiter"

Kontoinfo

* Zeigt das erforderliche Feld an.

Benutzer *	<input type="text" value="Max Mustermann"/>
Passwort *	<input type="password" value="••••••••"/>
Passwort bestätigen *	<input type="password" value="••••••••"/>
E-Mail *	<input type="text" value="email@alarmanlagenpro.de"/>
Landesvorwahl	<input type="text" value="Deutschland"/> <input type="text" value="49"/>
Mobiltelefon	<input type="text" value="0151123456789"/>
Festnetz	<input type="text" value="004972469447479"/>

Ich habe die folgende Dokumentation gelesen und stimme zu: [Nutzungsbedingungen](#)

4. Jetzt können Sie Angaben zu Ihrem Wohnort machen. Diese Angaben sind zunächst optional, dienen aber auch später für das sog. "Geofence" (Details dazu an späterer Stelle).

Alarmanlage registrieren

Ihre VESTA Alarmanlage wird über die MAC-Adresse und Ihrem Benutzeraccount im SmarHomeSec registriert.

Die zu Ihrer Alarmanlage passende MAC-Adresse ist auf einem Aufkleber vermerkt, der an Ihrer Alarm-Zentrale angebracht ist:



Übertragen Sie die MAC-Adresse in das Registrierungsformular der Smarthomesec-Plattform.

A screenshot of a web registration form titled "Registrierung". The form contains three main input areas: 1. "MAC" address, displayed as "00 : 1D : 94 : 15 : 28 : 4A" with each octet in its own small box. 2. "Zentralenname" (Central name) with a text input field containing "Test-Zentrale". 3. "Sprache Einstellungen" (Language settings) with a dropdown menu currently set to "Deutsch". At the bottom of the form, there are two buttons: "Zurück" (Back) on the left and "Senden" (Send) on the right.

Geben Sie der Zentrale dann noch einen Namen und stellen Sie die Sprache der Zentrale ein.

Mit einem Klick auf "Senden", schließen Sie die Registrierung ab.

Wichtig: Bitte denken Sie daran die E-Mail zu bestätigen, die Ihnen SmarHomeSec nach wenigen Minuten nach der Registrierung zusendet.

Sie können sich jetzt über die SmarHomeSec-App oder via Webbrowser durch Aufruf von

<https://www.smarthomesec.de>

am SmartHomeSec Portal mit den hier vergebenen Nutzerdaten anmelden und Ihre VESTA Alarmanlage verwalten.

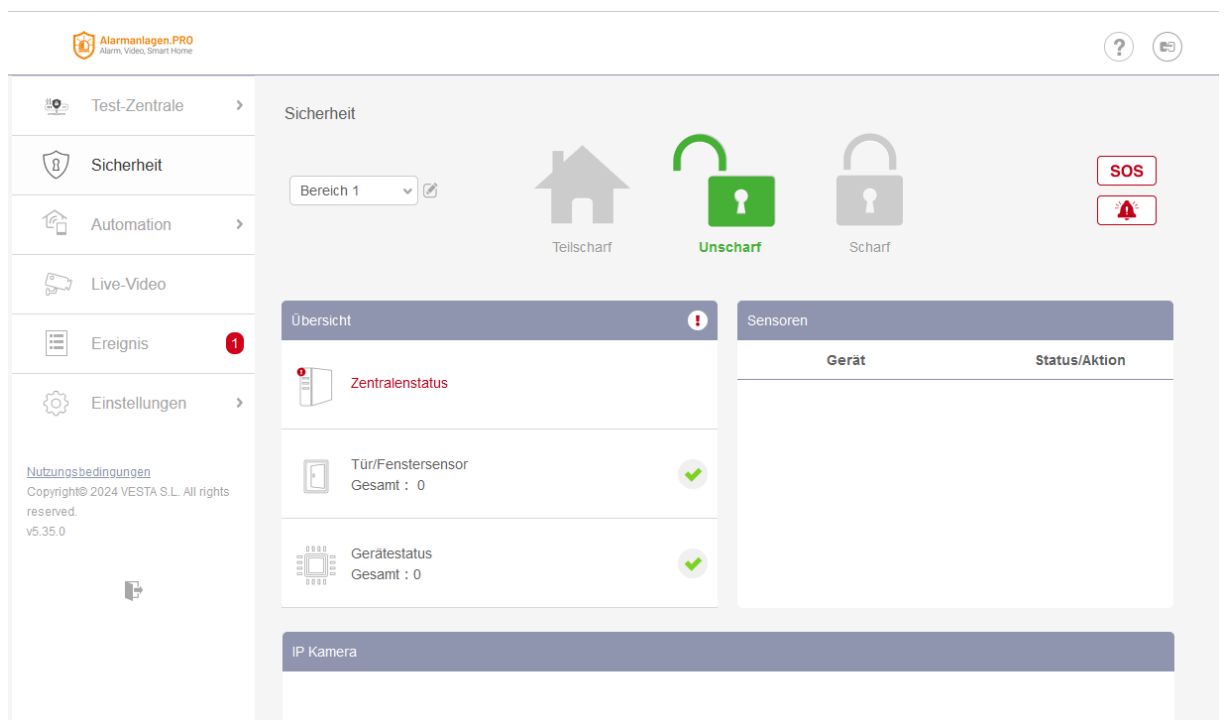
5. Alarmzentrale programmieren

Zur Vereinfachung dieses Handbuchs beziehen sich ab jetzt alle Informationen und Abbildungen auf die WEB-Plattform Smarthomesec.de! Aufgrund der großen Ähnlichkeit zwischen der APP- und der WEB-Plattform wird es als nicht notwendig erachtet, auf die gleichen und doppelten Informationen zu bestehen.

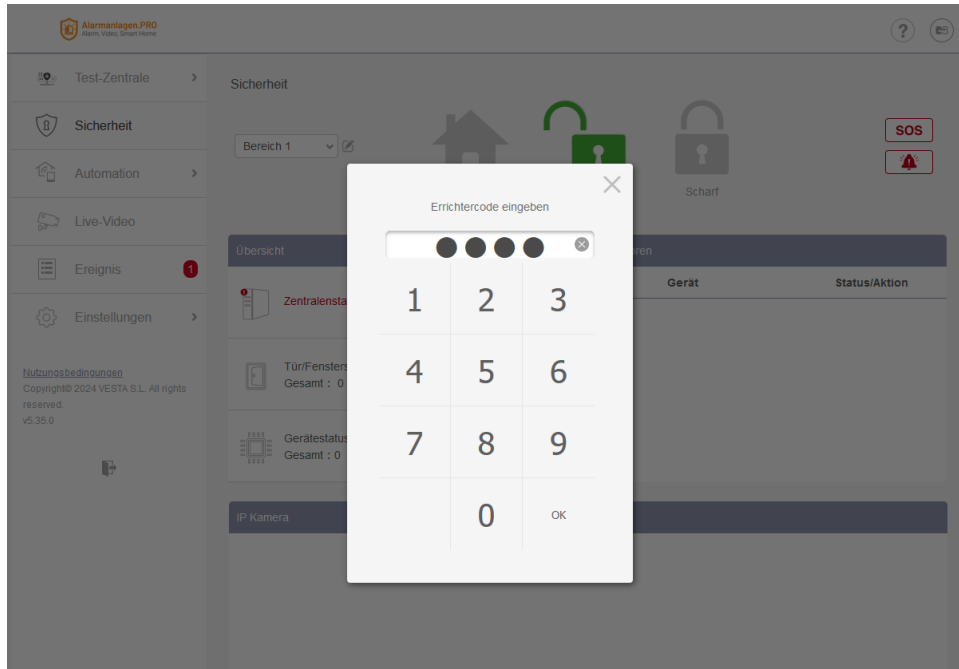
1. Melden Sie sich auf der SmartHomeSec-Website an:

<https://www.smarthomesec.de>

2. Melden Sie sich mit Ihrem registrierten Benutzernamen und Kennwort bei Ihrem Nutzerkonto an.



3. Klicken Sie auf Einstellungen
4. Errichter-Code einfügen, Werkseinstellung **7982**

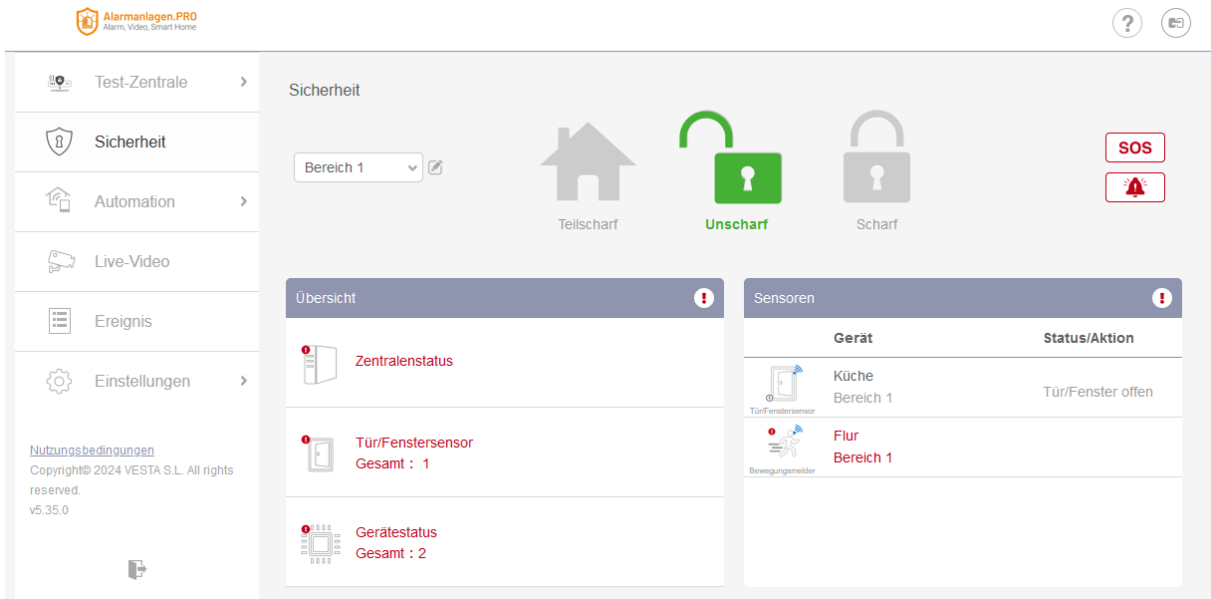


Sie haben jetzt Zugriff auf die Einstellungen. Ab Kapitel 8 erklären wir die einzelnen Einstellungen.

Hinweis: Es passiert, dass Sie immer aufs Neue den Errichter-Code eingeben müssen. Bitte merken Sie sich diesen Code. In Kapitel 10, erklären wir, wie der Errichter-Code und andere Codes geändert werden können.

6. Bereich Sicherheit

Von hier aus haben Sie einen Überblick über den aktuellen Status des Systems auf technischer Ebene (technische Störungen der Zentrale oder der Geräte), die rot hervorgehoben werden. Darüber hinaus können Sie überprüfen, ob die Bereiche der Zentrale scharf oder unscharf geschaltet sind.



Gerät	Status/Aktion
Küche Bereich 1 Tür/Fenstersensor	Tür/Fenster offen
Flur Bereich 1 Bewegungsmelder	

Zudem können Sie Ihre VESTA Alarmanlage Teilscharf, Unscharf oder Scharf schalten. Wählen Sie zunächst den Bereich aus und dann die Aktionen.

Hinweis: Ihre Alarmzentrale unterstützt (je nach Modell) 2 – 8 Bereiche. Ein Bereich ist als Einheit zu sehen. Zum Beispiel Haus, Büro, Einliegerwohnung usw...

- **Teilscharf:** Nur ein Teil der Sensoren des ausgewählten Bereichs ist scharf geschaltet. Dieser Modus ist sinnvoll, wenn Sie Zuhause sind, aber die Türen und Fenster sichern möchten, so dass Sie einen Einbruch mitbekommen. Bewegungsmelder sollen aber abgeschaltet sein, da Sie sich ja im Haus aufhalten.
- **Unscharf:** Der komplette Bereich ist unscharf. Nur Rauch und Wassermelder sowie Gasmelder reagieren auf Alarm.
- **Scharf:** Der komplette Bereich ist scharf. Alle aktiven Sensoren und Melder reagieren auf ein Alarmereignis (**Beachten Sie Kapitel 8 zu den Einstellungen der Sensoren**).

7. Bereich Ereignis

Im Bereich Ereignisse werden alle von der Zentrale erzeugten Ereignisse gespeichert und für einen Zeitraum von ca. 1 Monat angezeigt (abhängig vom System maximal 500 Ereignisse), darunter: Scharfschalten, unscharf schalten, technische Störungen, technische Alarme, Einbruchalarm.

The screenshot shows the 'Ereignis' (Event) section of the VESTA Alarmanlagen.PRO interface. The sidebar on the left contains navigation options: Test-Zentrale, Sicherheit, Automation, Live-Video, Ereignis (selected), and Einstellungen. The main content area displays a table of events for the date 06/09/2024. The table has columns for 'Ereignistyp', 'Bereich', 'Zeit', and 'Quelle'. The events listed are:

06/09/2024	Ereignistyp	Bereich	Zeit	Quelle
•	Zurücksetzen	Bereich 1	15:19:45	Flur (Zone 2)
•	Unscharf ferngesteuert	Bereich 1	15:19:45	user
•	Einbruchalarm	Bereich 1	15:18:33	Flur (Zone 2)
•	Scharf ferngesteuert	Bereich 1	14:32:34	Home Automation
•	Sabotage	Bereich 1	14:15:55	Flur (Zone 2)
•	Batterie fehlt/leer		13:49:18	System

Es steht eine Suchmaske zur Verfügung, mit der Sie Suchfilter nach Alarmbildern, Alarmereignissen oder nach Datum anwenden können.

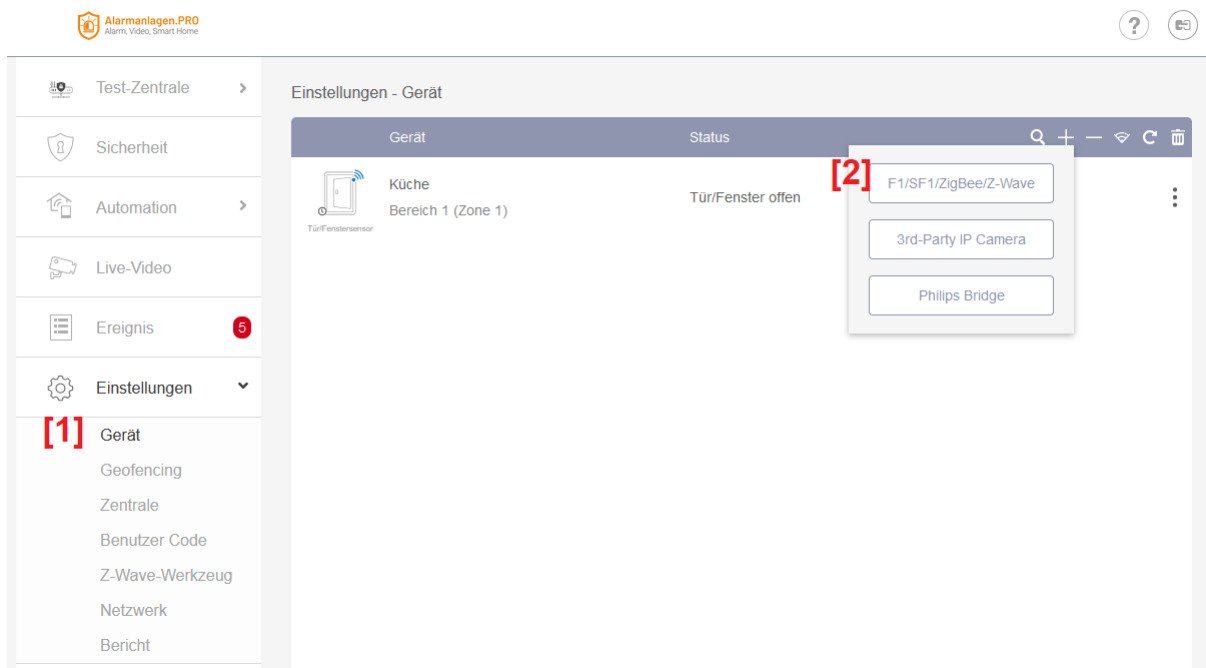
8. Geräte hinzufügen / anlernen

Hier beschreiben wir, wie Sie einen Sensor / ein Gerät hinzufügen

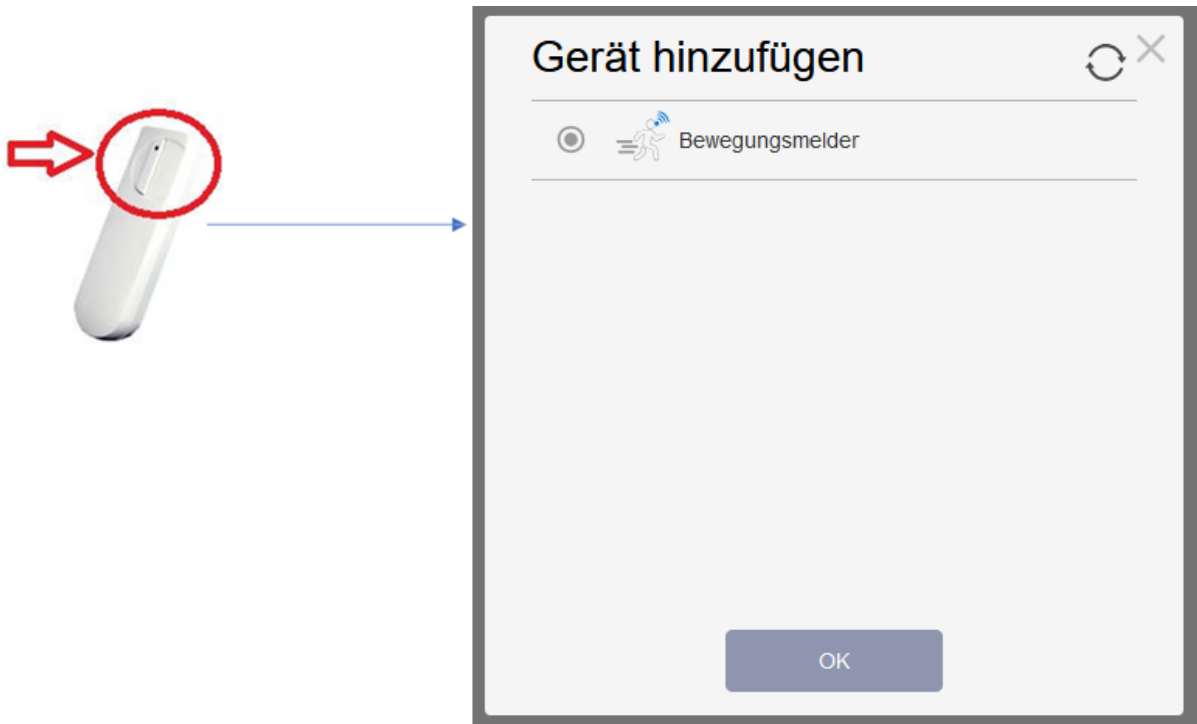
1. Klicken Sie auf Einstellungen
2. Geben Sie, wenn erforderlich, nochmal den Installer-Code (Standard 7982) ein
3. Klicken Sie auf + **[2]**
4. Wählen Sie den Typ aus. Für normale VESTA-Sensoren wählen Sie bitte

F1/SF1/ZigBee/Z-Wave

Die Zentrale schaltet in den Lernmodus und wartet auf Zuweisungssignale.




1. Drücken Sie die Taste des Geräts, das Sie hinzufügen möchten. Beispiel: DC-16SL Magnetkontakt. Sobald das Gerät auf dem Bedienfeld erkannt wird, wählen Sie es aus und bestätigen Sie mit OK.



Hinweis! Jeder Melder verfügt über eine spezielle Taste zur Anmeldung des Geräts. Schauen Sie in Ihrem spezifischen Handbuch nach, um sicherzustellen, dass Sie die richtige Taste auf die richtige Weise drücken.

2. Wählen Sie Bereich, Zone und vergeben Sie einen Namen für die Zone. Das Gerät ist nun erfolgreich zum Panel hinzugefügt worden

Geräteinfo

 Bewegungsmelder

Bereich

Zone

Gerätename

8.1 Gerät / Sensor konfigurieren

So konfigurieren Sie ein Gerät:

Menü aufrufen: Einstellungen -> Gerät

The screenshot displays the 'Ajuste - Dispositivo' (Device Settings) screen in the VESTA application. The left sidebar contains navigation options: Hybrid, Seguridad, Automatización, Evento, and Ajuste (1). The 'Ajuste' option is selected, and 'Dispositivo' is highlighted. The main content area shows a list of devices in 'Area 1' with columns for 'Dispositivo' and 'Estado'. The 'PIR CABLEADO' device is highlighted with a red box, and its settings icon (three dots) is also highlighted with a red box and a red '2'.

Dispositivo	Estado
AVISO de ARMADO Area 1 DIO52 (DO)	OFF
PIR CABLEADO Area 1 IR	
DH:6H0C0A8PAG853E1 Area 1 Cámara IP	
Sensor ambiente Area 1 Sensor de calidad d...	
Switch luces Area 1 Medidor de interrump...	Apagado , 0.0 W , Total » 0.0 kWh
PIR CAM Ext Area 1 Vista exterior	
DIMMER Area 1	Apagado , 0% , 0.0 W , Total » 0.0 kWh

Hinweis! Jeder Melder hat je nach seiner Art unterschiedliche Einstellungen. Im Folgenden finden Sie eine Zusammenfassung der allgemeinen Einstellungen für einen PIR-Melder

8.2 Konfiguration der Zone. Interne Einstellungen

The screenshot shows the 'Einstellungen - Gerät' (Device Settings) screen for a 'Tür/Fenstersensor' (Door/Window Sensor) in the 'Küche' (Kitchen) area. The interface includes a left sidebar with navigation options like 'Sicherheit', 'Automation', 'Live-Video', 'Ereignis', and 'Einstellungen'. The main content area is titled 'Küche Einstellungen' and contains various configuration options for the sensor.

Gerät

- Geofencing
- Zentrale
- Benutzer Code
- Z-Wave-Werkzeug
- Netzwerk
- Bericht

Küche Einstellungen

Tür/Fenstersensor

Bereich: Bereich 1

Zone: 1

Name: Küche

Übergehen: Aus

Must be Closed: No

Bypass Manipulation: Aus

Bypass Supervision: Aus

Auto Bypass: Deaktivieren

Activation: 1

Min.: 2

24 Std.

Einbruchalarm

Unscharf Reaktion: Klingel

Scharf Reaktion: Start Eingangsverzögerung 1

Zuhause 1 Reaktion: Start Eingangsverzögerung 1

Verlassen

Keine Reaktion

Aktiv-Zustand: Keine Reaktion

OK-Zustand: Keine Reaktion

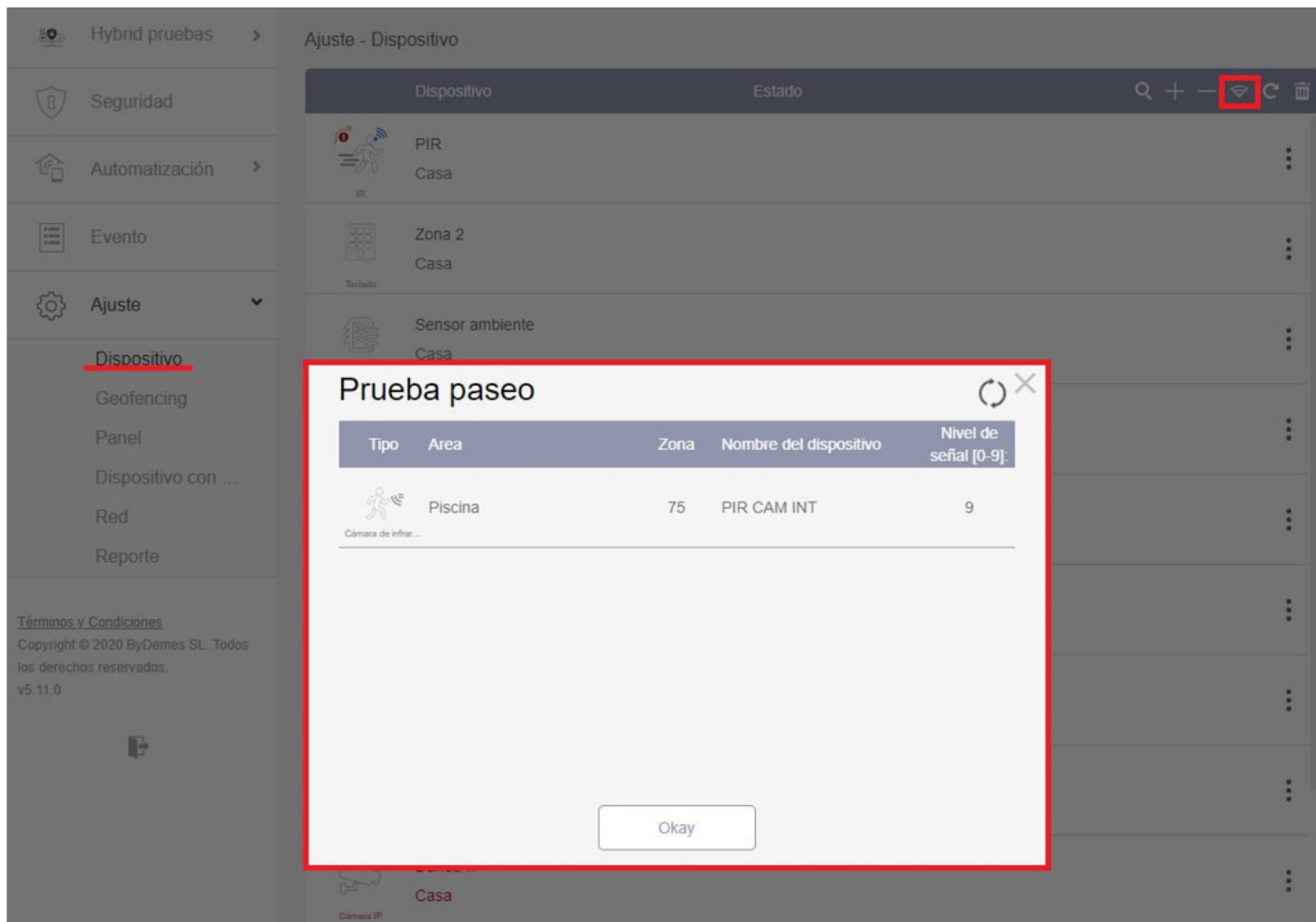
Zurück Senden

1. Wählen Sie Bereich [1/2/3/4/5/6/7/8].
2. 24. Std.: Soll der Sensor dauerhaft Alarm auslösen. Diese Einstellung ist bei einem Rauch oder Wassermelder zu wählen.
3. Wählen Sie eine Zonennummer aus [1-80].
4. Vergeben Sie einen Zonennamen ["Bewegungsmelder Küche"].
5. Umgehung der Zone ON Anular
 - a. Bypass OFF Habilitar zone
6. Aufhebung der Sabotage ON/OFF
7. Überwachung der Bypass-Zone
8. 24h Zone
9. Zonenreaktion mit Panel Unscharf
10. Zonenreaktion mit Scharfschaltung
11. Zonenreaktion bei der Hausscharfschaltung
 - a. Nicht handeln
 - b. Eingangsverzögerung 1
 - c. Eingangsverzögerung 2
 - d. Türklingel
 - e. Verfolgungsalarm
 - f. Sofortiger Alarm
 - g. Außenalarm
 - h. Stiller Alarm
 - i. Überquerter Bereich

12. Szene bei Alarm / Auslösen anwenden
13. Szene beim Wiederherstellen anwenden

8.3 Gehtest

Das Starten eines Lauftests prüft die Signalstärke, mit der die Zonen per Funk übertragen. So können Sie vor einen Bewegungsmelder laufen und prüfen, ob Bewegung erkannt wird.



Hinweis! Drücken Sie die Einlerntaste auf die gleiche Weise wie bei der Zuordnung des Gerätes. Die Signalstärke wird dann in einem Bereich von 0 bis 9 angezeigt. Wir empfehlen Stärke => 4 oder niedriger, wenn ein stabiles Signal über längere Zeit erhalten bleibt.

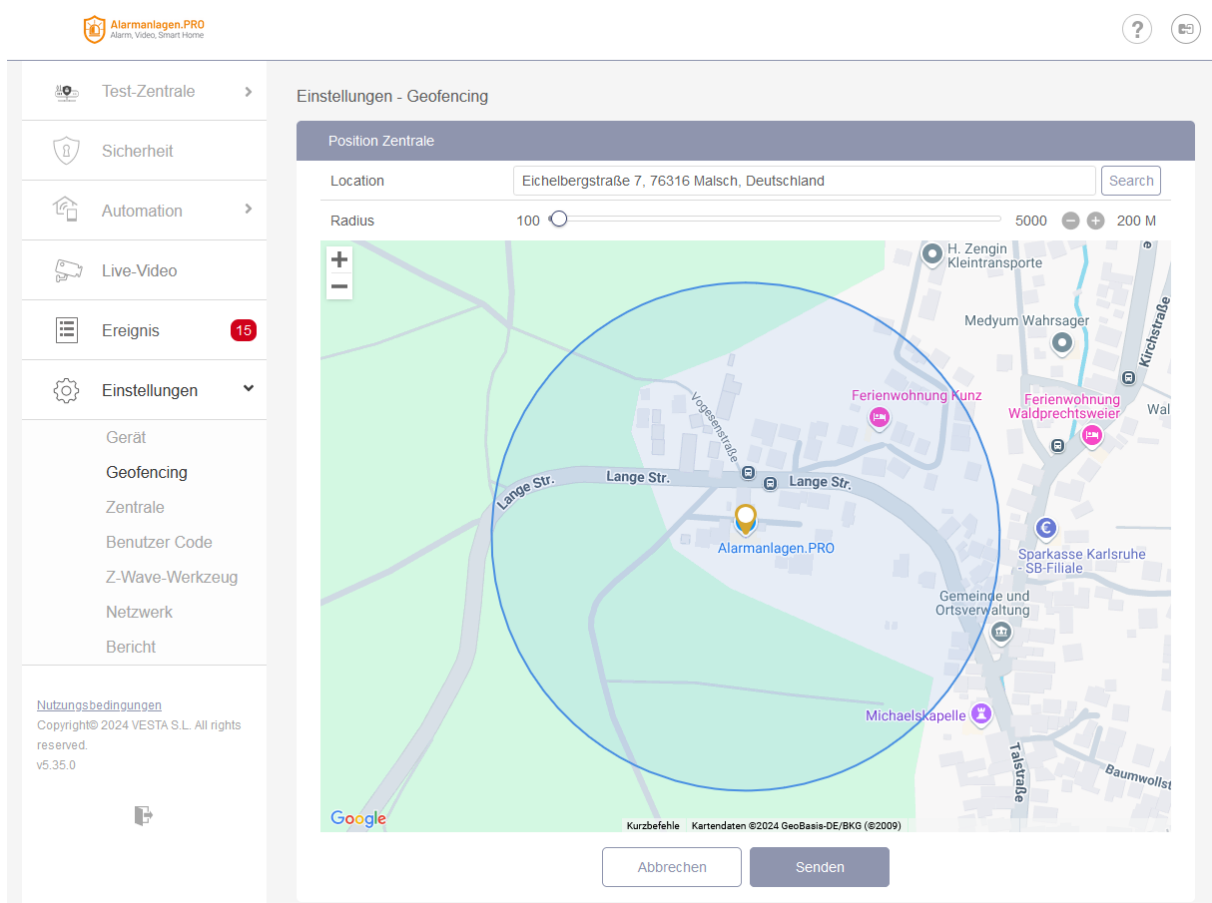
9. Geofencing einrichten

Ihre VESTA-Alarmanlage unterstützt zusammen mit Ihrem Smartphone und der SmartHomeSec-App Geofencing. Das bedeutet, die Alarmanlage schaltet scharf, wenn Ihr Smartphone einen vorgegebenen Bereich um Ihrem Haus verlässt.

So richten Sie Geofencing auf Ihrer VESTA-Alarmanlage ein:

9.1 Geofencing Bereich festlegen

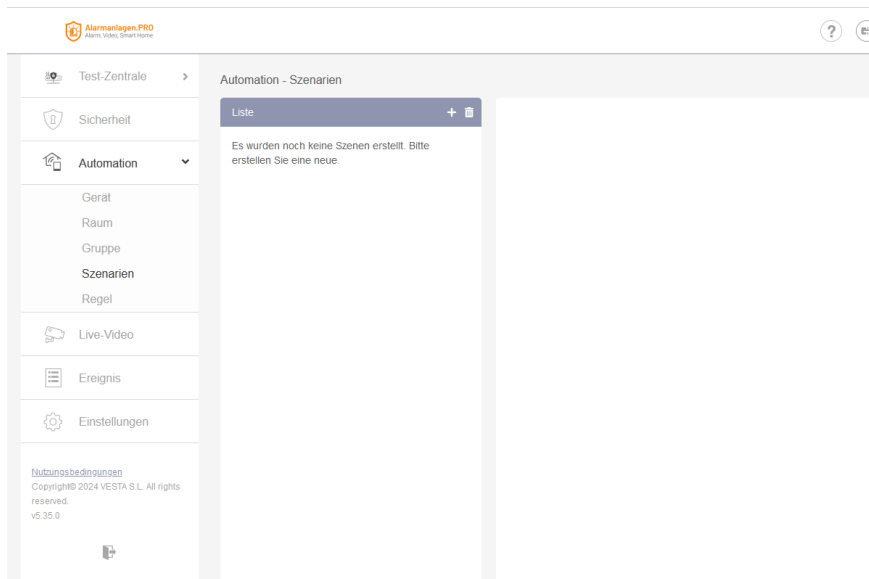
1. Rufen Sie **Einstellungen -> Geofencing** auf.
*Erinnerung: Der Erichtercode in der Grundeinstellung lautet **7982***
2. Suchen Sie Ihre Adresse unter Location (Ort, Straße, Hausnummer)
3. Stellen Sie einen gewünschten Radius, Beispiel 100 Meter, ein.
4. Klicken Sie auf "Senden"



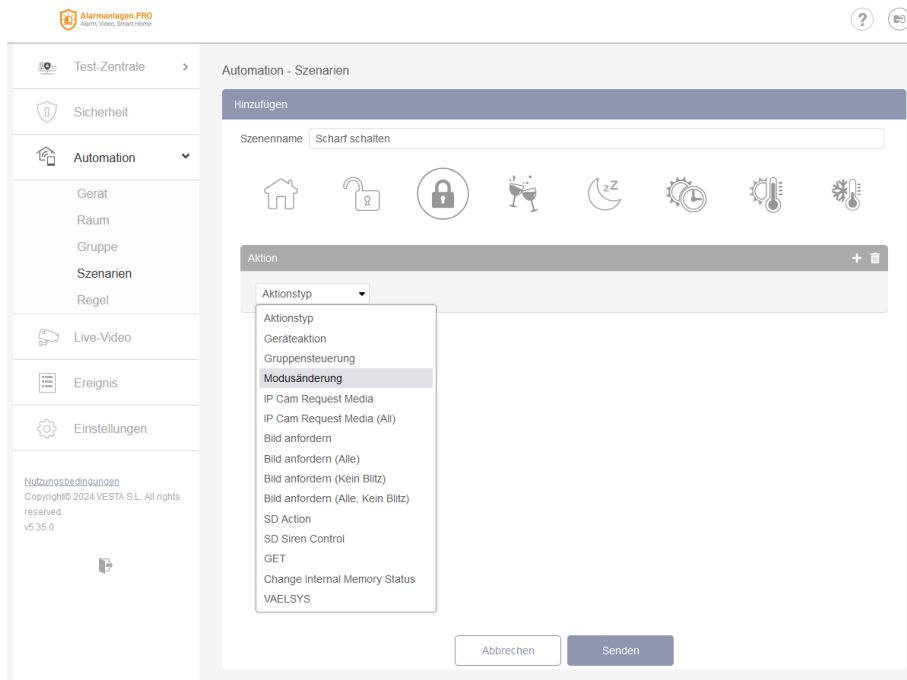
9.2 Szenario zum Scharfschalten der Alarmanlage erstellen

Nun benötigen wir ein Szenario für Ihre VESTA-Alarmanlage, dass diese scharf schaltet.

1. Rufen Sie **Automation -> Szenarien** auf

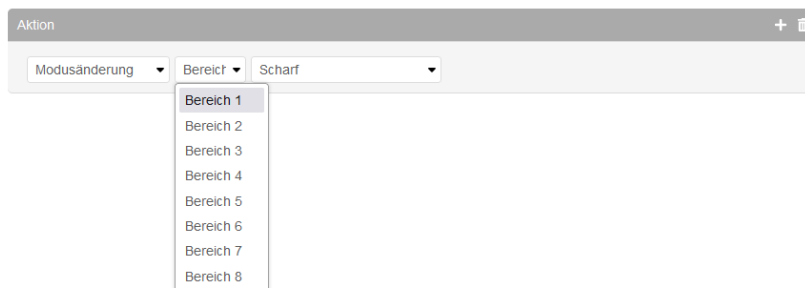


2. Klicken Sie auf das Icon **+**
3. Geben einen Szenennamen an, zum Beispiel "scharf schalten"
4. Wählen Sie dazu ein passendes Icon, Beispiel ein Schloss das geschlossen ist
5. Wählen Sie unter Aktionstyp, **Modusänderung** aus.



6. Unter der Annahme, dass Sie Bereich 1 scharfschalten wollen geben Sie jetzt folgendes an:

Modusänderung + Bereich 1 + Scharf



Hinweis: Sollen weitere Bereiche scharf schaltet werden, können Sie durch einen Klick auf das + , auch für weitere Bereiche ein die Scharfschaltung ermöglichen.

Aktion +

Modusänderung ▼ Bereich ▼ Scharf ▼

Modusänderung ▼ Bereich ▼ Scharf ▼

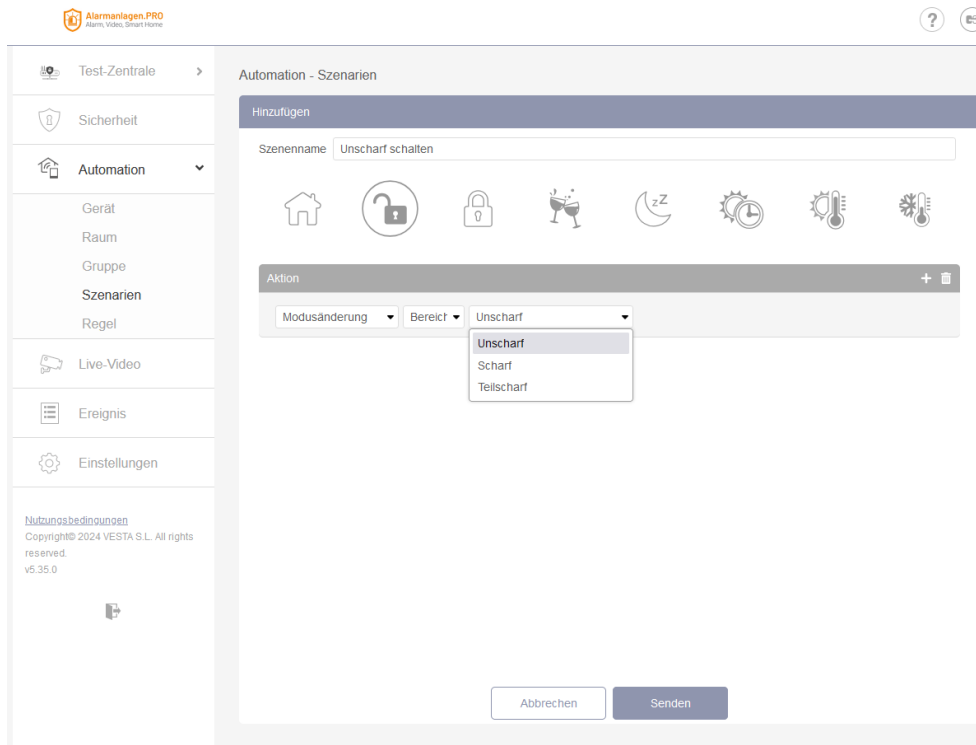
- Bereich 1
- Bereich 2**
- Bereich 3
- Bereich 4
- Bereich 5
- Bereich 6
- Bereich 7
- Bereich 8

7. Klicken Sie anschließend auf “Senden”, um die Szene zu speichern.

9.3 Szenario zum Unscharf-Schalten der Alarmanlage erstellen

Jetzt bedarf es noch ein Szenario, um Ihre VESTA-Alarmanlage unscharf zu schalten.

Hier gehen wir wie im **Abschnitt 9.2** vor, wählen allerdings als Aktion “Unscharf aus”



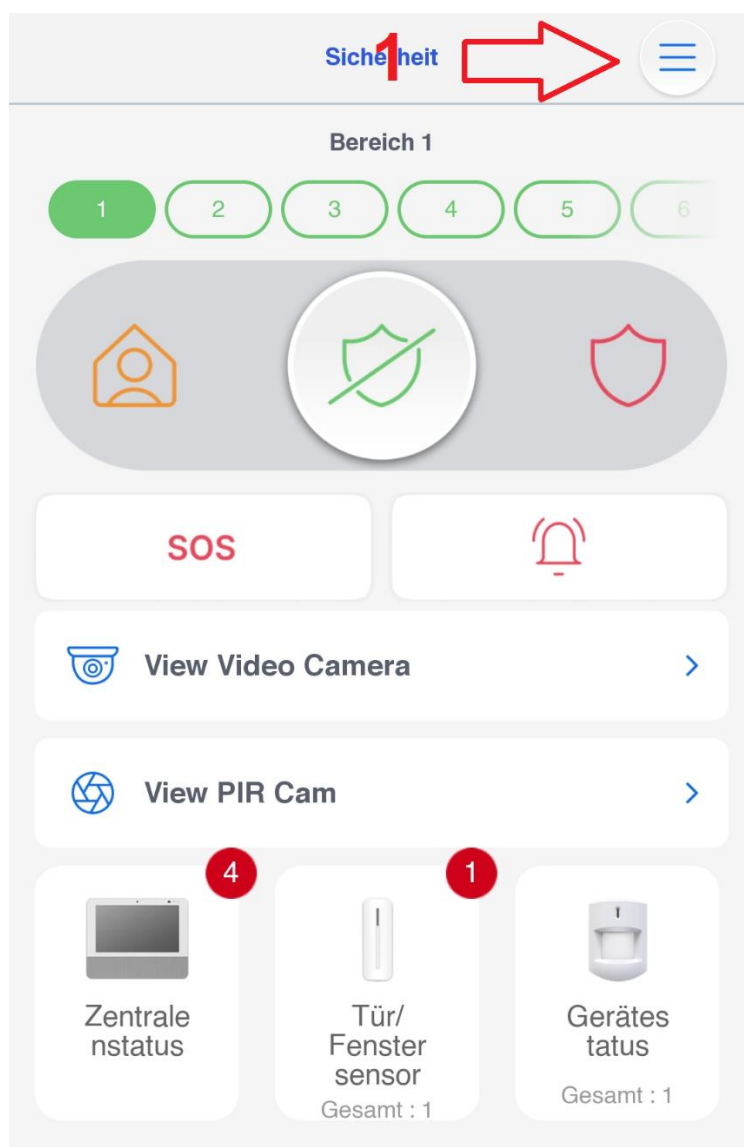
Vergeben Sie natürlich hier einen passenden Namen und als Icon zum Beispiel das geöffnete Schloss.

9.4 Szenarien in der SmartHomeSec-App aktivieren

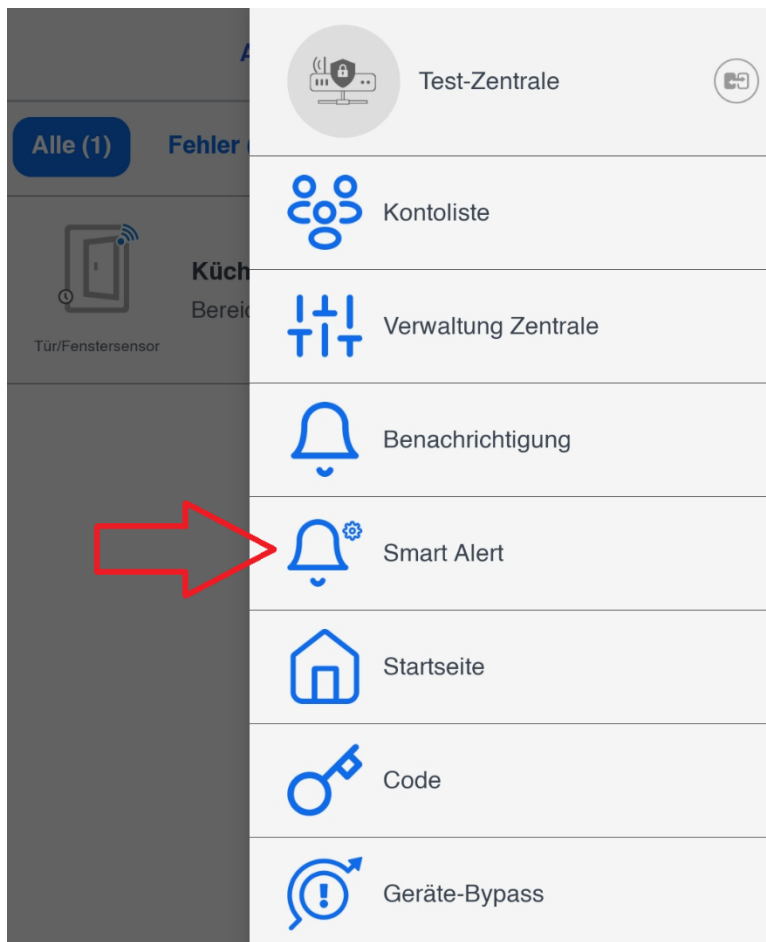
Mit der SmartHomeSec-App auf Ihrem Smartphone, können Sie die eben erstellen Szenarien dank Geofencing automatisch ausführen lassen, wenn Sie den von Ihnen vorgegebenen Bereich verlassen oder betreten.

Gehen Sie zum aktivieren der Szenarien wie folgt vor:

1. Starten Sie die SmartHomeSec-App
2. Klicken Sie oben Rechts auf das Menü [1]



3. Wählen Sie im Menü den Punkt „Smart Alert“ aus



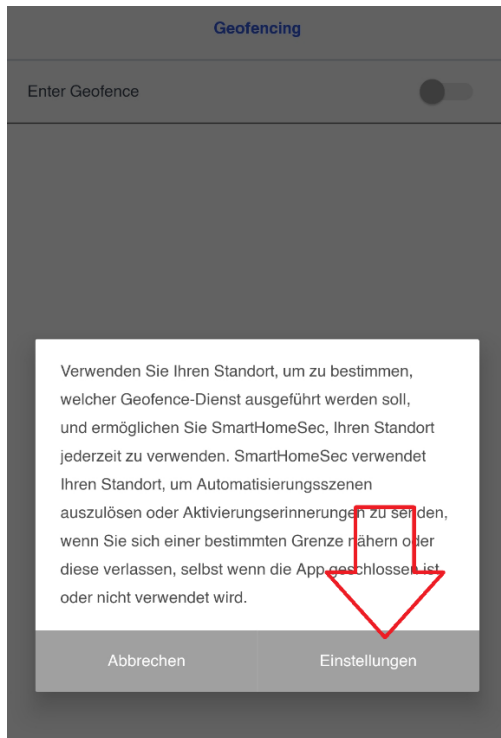
4. Wählen Sie **Geofencing -> Geofence verlassen** aus.

Haben Sie der App SmartHomeSec noch nicht die Erlaubnis gegeben, auch im Hintergrundmodus GPS-Daten zu verarbeiten, müssen Sie dieses jetzt tun.

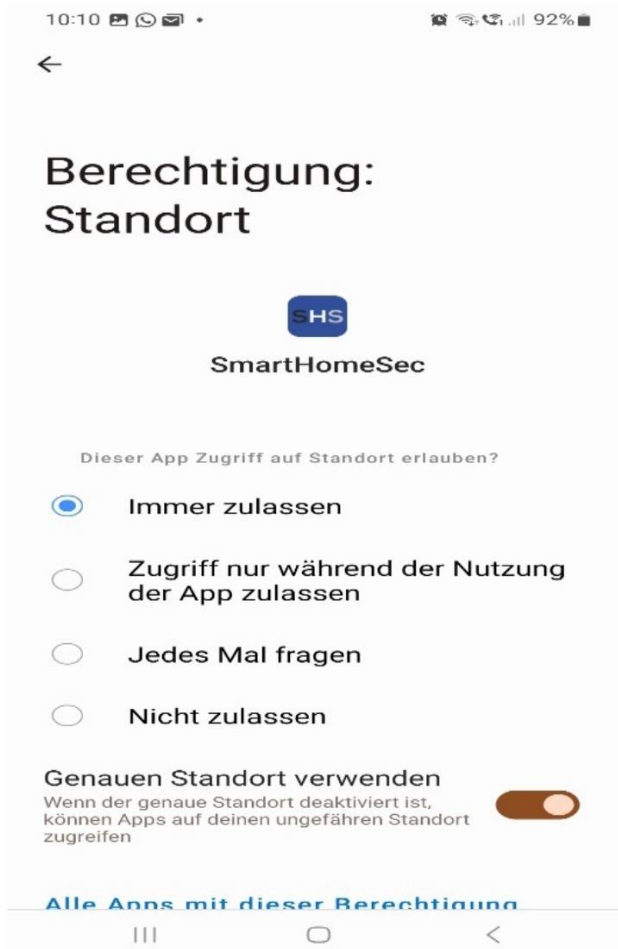
Erklärung: Die App SmartHomeSec entscheidet anhand von GPS Koordinaten, ob Sie im Geofencing Bereich sind oder diesen verlassen bzw. betreten.

5. Klicken Sie auf „Einstellungen“ wenn Sie der App die Erlaubnis geben möchten, GPS-Anfragen auch im Hintergrund vorzunehmen.

Haben Sie der App bereits die Erlaubnis erteilt, können Sie diesen Schritt überspringen. Setzen Sie unter Punkt 7. die Anleitung fort.



6. Setzen Sie die Einstellungen für den Standort wie folgt:



Sind die Berechtigungen vergeben (Kapitel 9.2), können Sie jetzt das eben angelegte Szenario zum Scharf-Schalten der Alarmzentrale auswählen:



7. Unter Benachrichtigungen können Sie sich jetzt auch eine Scharfschalterinnerung senden, anstatt das Szenario anzuwenden. Das bietet sich zum Beispiel an, wenn sich noch andere Personen in Ihrem Haus aufhalten.
8. Gehen Sie entsprechend mit dem Menüpunkt „Enter Geofence“ um. Hier können Sie jetzt das Szenario zum Unscharf-Schalten auswählen (**Kapitel 9.3**). So wird Ihre VESTA Alarmanlage unscharf geschaltet, wenn Sie den Bereich Geofence betreten.

10. Einstellungen Zentrale

Hier legen Sie grundlegende Einstellungen Ihrer VESTA-Alarmzentrale fest.

So rufen Sie die allgemeinen Bedienfeldeinstellungen auf: **Einstellungen [1] -> Zentrale [2] -> Sicherheit [3]**

Hinweis: Der Errichtercode ist im Auslieferungszustand: **7982**

The screenshot shows the 'Einstellungen - Zentrale' page with the following settings:

Alle Modus			
Finale Tür	Aus	Aktivierungsfehler Typ	Zwangsscharfschaltung
Sabotagealarm	Vollscharf	Supervision-Überwachung	Ein
Zeit Supervision	24 Std.	Supervision Timer(for Pendant)	Deaktivieren
Alarmdauer	2 Min.	Timer 2-Melderabhängigkeit	Deaktivieren
Timer Feuerverifizierung	Deaktivieren	Türklingel	Kein Ton
Ton bestätigen	Leise	Warnton	Kein Ton
Nur Endsignaltöne bei Eintritt/Austritt	3 Sek.		
Scharf			
Eintrittsverzögerungszeit 1	20 Sek.	Eintrittsverzögerungszeit 2	Deaktivieren
Austrittsverzögerungszeit	30 Sek.	Eingangsverzögerung Ton	Leise
Ton Austrittsverzögerung	Leise		
Teilscharf			
Eintrittsverzögerungszeit 1	20 Sek.	Eintrittsverzögerungszeit 2	Deaktivieren
Austrittsverzögerungszeit	30 Sek.	Eingangsverzögerung Ton	Leise
Ton Austrittsverzögerung	Leise		

Unterabschnitte:

1. Sicherheit
2. Zentrale
3. Code
4. Datum und Uhrzeit
5. Werkseinstellungen zurückgesetzt
6. FW-Update

10.1 Sicherheit

So greifen Sie auf den Unterabschnitt Sicherheit zu: **Einstellungen -> Zentrale -> Sicherheit**

Sie können jetzt im Dropdownmenü **[1]** auswählen, welchen Bereich Sie konfigurieren möchten.

The screenshot shows the 'Einstellungen - Zentrale' (Settings - Central Station) page. The left sidebar contains navigation options: Test-Zentrale, Sicherheit, Automation, Live-Video, Ereignis, and Einstellungen. The main content area is titled 'Einstellungen - Zentrale' and has tabs for 'Sicherheit', 'Zentrale', 'Code', 'Datum & Zeit', 'Werkseinstellungen zurückgesetzt', and 'FW-Update'. The 'Sicherheit' tab is active, and a dropdown menu [1] is open, showing 'Bereich 1' selected. The settings are organized into three sections: 'Bereich 1' [2], 'Schritt' [3], and 'Teilscharf' [4].

Bereich	Modus	Supervision-Überwachung	Supervision Timer(for Pendant)	Timer 2-Melderabhängigkeit	Türklingel	Warnton
Bereich 1	Aus	Ein	Deaktivieren	Deaktivieren	Kein Ton	Kein Ton
Bereich 2						
Bereich 3	Vollscharf	Ein	Deaktivieren	Deaktivieren	Kein Ton	Kein Ton
Bereich 4						
Bereich 5	24 Std.		Deaktivieren	Deaktivieren	Kein Ton	Kein Ton
Bereich 6						
Bereich 7	2 Min.		Deaktivieren	Deaktivieren	Kein Ton	Kein Ton
Bereich 8						

Eintrittsverzögerungszeit 1	Eintrittsverzögerungszeit 2	Eingangsverzögerung Ton
20 Sek.	Deaktivieren	Leise
30 Sek.		
Leise		

Eintrittsverzögerungszeit 1	Eintrittsverzögerungszeit 2	Eingangsverzögerung Ton
20 Sek.	Deaktivieren	Leise
30 Sek.		
Leise		

Die Ansicht ist in 3 Sektionen unterteilt:

Alle Modus [2]: Hier nehmen Sie Einstellungen vor, die immer für den Bereich gelten. Dazu zählen insbesondere der Feualarm, wie lange ein Alarm dauern darf, ob es eine Türklingel gibt usw.:

- **Finale Tür:** Gibt an ob der Bereich beim Schließen der “Finalen Tür” scharf geschaltet werden soll. Die Finale Tür wird in den Sensoreinstellungen angegeben (**Kapitel 8**)
- **Sabotage Alarm:** Wählen Sie aus ob Sabotagealarm der Sensoren **immer** ausgelöst werden soll oder nur wenn der Bereich **Vollscharf** geschaltet ist.
- **Zeit Supervision:** Zeitraum in dem die Sensoren regelmäßig überprüft werden soll.
- **Alarmdauer:** Wie lange sollen die Sirenen Alarm geben. In Deutschland sollte dieses nicht länger als 5 Minuten dauern (bitte Gesetz prüfen)
- **Timer Feuerverifizierung:** Wie lange soll die Überprüfung eines Feieralarms dauern.
- **Ton bestätigen:** Aktivieren des Bestätigung Tons in Sirenen bei einem Moduswechsel.
- **Nur Endsignaltöne bei Eintritt/Austritt:** Töne die beim Ein oder Austritt des Bereichs ausgegeben werden.
- **Aktivierungsfehler Typ:** Was soll passieren wenn ein Sensor einen Fehler beim Scharf-Schalten zurück meldet. Zum Beispiel wenn ein Fenster noch geöffnet ist, dass geschlossen sein muss.
- **Supervision-Überwachung:** Sollen die Geräte aus dem Bereich auf Fehler überwacht werden.
- **Türklingel:** Sollen die Sirenen des Bereichs klingeln, wenn eine Tür in dem Bereich geöffnet wird. Beachten Sie dazu auch die Sensoreinstellungen (**Kapitel 8**).
- **Warnton:** Soll die Zentrale regelmäßig einen Alarmton abgeben, wenn ein Sensor aus dem Bereich einen Fehler hat. Zum Beispiel eine Sabotage aufweist oder die Batterie bald leer ist.

Scharf [3]: Einstellungen die gelten, wenn der Bereich scharf geschaltet ist:

- **Eintrittsverzögerung 1 / 2:** Dauer der Eintrittsverzögerung 1 oder 2. Ist ein Sensor beim Zustand “scharf” / “arm” der Eintrittsverzögerung 1 oder 2 zugewiesen (**Siehe Kapitel 8**), dauert es die Anzahl in Sekunden bis der Sensor Alarm auslöst. So können Sie sich Zeit geben, die Alarmanlage unscharf zu schalten, wenn Sie einen Sensor auslösen der eine Eintritt-Verzögerung hat.

***Tipp:** Zum Beispiel geben Sie sinniger Weise der Haustür eine Eintrittsverzögerung, wenn das Keypad zum Entschärfen sich im Inneren des Hauses sich befindet.*

- **Austrittsverzögerung:** Dauer der Zeit zum Verlassen eines Bereichs wenn dieser scharf geschaltet wird. Ist ein Sensor beim Zustand “scharf” / “arm” der Austrittsverzögerung zugewiesen (**Siehe Kapitel 8**), dauert es die Anzahl in Sekunden die der Sensor noch keine Auslösung als Alarm wertet. So können Sie sich Zeit geben, die Alarmanlage scharf zu schalten, wenn Sie einen Sensor auslösen der eine Austritt-Verzögerung hat. Sinniger Weise setzen Sie

diese Einstellung bei der Haustür, damit Sie das Gebäude noch verlassen können.

- **Ton Austrittsverzögerung:** Sollen die Sirenen einen Ton beim Countdown der Austrittsverzögerung abgeben? **Wichtig:** Sie können jede Sirene individuell in den Sensoreinstellungen (**Kapitel 8**) konfigurieren, wie Sie auf den Austritt reagieren soll.
- **Eingangsverzögerung Ton:** Sollen die Sirenen einen Ton beim Countdown der Eingangsverzögerung abgeben? **Wichtig:** Sie können jede Sirene individuell in den Sensoreinstellungen (**Kapitel 8**) konfigurieren, wie Sie auf den Eintritt reagieren soll.

Teilscharf [4]: Sie können Sensoren auf den Zustand „teilscharf“ konfigurieren (**Siehe Kapitel 8**). Teilscharf kann ein Bereich zum Beispiel sein, wenn Sie Zuhause sind, die Außen-Türen aber vor Zutritt schützen möchten. Die Einstellungen sind gleich wie im Bereich „Scharf [3]“. Die Werte der Einstellungen gelten entsprechend.

10.2 Zentrale

So greifen Sie auf das Untermenü zu: **Einstellungen -> Zentrale -> Zentrale**

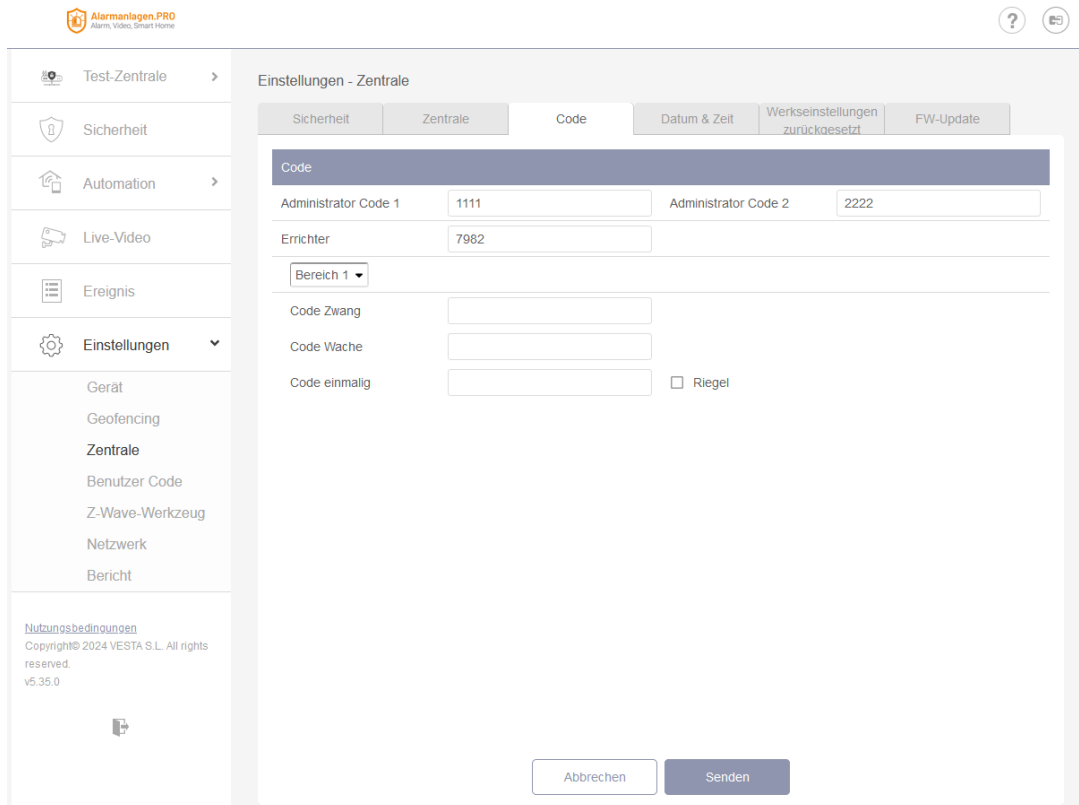
The screenshot displays the 'Einstellungen - Zentrale' configuration page in the VESTA Alarmanlagen.PRO interface. The page is organized into a sidebar on the left and a main content area on the right. The sidebar includes navigation options such as 'Test-Zentrale', 'Sicherheit', 'Automation', 'Live-Video', 'Ereignis', and 'Einstellungen'. The main content area is titled 'Einstellungen - Zentrale' and features several tabs: 'Sicherheit', 'Zentrale', 'Code', 'Datum & Zeit', 'Werkseinstellungen zurückgesetzt', and 'FW-Update'. The 'Zentrale' tab is active, showing a list of settings for the central unit. These settings include 'AC-Fehlerbericht' (5 Min.), 'AC-Fehler unterbrochen' (5 Sek.), 'Fremdfunk Report' (2 Min.), 'Auto Check-in-Intervall' (1 Std.), 'Auto Check-in Daily Time' (00 : 00), 'Stop Device Status Notify' (Deaktivieren), 'IR-Kameraauflösung von Alarmbildern' (320x240x6 images), 'Außen-IR-Kamera in Graustufen' (Aktivieren), 'Ethernet-Fehler umgehen' (Aus), 'Service Failure Report (Ethernet)' (Deaktivieren), 'Mute internal siren' (Aus), and 'DNS-Aktualisierung' (4 Std.). Below these settings is the 'External Battery' section, which includes 'External Battery' (Deaktivieren), 'Alarm Triggers Connection Time' (10 Min.), and 'Optimized Mode Connection Time' (08 : 00 ~ 14 : 30). The 'Funk-Sirene programmieren' section contains buttons for 'Sirenen Sabotage Ein' and 'Sirenen Sabotage Aus'. The 'Alarmzentrale Info' section at the bottom provides details about the central unit, including 'Zentralenname' (Test-Zentrale), 'Interne IP' (192.168.179.48), 'Öffentliche IP' (93.192.178.87), 'Konto Bericht' (127038466122), and 'GSM-Version' (Quectel Ltd M95FAR02A09). A 'Konfiguration erneut senden' button is also present. The page footer includes the text 'Nutzungsbedingungen Copyright© 2024 VESTA S.L. All rights reserved. v5.35.0'.

Im Unterabschnitt Zentrale allgemeine Einstellungen der Zentrale geändert werden:

- **AC-Fehlerbericht:** Nach welcher Zeit soll ein Stromausfall gemeldet werden
- **AC-Fehler unterbrochen:** Nach welcher Zeit gilt ein Stromausfall als vorhanden.
- **Fremdfunk Report:** Nach welcher Zeit sollen Störsender gemeldet werden.
- **Stop Device Status Notify:** Hier können Sie kurzzeitig Benachrichtigungen der Zentrale abschalten (zum Beispiel bei einer Großstörung, damit Sie in Ruhe arbeiten können)
- **IR-Kameraauflösung von Alarmbildern:** Auflösung der übertragenen Bilder von den PIR-Kameras
- **Außen-IR-Kamera in Graustufen:** Sollen Außenkameras Bilder nur in graustufen übertragen?
- **Ethernet-Fehler umgehen:** Sollen Netzwerkfehler nicht gemeldet werden.
- **Service Failure Report (Ethernet):** Versenden eines Reports von Netzwerk-Fehlern.
- **Mute internal siren:** Interne Sirene (die Sirene der Zentrale) ausschalten.
- **DNS-Aktualisierung:** Wie lange sollen DNS-Records intern gespeichert werden. (DNS ist das System zur Auflösung von Domainnamen im Internet).
- **External Battery:** Hier können Sie eine externe Batterie deaktivieren,.
- **Alarm Triggers Connection Time:** Nach welcher Zeit soll ein Alarm ausgelöst werden, wenn auf die externe Batterie umgeschaltet wurde?
- **Funk-Sirene programmieren:** Die Funk-Sirenen (externe Sirenen) warten auf Signale von der Zentrale. Wenn Sie bei einer Sirene zum Beispiel den Sabotageschutz abschalten möchten, um die Batterien zu wechseln, können Sie hier den Sabotageschutz der Sirenen ein und ausschalten.
- **Konfiguration erneut senden:** Rufen Sie die aktuell auf der Zentrale gesetzten Einstellungen ab.

10.3 Code

Zugriff auf den Unterabschnitt Code :



Im Unterabschnitt "**Code**" können die Zugangsparameter geändert werden. Das heißt, die Codes zu programmieren, die die verschiedenen Benutzertypen von jedem Tastenfeld aus authentifizieren.

- Master Code 1 und 2: Ermöglicht einem Benutzer die permanente Umgehung von Zonen, die Verwaltung von Codes usw. über ein App/WEB-Konto mit Administratorprofil.
- Errichtercode: ermöglicht die vollständige Programmierung der Zentrale.
- Code Zwang: Systemsteuerung mit stillem Alarm
- Code Wache: für Sicherheitspersonal
- Code Einmalig: Nur 1 Mal entschärfen und aktivieren

Codes von einzelnen Benutzern vergeben Sie in einem separaten Menü:

Einstellungen -> Benutzer Code

The screenshot shows the 'Einstellungen - Benutzer Code' (Settings - User Code) page in the VESTA Alarmanlagen.PRO application. The interface is divided into a left sidebar and a main content area. The sidebar contains navigation options: Test-Zentrale, Sicherheit, Automation, Live-Video, Ereignis, and Einstellungen (selected). Under 'Einstellungen', there are sub-options: Gerät, Geofencing, Zentrale, Benutzer Code (selected), Z-Wave-Werkzeug, Netzwerk, and Bericht. At the bottom of the sidebar, there are links for 'Nutzungsbedingungen' and 'Copyright © 2024 VESTA S.L. All rights reserved. v5.35.0'. The main content area has two tabs: 'Benutzer Code' (active) and 'Cross-Flair-Benutzer-Pin'. Below the tabs, there is a dropdown menu for 'Bereich 1'. The main area contains a table with 15 rows, each representing a user code. The first row is pre-filled with 'user' in the 'Benutzername' column and a masked PIN in the 'PIN Code' column. The other rows are empty. At the bottom of the table, there are two buttons: 'Abbrechen' (Cancel) and 'Senden' (Send).

- Benutzer-PIN: Benutzercode mit der Fähigkeit, den ausgewählten Bereich zu steuern.
- A. **Benutzer hinzufügen** oder **löschen**.
 - B. Vergeben Sie einen **Benutzernamen** und einen **Code** (4 bis 6 Ziffern).
 - C. Bis zu 240 Codes pro Gebiet

Unter dem Reiter „Cross-Flair-Benutzer Pin“ können Sie Nutzer-Codes vergeben, die zeitlich mehrere Bereiche steuern können. Wählen Sie aus, für welche Bereiche der Code gültig ist.

10.4 Datum und Uhrzeit

So rufen Sie den Unterabschnitt "Datum und Uhrzeit" auf: Einstellung Panel
 Ajustes- Datum und Uhrzeit

Seguridad	Panel	Código	Fecha y hora	Restablecimiento de fábrica	Actualización de FW
Reloj					
Zona horaria	(GMT+01:00) Madrid, Bruselas, Copenhague, París ▼				
Fecha y hora	📅 2022/08/11	🕒 17 : 12			
Hora de internet	pool.ntp.org ▼	<input checked="" type="checkbox"/> Sincronizar automáticamente con un servidor horario de Internet			

Hinweis: Es wird empfohlen, diesen Abschnitt in der Werkseinstellung zu belassen, solange Datum und Uhrzeit in der richtigen Zeitzone liegen.

10.5 Werksrückstellung

So rufen Sie den Unterabschnitt Reset auf: Einstellung Panel Ajustes- Factory Reset

Ajuste - Panel					
Seguridad	Panel	Código	Fecha y hora	Restablecimiento de fábrica	Actualización de FW
Restablecimiento de fábrica					
<input type="checkbox"/> Mantener la configuración de red actual					
<input type="checkbox"/> Mantener la lista actual de dispositivos					

Hinweis: Es ist auch möglich, einen Werksreset manuell durchzuführen. Mit dieser Softwarefunktion können Sie jedoch die Netzwerkkonfiguration sowie die Konfiguration der zugewiesenen Geräte nach dem Zurücksetzen beibehalten.

10.6 FW-Aktualisierung

Bevor Sie die Installation verlassen, sollten Sie das Panel auf die neueste verfügbare FW-Version aktualisieren lassen.

Wenn Sie aus irgendeinem Grund NICHT können, können Sie diese FW aus der Ferne aktualisieren, wann immer Sie wollen. Dies ist ein sehr sicherer Prozess, der < 3 min. dauert und nach dem das Panel neu gestartet wird.

Ajuste - Panel

Seguridad Panel Código Fecha y hora Restablecimiento de fábrica Actualización de FW

Actualización de FW

Panel Seleccione

IO MCU **1** Seleccione
 GL_demes-0.0.2.28H.bin
 GL_demes-0.0.2.28G4 [BETA].bin
 GL_demes-0.0.2.28C.bin
 GL_demes-0.0.2.28E .bin

Ajuste - Panel

Seguridad Panel Código Fecha y hora Restablecimiento de fábrica Actualización de FW

Actualización de FW

Panel Seleccione

IO MCU **2** Seleccione
 Seleccione
 U-IO_BL_A10_220622.bin
 U-IO_BL_A08_220208.bin
 U-IO_BL_A09_220513.bin

Hinweis! Das Modell des Panels, mit dem die Screenshots gemacht wurden, ist das Hybrid-Modell. Daher können Sie nicht nur die FW des Panels [1] aktualisieren, sondern auch die FW des IO-MCU-Controllers [2], der für die Verwaltung der verdrahteten und BUS-Expander zuständig ist.

Hinweis 2! Es wird empfohlen, immer die neueste FW-Version zu wählen, die normalerweise die Position 1 einnimmt.

10.7 Konventionelle verdrahtete Zonen

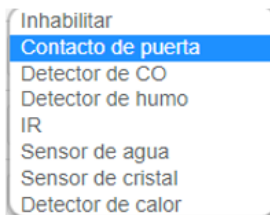
Ajuste- Dispositivo con cable ⓘ ← Tipo de lazo

Sensores cableados int€ ▾

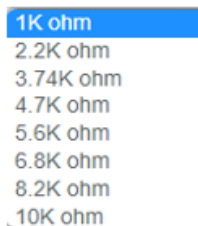
Zona	Tipo	Bucle	Resistor	Estado	Panel Area/ Zona
1	IR	8	5.6K ohm	Desencadenar	Area 2 Zona 25 Editar
2	Contacto de puerta	2	1K ohm	Desencadenar	Area 3 Zona 3 Editar
3	IR	8	1K ohm	Tamper abierto	Area 1 Zona 6 Editar
4	Inhabilitar	1	1K ohm	Restaurado	
5	Inhabilitar	1	1K ohm	Restaurado	
6	Inhabilitar	1	1K ohm	Restaurado	
7	Inhabilitar	1	1K ohm	Restaurado	
8	Inhabilitar	10	1K ohm	Tamper abierto	
9	Inhabilitar	1	1K ohm	Restaurado	
10	Inhabilitar	1	1K ohm	Restaurado	
11	Inhabilitar	1	1K ohm	Restaurado	
12	Inhabilitar	1	1K ohm	Restaurado	
13	Inhabilitar	1	1K ohm	Restaurado	
14	Inhabilitar	1	1K ohm	Restaurado	
15	Inhabilitar	1	1K ohm	Restaurado	
16	Inhabilitar	1	1K ohm	Restaurado	

Exklusiv in der HIBRIDA-Steuereinheit stehen 16 verdrahtete Zonen zur Verfügung, mit der Möglichkeit, die Schleife mit EOL-, DEOL-, 3EOL-Widerständen zu schützen oder einfache NC / NO-Schleifen zu realisieren. Um die Zone zu aktivieren, ist es nur notwendig, anzuzeigen:

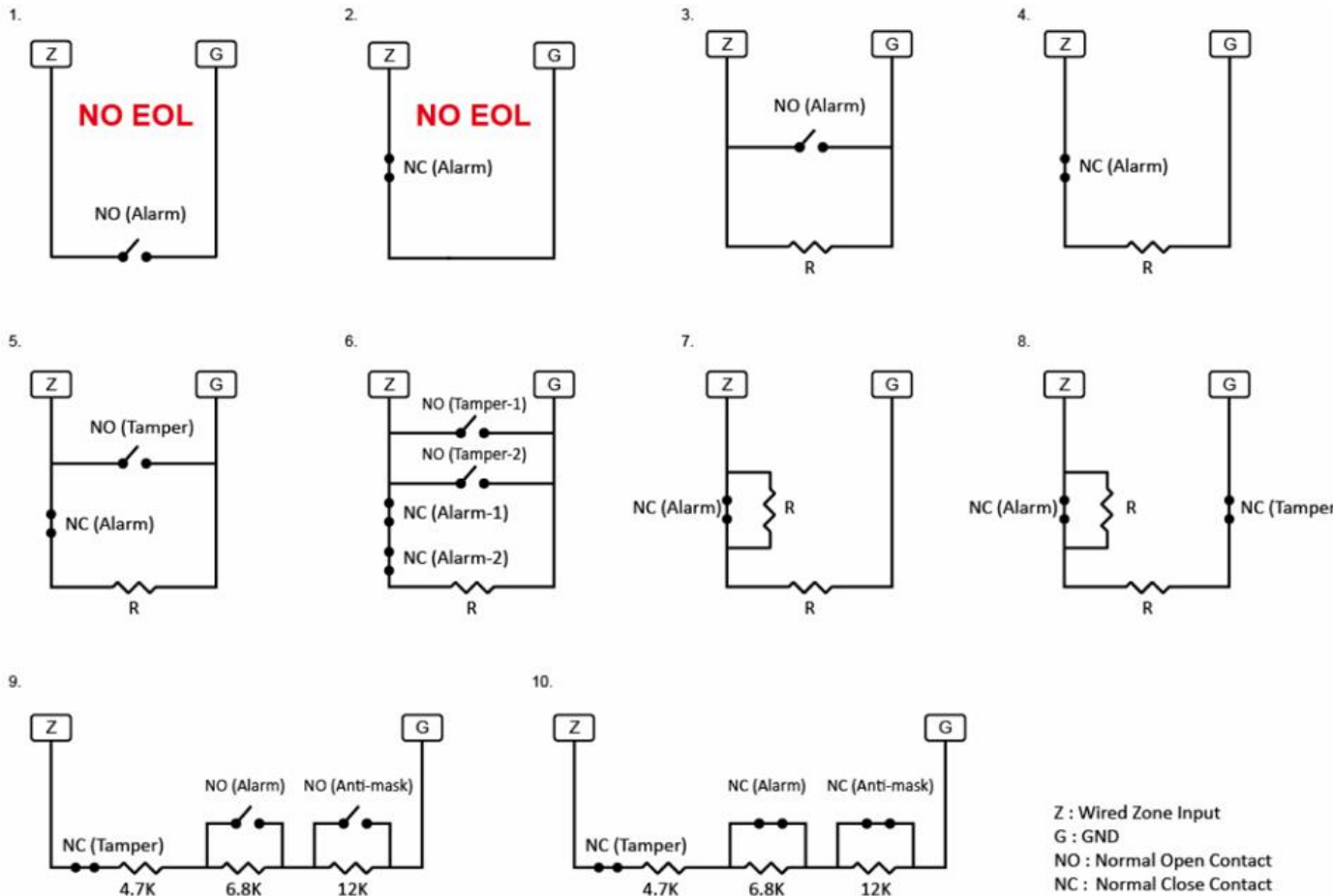
- Art der Zone



- Art der Schleife, klicken Sie auf oder siehe nächste Folie
- EOL- oder DEOL-Widerstand, wählbar für jeden der 16 Eingänge



- Adresse zu einem virtuellen Bereich und einer Zone. Standardmäßig verknüpft das System den Melder mit einem freien virtuellen Bereich und einer Zone. Durch Klicken auf die Schaltfläche können Sie diese Werte bearbeiten.



Anschluss der Zone



Hinweis! Die Widerstandswerte innerhalb derselben Schleife können gewählt werden [1k, 2.2K, 3.74K, 4.7K, 5.6K, 6.8K, 8.2K, 10K], müssen aber für beide Widerstände gleich sein, außer für die Schleife 9 und 10, die für 3xEOI-Detektoren mit Anti-Masking, Alarmkontakt und Sabotage vorgesehen ist. In diesem Fall müssen die im Diagramm angegebenen Widerstandswerte beachtet werden.

10.8 NETZWERK-Einstellungen: GSM

Einstellung Red GSM / GPRS / LORA

The screenshot displays the 'Ajuste - Red' (Network Settings) screen in the VESTA application. The left sidebar contains a menu with 'Ajuste' and 'Red' highlighted. The main content area is divided into sections for GSM, MMS, and SMS. The GSM section includes fields for IMEI, IMSI, Operator, Signal Level (0), SIM card detection (Inhabilitar), GSM Event (Habilitar), GPRS connection limit (1 hora), and Antenna (Externo). The MMS section includes fields for APN, Contraseña, Dirección proxy, Nombre de usuario, URL, and Puerto proxy. The SMS section includes fields for Palabra clave de SMS (7982) and Palabra P SMS (PROG). Buttons for 'Cancelar' and 'Enviar' are located at the bottom of the screen.

Wenn Sie den Unterabschnitt GSM aufrufen, werden die folgenden Informationen angezeigt:

1. GSM Operator: mit dem das Panel verbunden ist
2. GSM-Signalpegel [0-9], wobei 0 keine GSM-Abdeckung und 9 ein ausgezeichnetes Signal bedeutet.
3. SIM-Erkennung. Es ist möglich, den Kommunikator zu aktivieren/deaktivieren.
4. GSM-Ereignis: Bei wiederholten Ausfällen aufgrund mangelnder Netzabdeckung kann dieses Ereignis deaktiviert werden.
5. Begrenzung der GPRS-Verbindung:

- a. Bei Einrichtungen mit Zwei-Wege-Kommunikation ist es ratsam, 1h zu wählen.
 - b. Bei Installationen, die nur über GPRS/LTE-Kommunikation verfügen, wählen Sie Deaktivieren.
6. Antenne: Wenn eine GSM-Verstärkerantenne an den externen Anschluss angeschlossen ist, muss dieser Parameter aktiviert werden.

10.9 NETZWERK-Einstellungen: GPRS

Einstellung Red GSM / **GPRS** / LORA

The screenshot shows the 'Ajuste - Red' (Network Settings) screen in the VESTA mobile application. The interface is in Spanish. On the left, a sidebar menu is visible with options: Seguridad, Automatización, Evento, Ajuste (highlighted with a red box), Dispositivo, Geofencing, Panel, Dispositivo con cable, Red (highlighted with a red box), and Reporte. The main content area is titled 'Ajuste - Red' and has three tabs: GSM, GPRS (selected), and LoRa. Under the GPRS tab, there are two rows of input fields: 'APN' with the value 'Internet', 'Nombre de usuario' with the value 'Nombre de usuario', 'Contraseña' with the value 'Contraseña', and another 'Nombre de usuario' field. At the bottom of the screen, there are two buttons: 'Cancelar' and 'Enviar'. The footer contains the text: 'Términos y Condiciones', 'Copyright © 2020 ByDemes SL. Todos los derechos reservados.', and 'v5.10.0'.

Greifen Sie auf den Unterabschnitt GPRS zu, um den Zugangspunkt zu konfigurieren und in der Lage zu sein, ins Internet zu gehen und das Panel über GPRS/LTE-Kommunikator zu kommunizieren.

Sie können den [APN der SIM-Karte](#) bei Ihrem Betreiber erfragen, und wenn Sie ihn nicht kennen, können Sie in

APN: Internet

Benutzer: [Leer lassen] **Benutzer:** [Leer lassen] **Benutzer:** [Leer lassen]

Benutzer: [Leer lassen] **Benutzer:** [Leer lassen] **Benutzer:** [Leer lassen]

Passwort: [Leer lassen]

10.10 NETZWERK-Einstellungen: LORA

Einstellung Red GSM / GPRS / [LORA](#)

The screenshot shows the 'Ajuste - Red' (Network Settings) screen in the VESTA application. The interface is in Spanish. On the left, a sidebar menu is visible with 'Ajuste' (Settings) and 'Red' (Network) highlighted with red boxes. The main content area is titled 'Ajuste - Red' and has three tabs: 'GSM', 'GPRS', and 'LoRa'. The 'LoRa' tab is active. At the top, there is a toggle for 'Habilitar dongle LoRa' (Enable LoRa dongle) set to 'Habilitar'. Below this is a 'Configuración de LoRa' section with an 'Actualizar' (Update) button. The configuration fields are: 'APP KEY' (AE3D87F1781A93DC6402318DAC982197), 'APP EUI' (0101010101010101), and 'DEVICE EUI'. There is also a 'Versión del dongle' (Dongle version) field with 'Estado' (Status) and 'Fallido' (Failed) indicators. A 'Nivel de señal [0-9]' (Signal level) field is set to '0 dBm'. A note at the bottom states: 'Nota: Por favor, asegúrese de que una de las rutas de reporte se tiene que establecer en Lora.' (Note: Please ensure that one of the reporting routes is set to Lora.) At the bottom of the screen, there are 'Cancelar' (Cancel) and 'Enviar' (Send) buttons.

Durch Zugriff auf den Unterabschnitt LORA kann [dieser dritte Kommunikationskanal](#) aktiviert werden.

Auf diese Weise können wir im Falle eines IP-Ausfalls über Ethernet (Hauptroute) oder IP über GPRS/LTE (2. Backup-Route) die Ereignisse des Panels über [LORAWAN](#) (3. Backup-Route) übertragen und das Panel mit dem ARC verbunden halten, während die anderen Routen nicht verfügbar sind.

Für weitere Informationen wenden Sie sich bitte an Ihren Vertriebsmitarbeiter oder an SAT Bydemes. [Spezifisches Handbuch](#) für die LORA-Kommunikationskonfiguration verfügbar.

10.11 ARC-Verbindungseinstellungen: Ereignisse

Einstellung Reporte [Reporte](#) / Erfasste Datei

Hybrid > Ajuste - Reporte

Reporte SMS Archivo capturado SMTP

Reporte

URL 1 Grupo 1

URL 2 Grupo 2

Nota:

- Informe a través de IP (Ethernet o GPRS) en formato CID, por ejemplo: ip://ACCT@server.port/CID
- Informe a través de IP (Ethernet o GPRS) en formato SIA, por ejemplo: ip://ACCT@server.port/SIA
- Informe a través de IP (Ethernet o GPRS) en formato Manitou, por ejemplo: ip://ABONADO@server.port/MAN
- Informe a través de llamada GSM, por ejemplo: gsm://ACCT@telefono/BEEP
- Informe por correo electrónico, por ejemplo: mailto: usuario@ejemplo.com
- Reporte por LoRaWAN: lora://INDEX+ABONADO@local/CID
INDEX= Identificador facilitado por CRA.
ABONADO= N° de Abonado facilitado por CRA.
Por ejemplo Index "AB" y Abonado "1234": lora://AB1234@local/CID

	Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
Secuencia de informes	Esencial	Esencial	Esencial	Esencial	Esencial
Procesar de nuevo	99 Procesar	3 Procesar d	99 Procesar	99 Procesar	99 Procesar

Configuración de reporte

Cancelar Enviar

Términos y Condiciones
Copyright © 2020 ByDemes SL. Todos los derechos reservados.
v5.10.0

Im Unterbereich **BERICHT** können Sie die Daten Ihrer Überwachungsstation oder Ihres Ereignisempfängers konfigurieren. Klicken Sie einfach auf die Schaltfläche "+", um ein weiteres Feld für die Verbindung mit der ARC zu öffnen.

Im Abschnitt Hinweis finden Sie alle kompatiblen Formate sowie Beispiele für den zu konfigurierenden URL-String. Das zu verwendende Standardformat ist das in Beispiel 3 [MANITOU] gezeigte.

- **Teilnehmer:** mit der CRA vereinbarte Teilnehmernummer
- **Server:** Öffentliche IP der CRA
- **Hafen:** Öffentlicher Hafen der CRA

/MAN, bezieht sich auf die Übertragung von Ereignissen im **Manitou-Format**. Unser ARC-Gateway ALARMSPACE sorgt für die Konvertierung der Ereignisse in eine Sprache, die für die vorhandene Empfänger-Software geeignet ist.

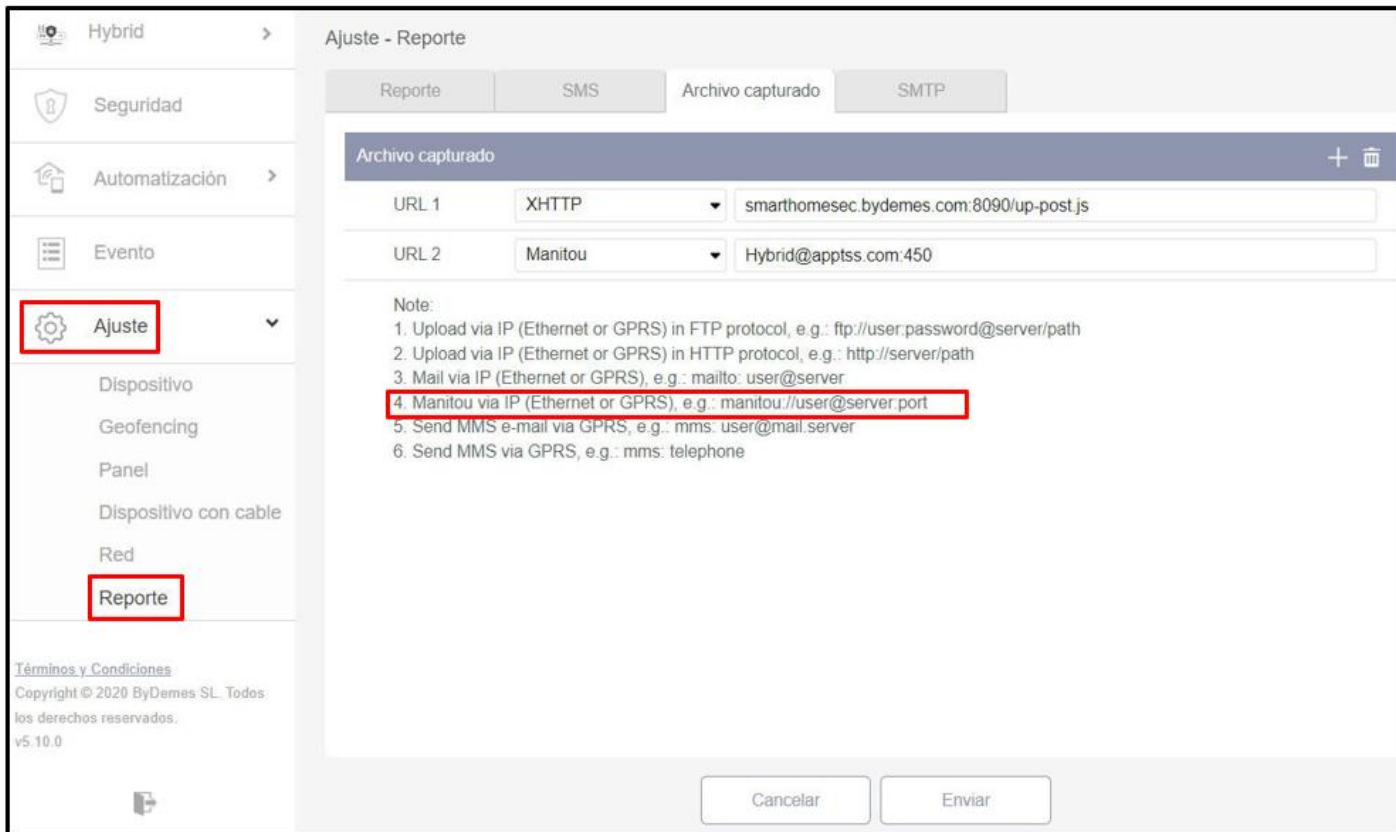
Gruppe: Die Ereignisse werden an alle URLs übertragen, die zu verschiedenen Gruppen gehören. URLs innerhalb der gleichen Gruppe fungieren als Backup und das Ereignis wird nur an eine von ihnen übertragen, beginnend in der Reihenfolge der Liste (URL1,2,3...).

Hinweis! Für die Verbindung zu einer CRA-Adresse ist die URL der Gruppe 2 als Gruppe 1 für die VESTA-Cloud vordefiniert.

Wiederaufbereitung: 3/5 Wiederholungsversuche für alle Gruppen empfohlen

10.12 ARC-Verbindungseinstellungen: Bilder

Einstellung Reporte Reporte / [Erfasste Datei](#)



Im Unterabschnitt "[Erfasste Datei](#)" können Sie die Daten Ihres Empfängers so konfigurieren, dass er die von [vorhandenen PIR-CAMs oder IP-Kameras](#) erzeugten Bilder empfängt.

Klicken Sie einfach auf die Schaltfläche "+", um ein weiteres Feld zu öffnen.

um eine Verbindung mit der CRA herzustellen.

Im Abschnitt Hinweis finden Sie alle kompatiblen Formate sowie Beispiele für den zu konfigurierenden URL-String. Das Standardformat, mit dem Sie sich verbinden müssen, ist im Beispiel Nr. 4 dargestellt

- [Benutzer](#): mit der CRA vereinbarte Teilnehmernummer
- [Server](#): Öffentliche IP der CRA
- [Hafen](#): Öffentlicher Hafen der CRA

Wählen Sie das [MANITOU-Protokoll](#) aus dem Dropdown-Menü. Unser ARC-Gateway, ALARMSPACE, empfängt die Fotos und überträgt sie an die ARC-Software.