

DRAHTLOSE ZENTRALE MIT IP-, WLAN- UND 4G-NETZWERK

Artikelnummer 1051/020



**Installations- und Programmieranleitung
mittels PC**

INHALTSVERZEICHNIS

1	EINLEITUNG	4
2	BESCHREIBUNG DER ZENTRALE	4
2.1	Identifizierung der Teile	5
2.2	Einsetzen der SIM-GSM-Karte (Option).....	6
2.3	Versorgung.....	6
2.4	Aufzeichnung der Sprachnachrichten	7
3	INSTALLATION	8
3.1	Grundvoraussetzungen	8
3.2	Schritte zur Montage der Zentrale	8
3.3	Programmierung der Zentrale 1051/020	10
3.4	Installation der Software Finder	12
4	ZUGRIFF AUF DIE WEBOBERFLÄCHE DER ZENTRALE	14
5	GERÄTEVERWALTUNG	15
5.1	Einlernen.....	15
5.2	Walk Test	17
5.3	Bearbeiten der Geräte.....	17
5.3.1	Detektoren	18
5.3.2	Funksteuerung und Tastatur	21
5.3.3	Geräte Foto/Video	23
5.3.4	Sirenen	25
6	SYSTEMEINSTELLUNGEN	26
6.1	Zugang - Allgemeine Informationen.....	26
6.2	Homepage	26
6.3	Ereignisprotokoll.....	29
6.4	Ereignisbericht	30
6.5	Einstellungen Zentrale.....	30
6.6	Benutzerdaten.....	33
6.7	Ereigniserfassung	34
6.8	Ereignisübertragung (Menü für spezialisierte Benutzer)	35
6.9	Gerätespeicher HA	35
7	NETZSTEUERUNG	36
7.1	GSM.....	36
7.2	LAN	37
7.3	WLAN	38
8	SYSTEMSTEUERUNG	39
8.1	Passwortänderung	39
8.2	Home Automation	39
8.3	Szenarien.....	39
8.4	BERICHT	39
8.5	SMS-Bericht.....	42

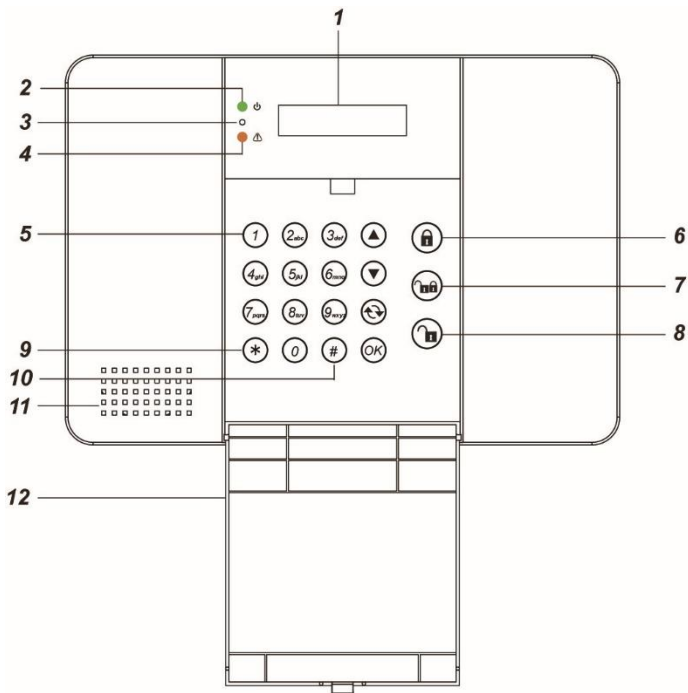
8.6	Upload Video	42
8.7	XMPP	43
8.8	Datum und Uhrzeit	43
8.9	Firmware & Firmware RF	44
8.10	Reset auf werkseitige Einstellungen	44
8.11	Backup & Rückstellen	45
8.12	Systemprotokoll	45
9	TECHNISCHE EIGENSCHAFTEN DER ZENTRALE	46
10	FERNSTEUERUNGSGERÄTE	47
11	ANHÄNGE	49
11.1	Typologien der im System generierten Alarme und Ereignisse	49
11.2	Anweisungen zum Ersetzen und Entsorgen der Batterien	50

1 EINLEITUNG

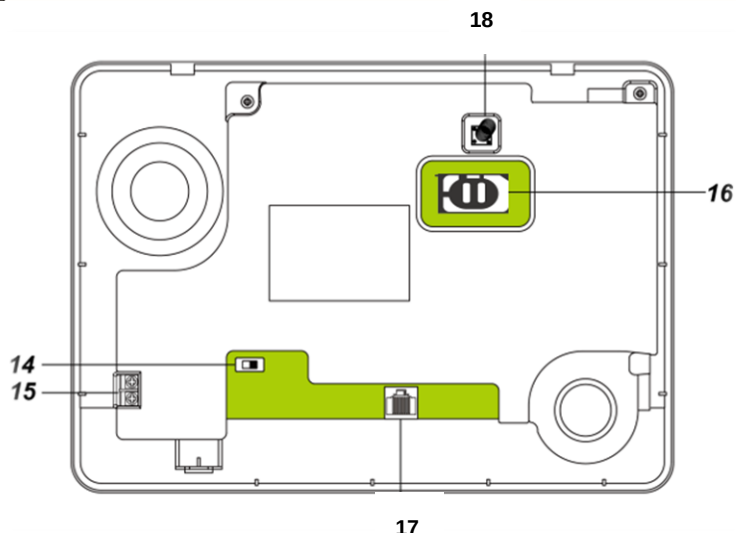
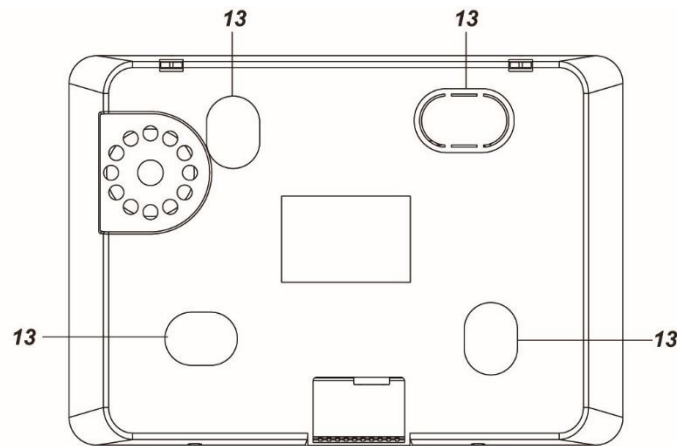
Dieses Handbuch befasst sich mit der Installation der Zentrale 1051/020 der Drahtlos-Alarmanlage Zeno mit Videoprüfung der Alarme.

2 BESCHREIBUNG DER ZENTRALE

VORDERANSICHT



RÜCKANSICHT (MIT ABDECKUNG)



RÜCKANSICHT (INNEN)

2.1 IDENTIFIZIERUNG DER TEILE

1. **LCD-Display mit Hintergrundbeleuchtung.**
2. **Versorgungs-Led (grün)**
LED EINGESCHALTET - System korrekt versorgt
LED AUSGESCHALTET - Netzversorgung fehlt, Pufferbatterie vollständig entladen oder Schalter auf OFF
BLINKENDE LED - Netzversorgung fehlt, Versorgung nur über die Pufferbatterie
3. **Mikrofon**
4. **Betriebsstatus-LED (gelb)**
LED EINGESCHALTET - System im Fehlerstatus
LED AUSGESCHALTET - System im normalen Betriebsstatus
5. **Tastatur**
▲: zum Bewegen des Cursors auf dem Display nach oben
▼: zum Bewegen des Cursors auf dem Display nach unten
↶↷: zum Verlassen der aktuellen Ansicht, um zur vorigen zurückzukehren
OK: zum Bestätigen einer Auswahl oder eines Werts
6. **Taste zur vollständigen Aktivierung des Systems**
7. **Taste zur Teilaktivierung des Systems**
8. **Taste zur Deaktivierung des Systems**
9. *****: wird diese Taste 3 Sekunden lang betätigt, gelangt man in das Techniker-Menü
10. **#**: wird diese Taste 3 Sekunden lang betätigt, gelangt man in das Benutzer-Menü
11. **Interne Sirene**
12. **Tastaturabdeckung**
13. **Auslegung für Wandmontage.**
14. **Schalter zur Aktivierung der wiederaufladbaren Pufferbatterie**
15. **Klemmleiste Netzversorgung**
16. **Aufnahme für SIM-Telefonkarte**
17. **Ethernet-Port für lokale Programmierung**
18. **Sabotageschutzvorrichtung (Tamper) Stellt eine Beschädigung durch Öffnen des Gehäuses oder Abreißen von der Wand fest**

2.2 EINSETZEN DER SIM-GSM-KARTE (OPTION)

Die Zentrale 1051/020 setzt zur Überwachung und Steuerung der System- und Gerätestatus die integrierte 4G-Konnektivität ein. Zur Verwendung der 4G-Funktion muss eine für die Nutzung von Sprachnachrichten und Daten aktivierte SIM-Karte in die Zentrale eingesetzt werden.

Die GSM-SIM-Karte muss in den dafür vorgesehenen Einschub auf der Zentralenrückseite eingelegt werden:



SIM-EINSCHUB

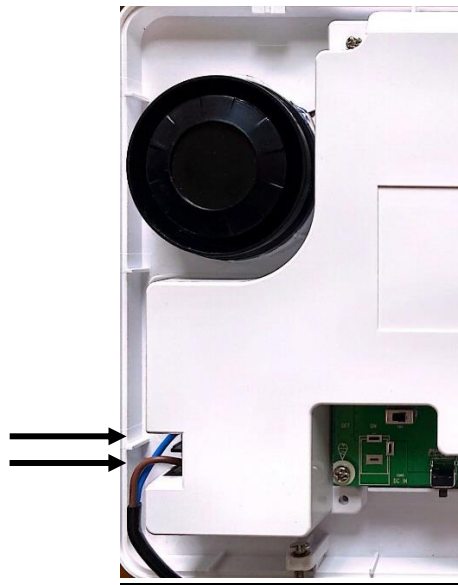
- Verschieben Sie den Kartenhalter nach links, um den Einschub freizulegen
- Heben Sie den Kartenhalter an und legen Sie die SIM-Karte vorsichtig mit nach unten gerichteten Kontakten ein
- Klappen Sie den Kartenhalter wieder nach unten und schieben Sie ihn nach rechts, um den Einschub zu sperren

<HINWEISE>

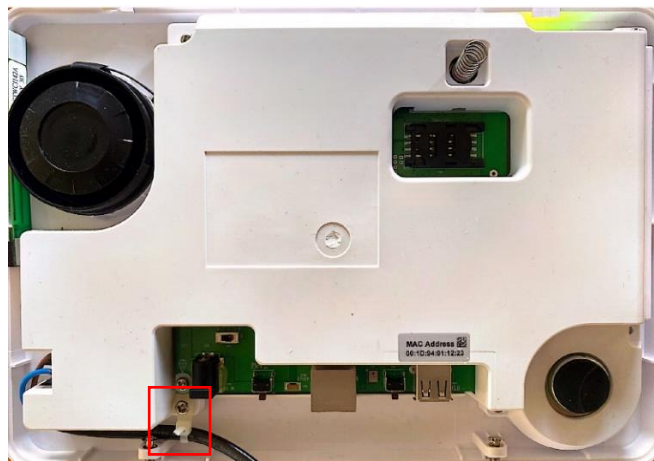
Deaktivieren Sie den PIN-Code der SIM-Karte vor dem Einlegen in die Zentrale, wenn dies nicht bereits geschehen ist (es ist möglich, für diese Art Anwendungen vorgesehene SIM-Karten zu verwenden).

2.3 VERSORGUNG

Die Zentrale 1051/020 wird über das Stromnetz (230 VCA) versorgt. Schließen Sie das im Lieferumfang enthaltene Kabel an die beiden Klemmen seitlich der Zentrale an, wie in den untenstehenden Abbildungen angegeben.



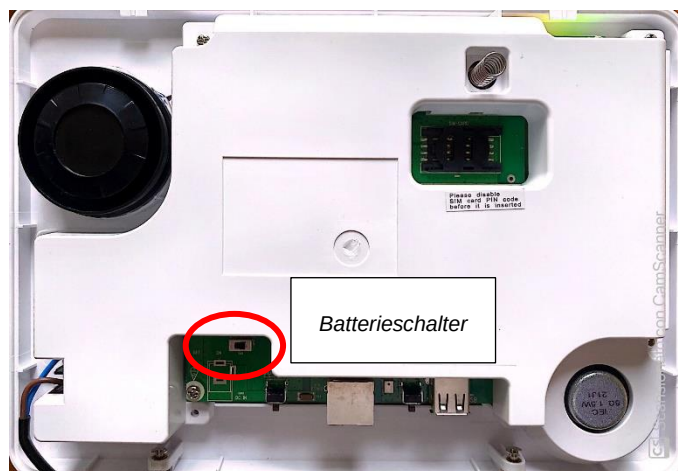
Verwenden Sie die im Lieferumfang enthaltene Schelle mit Schraube, um das Kabel in der unten angegebenen Position zu befestigen und führen Sie das Kabel an der dafür vorgesehenen Stelle an der Unterseite nach außen.



Bringen Sie dann die rückseitige Abdeckung der Zentrale wieder an und verschrauben sie diese mit den beiden Schrauben.

WICHTIGER HINWEIS: NEHMEN SIE DEN ANSCHLUSS AN DIE STROMVERSORGUNG ERST AM ENDE DER VORGÄNGE VOR.

Wiederaufladbare Batterie



- Im Inneren der Zentrale befindet sich eine wiederaufladbare Batterie, die im Fall eines Stromausfalls als Pufferbatterie dient.
- Während des normalen Betriebs wird zum Versorgen der Zentrale und gleichzeitigen Wiederaufladen der Batterie die Netzstromversorgung verwendet. Zum vollständigen Aufladen der Batterie sind ca. 72 Stunden erforderlich.

Die werkseitige Position des Batterieschalters ist **OFF**. Unter diesen Bedingungen wird die Batterie nicht aufgeladen, wenn die Zentrale an das Stromnetz angeschlossen ist und kann bei einem Stromausfall nicht als Pufferbatterie fungieren. Der Schalter muss daher auf **EIN** gestellt werden, um den Betrieb zu garantieren.

<HINWEIS>

- Bei einem Stromausfall wird, wenn die Batterie fast entladen ist, über Fernkommunikationen auf die entladene Batterie hingewiesen und die interne Sirene wird zur Energieeinsparung deaktiviert.
- Die Betriebsdauer der nur mit Batterie versorgten Zentrale beträgt ca. 15 Stunden.
- Wird die Zentrale nur mit der Batterie betrieben, kommt eine Betriebsart mit geringem Energieverbrauch zum Einsatz, bei der die WLAN-Verbindung deaktiviert und die Interaktionen mit den Fernverbindungen eingeschränkt werden: Es werden weiterhin Meldungen der Ereignisse versandt, doch die Zentrale kann keine Fernsteuerungen empfangen, sollte die Fernverbindung über die APP erforderlich sein. Da auch der Router von der Versorgung getrennt sein könnte, ist die Kommunikation natürlich garantiert, wenn die Zentrale mit einer SIM ausgestattet ist.

2.4 AUFZEICHNUNG DER SPRACHNACHRICHTEN

Die Zentrale 1051/020 ist in der Lage, eine eigene Sprachnachricht mit der Identifizierung der Wohnung des Benutzers aufzuzeichnen. Die Nachricht wird an die Zentrale versandt und im Alarmfall zusammen mit der Beschreibung des eingetretenen Ereignisses wiedergegeben.

Die maximale Dauer der Nachricht beträgt 10 Sekunden.

Hinsichtlich der Aufzeichnung der Nachricht siehe Handbuch zur Bedienung und Programmierung mittels Tastatur.

3 INSTALLATION

3.1 GRUNDVORAUSSETZUNGEN

Die Zentrale ist für die Wandmontage ausgelegt. Für eine korrekte Installation wird empfohlen, die folgenden Leitlinien zu berücksichtigen:

- Die Zentrale erfordert eine Ethernet-Verbindung und das Hinzufügen einer SIM-Karte ist empfehlenswert.
- Die Zentrale muss in einer von außen nicht einsehbaren Position installiert werden.
- Vermeiden Sie es, die Zentrale in der Nähe großer Metallgegenstände zu montieren, die die Stärke der Funksignale beeinträchtigen könnten.
- Die Zentrale muss mit Hilfe von Detektoren geschützt werden, damit keine Eindringlinge in Ihre Nähe gelangen können, ohne dass zuvor ein Alarm ausgelöst wurde.

3.2 SCHRITTE ZUR MONTAGE DER ZENTRALE

Schritt 1. Die Schrauben unten an der Zentrale (**Abbildung 1**) lösen und die hintere Abdeckung der Zentrale entfernen, indem diese nach oben geschoben wird, um das Beschädigen der Befestigungen im Inneren zu vermeiden.

Schritt 2. Die hintere Abdeckung weist 4 vorgestanzte Bereiche auf, an denen die Öffnungen für die Wandmontage angebracht werden können (**Abbildung 2**). Am Rand der Abdeckung befinden sich außerdem weitere vorgestanzte Öffnungen für das Durchführen der Kabel.

Abbildung 1

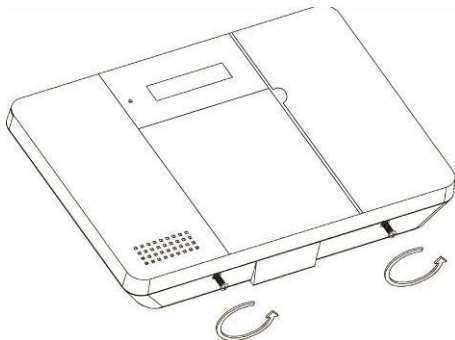
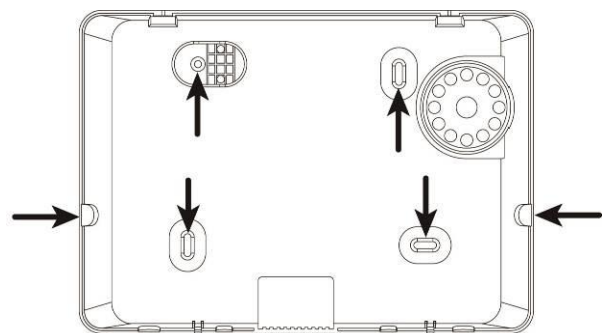


Abbildung 2



Schritt 3. Verwenden Sie die Basis als Schablone, um die Positionen der Montagebohrungen an der Wand anzuzeichnen (**Abbildung 3**). Befestigen Sie die Zentrale mit den im Lieferumfang enthaltenen Dübeln an der Wand (**Abbildungen 4 und 5**).

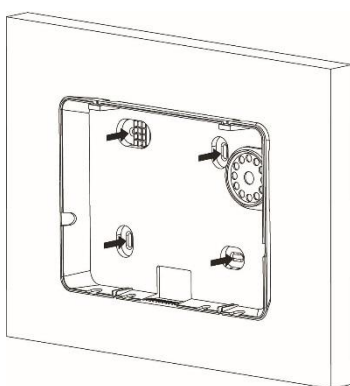


Abbildung 3

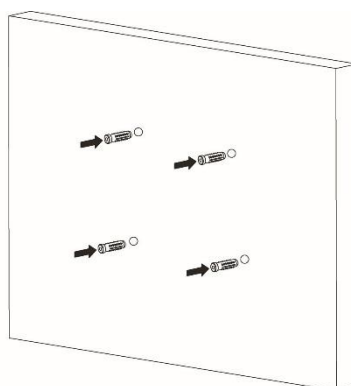


Abbildung 4

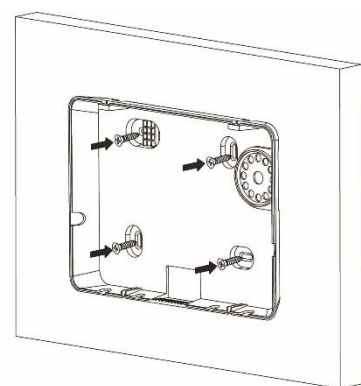


Abbildung 5

Schritt 4. Schließen Sie das mit der Zentrale gelieferte Ethernet-Kabel an. (**Abbildung 6**)

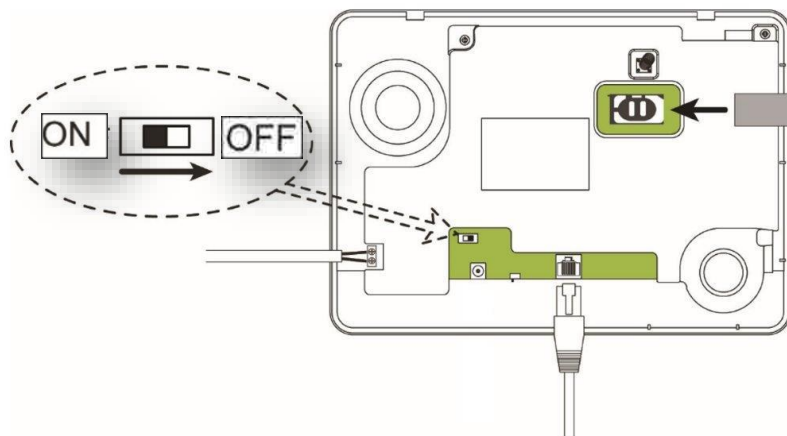
Sollte die Absicht bestehen, die 4G-Verbindung zu nutzen, eine SIM-Karte in den entsprechenden Sitz einführen. Vergewissern Sie sich vor dem Einführen der SIM-Karte, dass der PIN-Code der Karte deaktiviert wurde.

HINWEIS: Es kann eine gewisse Zeit in Anspruch nehmen, bis sich die SIM im Mobilfunknetz registriert. Nach dem Einschalten der Zentrale ist daher vor ihrer Verwendung einige Minuten abzuwarten.

HINWEIS 2: Sollte die WLAN-Verbindung mit dem Router verwendet werden können, muss das Netzkabel abgetrennt werden.

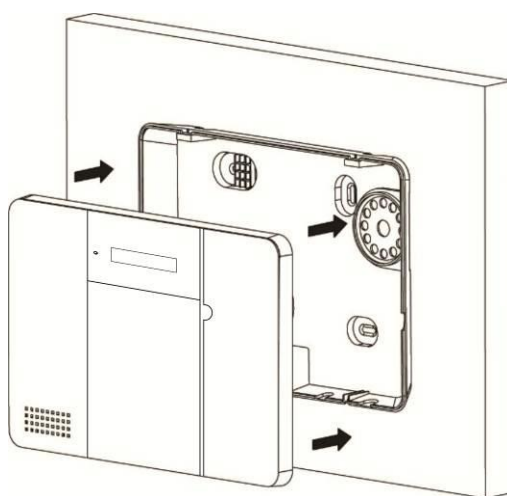
Schritt 5. Versorgen Sie die Zentrale mit Strom und schieben Sie den Batterieschalter in Position ON.

Abbildung 6



Schritt 7. Lassen Sie die Zentrale an der Basis einrasten und befestigen Sie sie mit den dazu vorgesehenen Schrauben (**Abbildung 7**).

Abbildung 7



3.3 PROGRAMMIERUNG DER ZENTRALE 1051/020

Die Zentrale kann für ihre Verwendung über einen PC programmiert werden:

Anforderungen des PC

Um das System zu installieren, muss der Computer, mit dem die Programmierung erfolgen soll, die folgenden Anforderungen erfüllen:

- Betriebssystem Microsoft Windows 98, ME, NT4.0, 2000, XP, Vista, 7, 8, 10 oder 11.
- Google Chrome (empfohlen) oder Firefox. Von der Verwendung von Internet Explorer wird abgeraten.
- CPU: Intel Pentium II 266 MHz oder höher
- Speicher: 64 MB oder mehr
- VGA-Auflösung: 800x600 oder höher

VORBEREITUNG DES LOKALEN NETZWERKS (LAN) UND DES INTERNETS (WAN)

Anforderungen für die Internetverbindung

Um den vollumfänglichen Betrieb des Systems Zeno zu garantieren, muss die Zentrale wie folgt angeschlossen sein:

1. mittels Ethernet-Kabel oder WLAN-Verbindung an einen ADSL-Router

und/oder:

2. mittels einer für den Datenverkehr aktivierten SIM-Karte, die in die Zentrale eingesteckt wird, an das Mobilfunknetz 4G.

Um größte Sicherheit und höchste Leistungen zu garantieren, ist es empfehlenswert, beide Verbindungen vorzusehen:

- ☞ das ADSL-Netz gestattet bessere Leistungen beim Fernzugriff und beim Laden von Videos und Fotos
- ☞ die doppelte Verbindung garantiert, dass im Fall des Ausfalls einer der beiden das System weiter und unter Verfügbarkeit aller Funktionen in Betrieb bleibt

Für den korrekten Betrieb sind auf dem Router weder die Port Forwarding-Funktion noch der DDNS-Dienst (Dynamic Domain Name System) erforderlich. Empfehlenswert ist dagegen die Aktivierung des DHCP-Servers direkt auf dem Router.

Anschluss der Zentrale an einen PC zur Inbetriebnahme

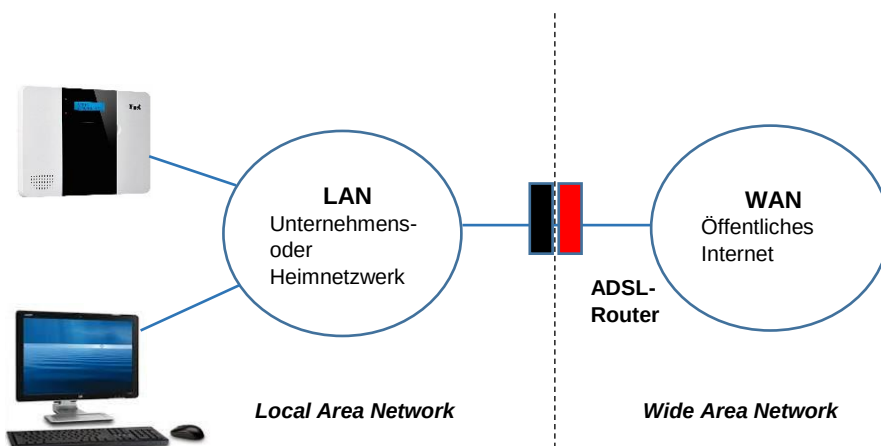
Die Inbetriebnahme der Zentrale muss über einen PC erfolgen.

Die Verbindung kann mittels zwei Anschlussarten über Kabel erfolgen:

- ☞ über einen zur Verbindung der Zentrale mit dem Internet verwendeten ADSL-Router und Anschluss mit dem im Lieferumfang enthaltenen Ethernet-Kabel (empfohlen)
- ☞ über direkten Anschluss an den PC mit dem im Lieferumfang enthaltenen Ethernet-Kabel

HINWEIS: Die Programmierung kann nicht über eine WLAN-Verbindung erfolgen, hierzu ist die Verbindung mit Kabel erforderlich. Die WLAN-Verbindung kann dagegen bei Normalbetrieb eingesetzt werden.

Anschluss mit Router



Verwenden Sie für die Verbindung mit Ihrer Zentrale einen an den Router angeschlossenen PC.

Die Zentrale ist bereits darauf ausgelegt, mit dem Großteil der möglichen Netzwerkkonfigurationen in Betrieb genommen zu werden. Die werkseitigen Parameter lauten:

- IP = **192.168.1.xxx (DHCP)**
- DNS = 8.8.8.8; DNS2 = 8.8.4.4
- Gateway = 192.168.1.1
- NetMask = 255.255.255.0
- DHCP = ON

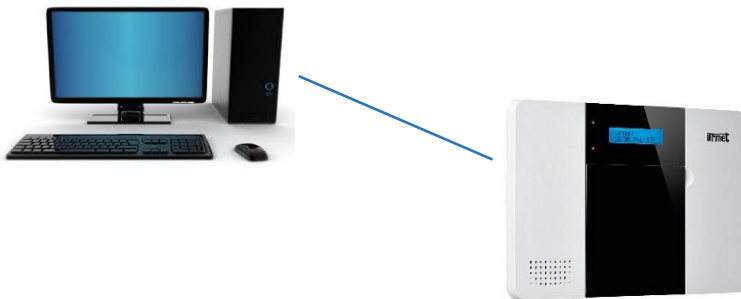
Ist der verwendete Router mit einem DHCP-Server ausgestattet, ist es empfehlenswert, die DHCP-Adresse über das Programm Finder auch auf der Zentrale beizubehalten, wie im nachfolgenden Absatz beschrieben.

Ist der Router nicht mit DHCP-Server ausgestattet, muss auf der Zentrale eine statische Adresse derselben Familie wie der des verwendeten LANs konfiguriert werden.

ACHTUNG! Ist der Router nicht mit DHCP-Server ausgestattet und auf der Zentrale wird die DHCP-Adresse aktiviert, ist diese nicht mehr erreichbar!!

<HINWEIS>

Verbindung mit Direktanschluss



Um die Zentrale mittels Direktanschluss an einen PC konfigurieren zu können, ist auf eine der folgenden beiden Arten vorzugehen:

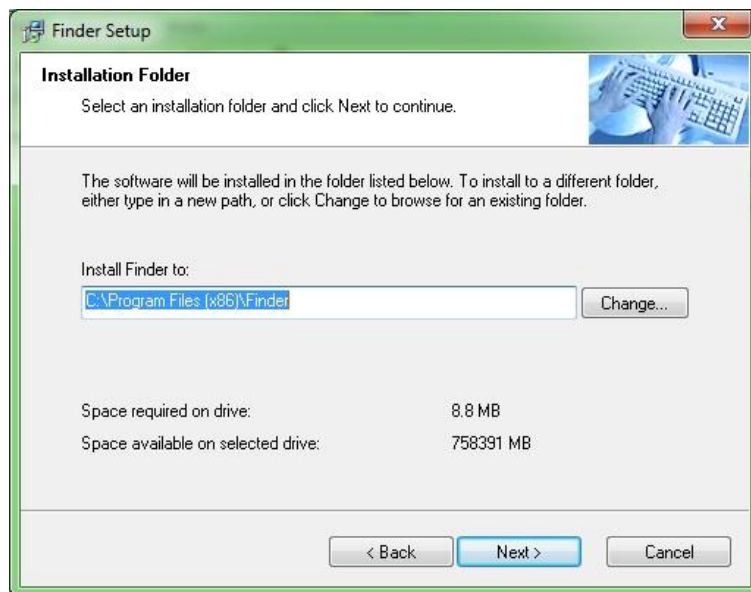
1. Konfigurieren Sie den PC mit einer IP-Adresse derselben Familie wie die der Zentrale und verwenden Sie dann eine Adresse 192.168.1.xxx (mit xxx nicht 130) und eine SUBNET MASK 255.255.255.0
2. Oder konfigurieren Sie über das Programm Finder (siehe unten) die Zentrale mit einer IP-Adresse derselben Familie wie der des PC. Gehört die Adresse des PC zum Beispiel zur Familie 192.168.0.xxx, konfigurieren Sie die Zentrale mit einer zu derselben Familie gehörenden Adresse, die jedoch von der des PC verschieden ist, und mit einer SUBNET MASK 255.255.255.0

3.4 INSTALLATION DER SOFTWARE FINDER

DIESE INSTALLATION IST NUR BEI DER ERSTEN VERWENDUNG ERFORDERLICH

Um die Zentrale zu programmieren und zu steuern, wird die spezielle Software „**Finder**“ eingesetzt (geeignet für Betriebssystem Microsoft Windows 7 oder höher), die die Identifizierung und Lokalisierung der Zentrale im lokalen Netzwerk (LAN) gestattet. Zur Installation der Software „**Finder**“:

- Schritt 1.** Begeben Sie sich auf die Website www.urmet.com und dann in den der Zentrale Zeno Cod. 1051/020 vorbehaltenen Bereich im Abschnitt Produkte-Einbruchsicherung. Am Ende dieses Handbuchs finden Sie den QR-Code des Links.
- Schritt 2.** Laden Sie die Software **Finder** herunter.
- Schritt 3.** Klicken Sie zweimal auf **Finder**, um die Installation der Applikation zu starten. Sollte Ihr PC aufgrund von Schutzvorrichtungen oder Firewalls blockieren, gestatten Sie die Installation der Applikation gemäß den vom jeweils verwendeten Betriebssystem vorgesehenen Bedingungen.

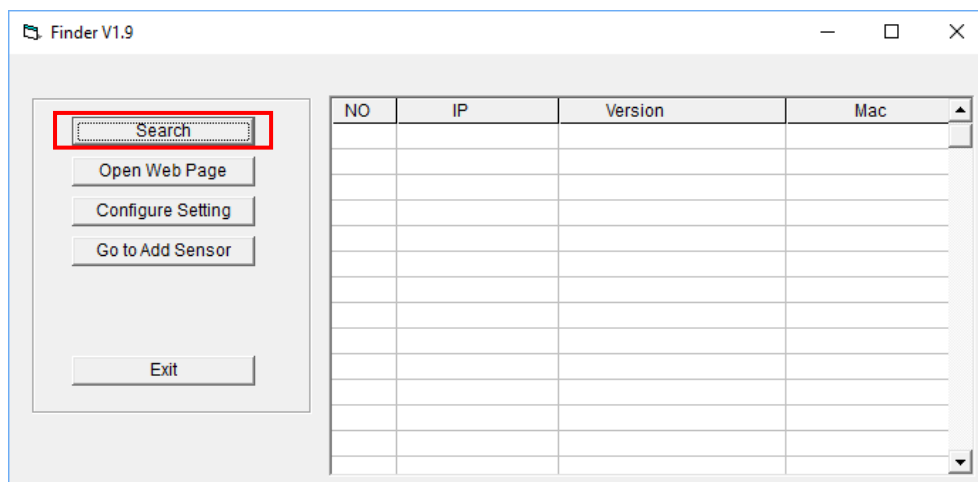


- Schritt 5.** Klicken Sie auf „**Change**“, um den Ordner der Datei auszuwählen. Besteht keine Notwendigkeit, den Pfad zu ändern, klicken Sie auf „**Next**“, um fortzufahren.
- Schritt 6.** Klicken Sie auf „**Next**“, um die Installation zu starten. Am Ende der Installation klicken Sie auf „**Finish**“.

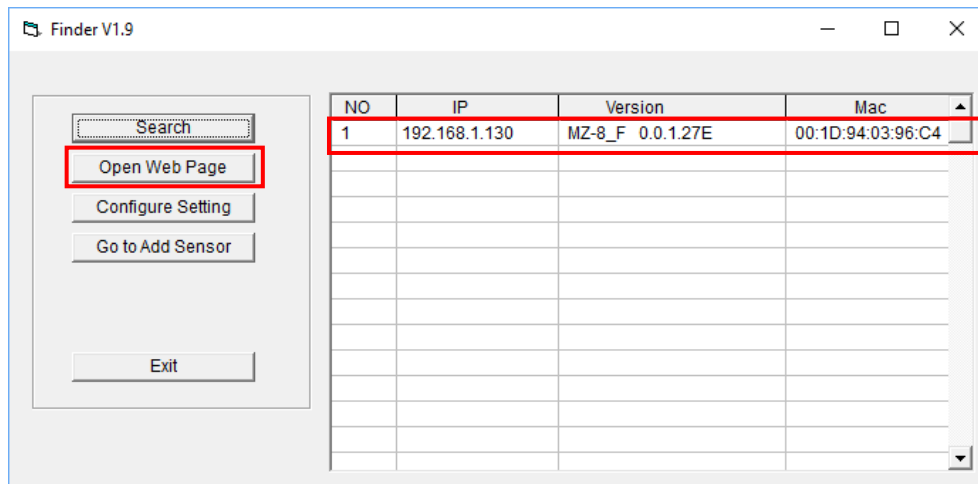


- Schritt 7.** Auf dem Desktop erscheint ein neues Symbol : **Finder.exe**

- Schritt 8.** Klicken Sie zweimal auf „**Finder.exe**“, um die Installation zu starten. Das folgende Fenster erscheint:



- Schritt 9.** Klicken Sie auf „**Search**“: das Programm beginnt mit der Suche der bekannten IP-Adressen im lokalen Netzwerk.
- Schritt 10.** Stellen Sie die IP-Adresse der Zentrale in der Liste fest. Es werden außerdem die MAC-Adresse und die Firmwareversion des Produkts angezeigt.

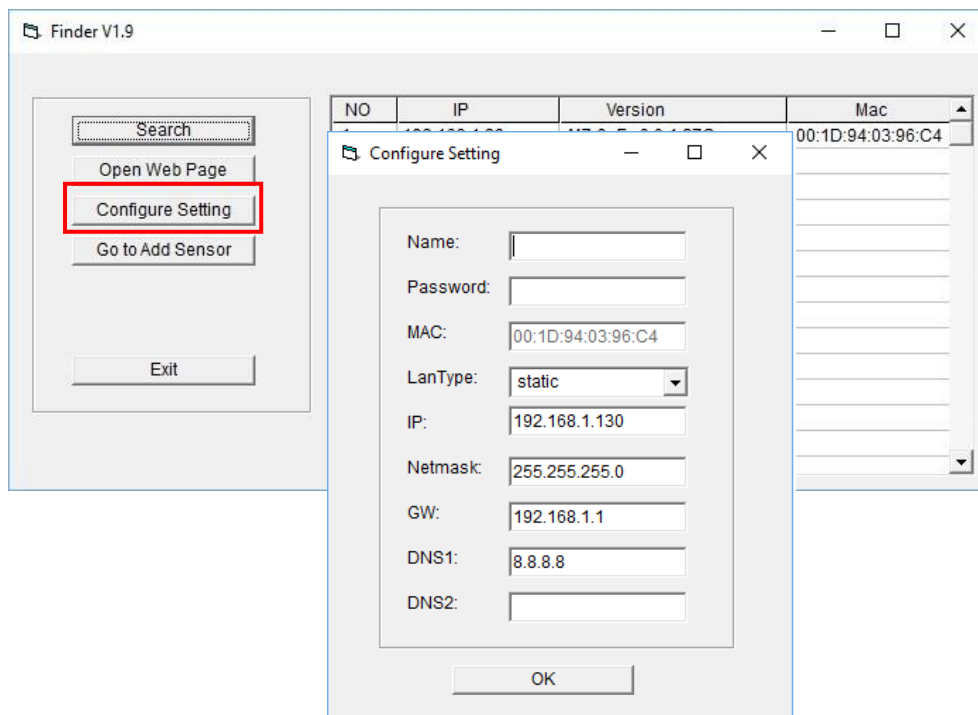


Schritt 11. Sobald die Zentrale festgestellt wurde, wählen Sie diese aus und klicken Sie auf „**Open Web Page**“, um sich mit der lokalen Bedientafel der Zentrale Zeno zu verbinden. Es wird um die Eingabe der Zugangsdaten gebeten, wie in Kapitel 4 beschrieben.

KONFIGURATION DER NETZWERKEINSTELLUNGEN DER ZENTRALE

Diese Funktion ist nur dann erforderlich, wenn die Netzwerkeinstellungen manuell konfiguriert werden sollen.

Schritt 1. Wählen Sie die Zentrale und klicken Sie dann auf **Configure Setting**: das folgende Fenster wird eingeblendet:



Schritt 2. Geben Sie den Benutzernamen und ein Passwort für die Konfiguration der Einstellungen ein.

Benutzername (Standard): **admin**

Passwort (Standard): **cX+HsA*7F1**

ACHTUNG!: um den vor kurzem ergangenen Anti-Hacker-Bestimmungen nachzukommen, verwendet die Zentrale Zeno zur Passwortgenerierung den folgenden Mechanismus. Nach der Eingabe des Standardpassworts **cX+HsA*7F1** bittet das System beim ersten Zugriff darum, dieses zu ändern und ein eigenes einzugeben. Erfolgt dies nicht innerhalb einer Stunde, verweigert das System den Zugriff und die Zentrale muss vollständig abgeschaltet und wieder eingeschaltet werden, um den kompletten Vorgang auszuführen.

HINWEIS: Im Anschluss an einen Reset auf werkseitige Einstellungen verwendet die Zentrale erneut das Standardpasswort.

Schritt 3. Auswahl von **DHCP** oder **Static** als LAN-Typ. Wird **Static** gewählt, kann mit der manuellen Eingabe der verbleibenden Netzwerkinformationen fortgefahren werden. Wird „**DHCP**“ gewählt, ist es nicht möglich, die anderen Netzwerkinformationen zu ändern.

Schritt 4. Klicken Sie, nachdem eine neue Einstellung eingegeben wurde, auf **OK**, um zu bestätigen. Sind der Benutzername und das Passwort korrekt, wird in einem Fenster die folgende Nachricht eingeblendet: **Status: Configure success!!** (Status: Konfiguration erfolgreich!)

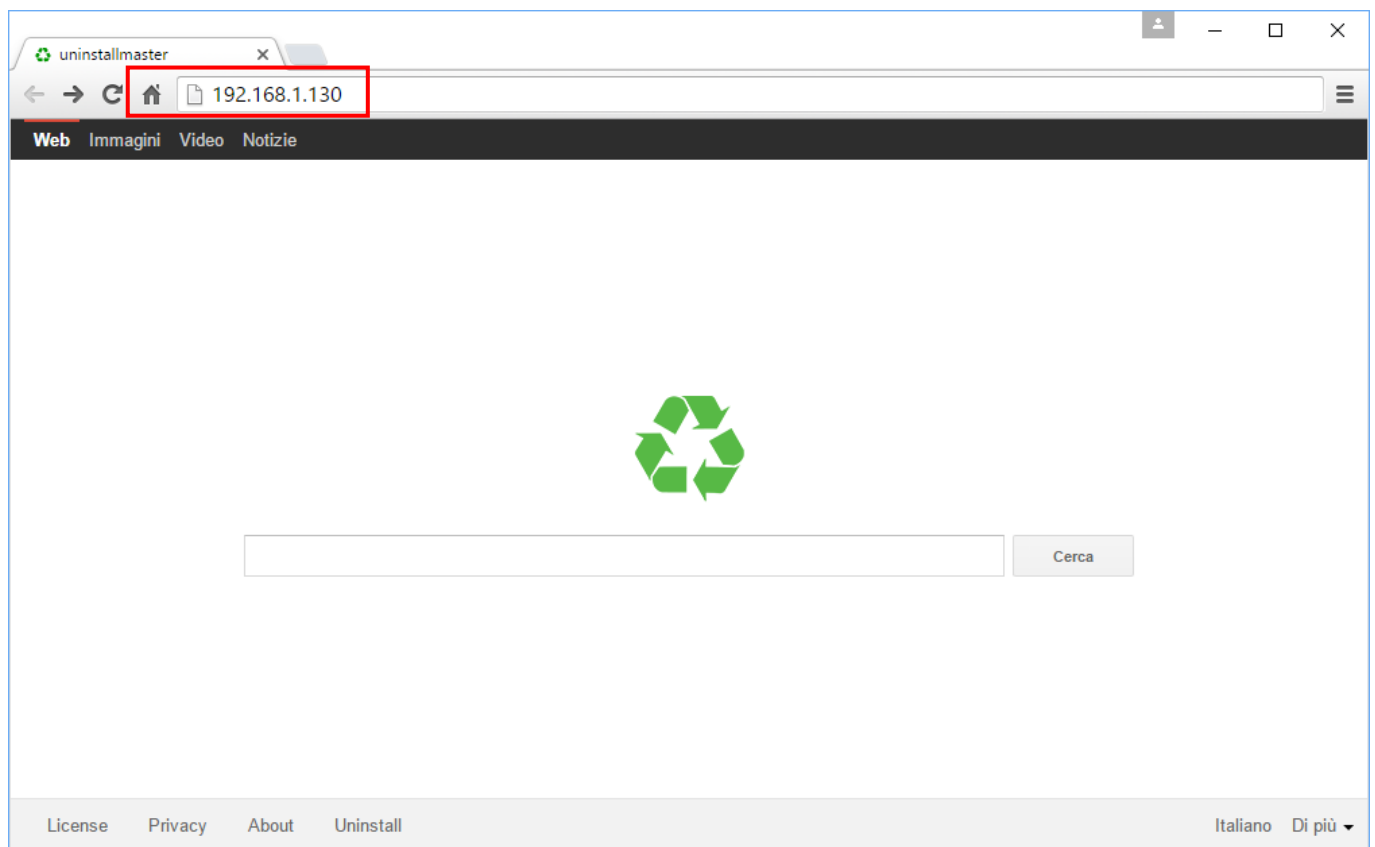
<HINWEIS>

Die Option „Go to add sensor“ steht in der vorliegenden Version nicht zur Verfügung.

4 ZUGRIFF AUF DIE WEBOBERFLÄCHE DER ZENTRALE

Schritt 1. Wählen Sie die Zentrale in der Software Finder und klicken Sie auf „Open Webpage“, um sich mit der Zentrale zu verbinden.

Alternativ dazu können Sie einen Browser verwenden und in die Adressleiste die IP-Adresse der in der Software Finder angezeigten Zentrale eingeben.



Schritt 2. Geben Sie im Fenster der Eingabe der Zugangsdaten den Benutzernamen und das Passwort ein und betätigen Sie „**Zugriff**“.

Standard-Benutzername: **admin**

Standard-Passwort: **cX+HsA*7F1**

ACHTUNG!: Um den vor kurzem ergangenen Anti-Hacker-Bestimmungen nachzukommen, verwendet die Zentrale zur Passwortgenerierung den folgenden Mechanismus. Nach der Eingabe des Standardpassworts **cX+HsA*7F1** bittet das System beim ersten Zugriff darum, dieses zu ändern und ein eigenes einzugeben. Erfolgt dies nicht innerhalb einer Stunde, verweigert das System den Zugriff und die Zentrale muss vollständig abgeschaltet und wieder eingeschaltet werden, um den kompletten Vorgang auszuführen.

HINWEIS: Im Anschluss an ein Abschalten, einen Reset oder eine FW-Aktualisierung verwendet die Zentrale erneut das Standardpasswort.

Schritt 3. Die unten abgebildete Ansicht zeigt den Zugriff auf die Weboberfläche mit den der Zentrale betreffenden Informationen an.

urmet

Allgemeine Informationen

Firmware-Version ML-PRO 0.0.2.28E BG_U-ITR-F1-BD_BL_A30.20201225 4.1.2.6.2

Firmware/RF-Version: BG_U-ITR-F1-BD_BL_A30.20201225

ZigBee-Version: 4.1.2.6.2

Z-wave-Version:

GSM-Version: Quectel EC21EFAR06A03M4G

Öffentliche IP-Adresse 80.16.165.62

Private IP-Adresse 192.168.1.124

MAC Address: 00:1D:94:12:EE:87

© 2021 Urmet

5 GERÄTEVERWALTUNG

In diesem Kapitel werden die Vorgehensweisen zum Erkennen, Bearbeiten, Entfernen und Steuern der verschiedenen Geräte ausgeführt, aus denen sich das System Zeno zusammensetzen kann. Es können bis zu **80** Geräte und insgesamt maximal **6** Melder mit Kamera oder Videokamera und insgesamt **4** IP-Kameras (INT oder EXT) erfasst werden.

Die Zentrale kann maximal 40 Zigbee-Geräte vorsehen.

5.1 EINLERNEN

Schritt 1. Betätigen Sie bei Zentrale im Status **Deaktiviert** die Taste „**Einlernen**“ im Menü „**Gerätesteuerung**“.

Einlernen Geräte

Start

Uhrzeit	Gerät	Typ	Name	RSSI	ID
Kein Element gefunden					

Gerät erkannt

Uhrzeit	Typ	RSSI	ID
Kein Element gefunden			

Betätigen Sie die Taste „**Start**“: Die Zentrale begibt sich in die Einlernphase.

Schritt 2. Betätigen Sie die Einlertaste auf dem Gerät. Für einige Geräte (siehe Bedienungsanleitungen der einzelnen Produkte) muss die Einlertaste ca. 10 Sekunden betätigt werden, um einen Einlerncode zu übertragen (zu weiteren Einzelheiten siehe Geräteanleitung).

Schritt 3. Wenn die Zentrale den Einlerncode erhält, sendet sie 2 kurze Pfeiftöne aus und zeigt die Geräteinformationen in der Ansicht an. Sendet die Zentrale dagegen einen langen Pfeifton aus, bedeutet dies, dass das Gerät bereits von der Zentrale erfasst wurde.

<Hinweis>

☞ Wenn das einzulernende Gerät bereits zuvor eingelernt wurde, erscheint es im Abschnitt der **Eingelernten Geräte**.

Schritt 4. Betätigen Sie „**Hinzufügen**“, um das Gerät in die Zentrale aufzunehmen. Das Gerät wurde in das System eingelernt.

<Hinweis>

Die Zentrale ist nur in der Lage, den Überwachungstest auf den Geräten auszuführen, wenn der Überwachungstest zuvor im Untermenü „**Einstellungen Zentrale/Überwachung**“ aktiviert wurde. Werden die Geräte dagegen bei deaktiviertem Überwachungstest eingelernt, ist es nicht möglich, diesen im Anschluss zu aktivieren und die Geräte, die dem Überwachungstest unterzogen werden sollen, müssen gelöscht und erneut eingelernt werden.

Schritt 5. Führen Sie den Vorgang von Schritt 2 bis Schritt 4 aus, um weitere Geräte zu erfassen. Um den Einlernmodus der Zentrale zu verlassen und zum Normalbetrieb zurückzukehren, klicken Sie auf die Taste „**Stopp**“.

Schritt 6. Wird erneut das Menü „**Home**“ angeklickt, werden alle zuvor eingelernten Geräte eingeblendet.

Geräteliste										
Gerät	Typ	Name	Zustand	Batterie	Tamper	Ausschluss	RSSI	Status		
1	IR	Sensore Sala				No	N/D		Bearbeiten	Löschen
2	Magnetkontakt	contatto cucina				No	N/D		Bearbeiten	Löschen
3	IR					Tamper	No	Stark, 9	Bearbeiten	Löschen

Bedeutung der Spalten:

- **Gerät:** Nummer der Geräteeingabe
- **Typ:** Gerätetyp
- **Name:** Name, der dem Gerät im Inneren des Systems zugeordnet werden kann
- **Zustand:** Betriebsstatus des Geräts (zum Beispiel wird angegeben, ob es außer Betrieb ist)
- **Batterie:** Batteriestatus (es wird angegeben, ob die Ladung schwach ist)
- **Schutz:** Sabotagestatus (Tamper) des Geräts
- **Umgehung:** Zeigt den Status der ständigen oder vorübergehenden Deaktivierung des Geräts an
- **RSSI:** Funksignalstärke, gemessen von 1 bis 9. Bei einer Stärke von unter 3 wird die Kommunikation noch garantiert, doch es wird empfohlen, eine Position zu suchen, die eine größere Reichweite garantiert
- **Status:** Informationen zum Gerätestatus

Bedeutung der Steuerungen:

- **Bearbeiten:** Gestattet das Konfigurieren des Verhaltens der Geräte (siehe unten)
- **Löschen:** Gestattet das Löschen des Geräts
- **Umgehen:** Gestattet das Umgehen des Geräts (siehe Beschreibung im Kapitel der Homepage)

- **Identifizieren:** Gestattet das Identifizieren einiger Gerätetypen (siehe Beschreibung im Kapitel der Homepage)

5.2 WALK TEST

Der Walk Test muss verwendet werden, um das Vorhandensein der Geräte, ihre Funkreichweite und die korrekte Alarmgenerierung zu überprüfen.

<Hinweis>

Für die Tests der Reichweite der Bewegungsmelder siehe jeweilige Bedienungsanleitungen.

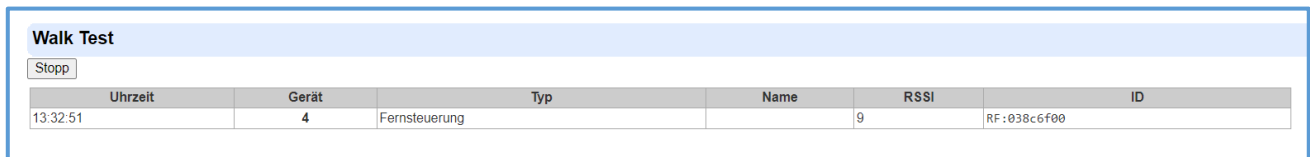
Schritt 1. Wählen Sie das Untermenü „Walk Test“ des Menüs „Gerätesteuerung“.



Betätigen Sie die Taste „Start“: Die Zentrale gibt sich in die Testphase.

Schritt 2. Betätigen Sie die Einlerntaste auf dem Gerät, um einen Testcode zu übertragen (zu Einzelheiten siehe Anleitung des Geräts) bzw. einen Alarm zu generieren.

Schritt 3. Wenn die Zentrale den Testcode erhält, sendet sie einen „langen Pfeifton“ aus und zeigt die Informationen des Geräts in der Ansicht an. Unter diesen ist insbesondere die Reichweite des Geräts zu überprüfen (Spalte RSSI).



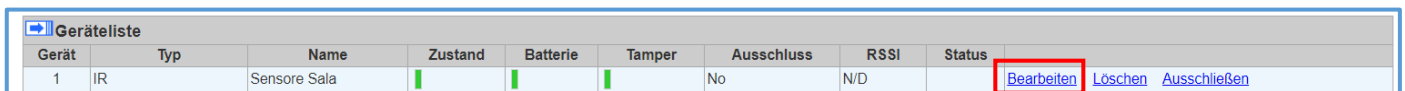
Schritt 4. Klicken Sie, um den Walk Test abzuschließen und die Zentrale in den normalen Betriebszustand zu versetzen, auf die Taste „Stopp“.

HINWEIS: Der Wert des Funksignals (RSSI) der IP-Kamera hat keine Bedeutung, da die Verbindung mit der Kamera des Typs IP ist.

5.3 BEARBEITEN DER GERÄTE

Nachdem ein Gerät im System erfasst wurde, kann in der Ansicht „Home“ die Bearbeitung seiner Einstellungen erfolgen.

Schritt 1. Klicken Sie auf dem Gerät, das programmiert werden soll, auf **Bearbeiten**.



Schritt 2. Die Einstellungen von Meldern, Funksteuerungen, Tastaturen, Foto-/Videogeräten und Sirenen werden auf den nachfolgenden Seiten beschrieben. Klicken Sie nach der Eingabe der gewünschten Einstellungen und Informationen auf die Taste **Absenden**.

5.3.1 Detektoren

Gerät bearbeiten

Magnetkontakt

ID: RF:00818810

Version:

Reserviert:

Name:

Tag:

Gerät:

Attribut: ☐ Dauerhafter Ausschluss

Attribut: ☒ Latch report

Attribut: ☐ Einst/Unsetz

Attribut: ☐ 24 STD:

Deaktivierung ->:

Vollaktivierung ->:

Heim Akt A ->:

Heim Akt B ->:

Heim Akt C ->:

Trigger-Aktivierung:

Reaktivierung:

Ausgang: ☒ Keine

Oder [Löschen](#)

Bedeutung der Felder

- **ID:** Geräteidentifizierung, nicht bearbeitbares Feld.
- **Version:** Nicht verfügbar. Für zukünftige Anwendungen.
- **Name:** Geben Sie den Namen für das Gerät ein. Es sind maximal 27 Zeichen zulässig.
- **Tag:** Nicht verfügbar. Für zukünftige Anwendungen.
- **Zone:** Nummer des Geräts, normalerweise ist es nicht notwendig, diese zu ändern, ändern Sie sie nur bei besonderen Anforderungen.
- **Attribut: Ständiger Bypass (Umgehung):** Diese Option deaktiviert (umgeht) das ausgewählte Gerät, bis die Funktion wieder abgewählt wird. Die vom Gerät versendeten Meldungen der entladenen Batterie und der Sabotage werden in jedem Fall angezeigt. Um die Meldungen vollständig auszuschließen, muss das Gerät entfernt werden.

ACHTUNG! Der ständige Bypass deaktiviert Folgendes nicht:

- **Die Sirenen, er schließt nur den Versand der Störungsmeldungsberichte in Bezug auf die Sirenen aus.**
- **Die Geräte der Home Automation, er schließt nur deren Überwachungsnachrichten aus.**
- **Den audiovisuellen Alarm auf dem Rauchmelder.**

Für die Funktion „vorübergehender Bypass“ des Geräts siehe Absatz **6.2. Funktion „Geräteumgehung“**.

- **Attribut: Gespeichert:** Diese Option wird nur für Fernbedienungen und für zum Aktivieren des Systems verwendete Türkontakte verwendet. Gestattet es, festzulegen, ob die Ereignisse in Bezug auf dieses Gerät unter den Systemereignissen gespeichert werden sollen. Es wird empfohlen, diese Option aktiviert zu lassen.
- **Attribut: Einst/Unsetz:** Diese Option gestattet es, die Türkontakte zum Aktivieren und Deaktivieren des Systems zu verwenden. Wird „**Schließer**“ ausgewählt, befindet sich der Türkontakt in Ruheposition, wenn er geöffnet ist. Wenn der Türkontakt geschlossen wird, wird das System vollständig aktiviert. Wird „**Öffner**“ ausgewählt, befindet sich der Türkontakt in Ruheposition, wenn er geschlossen ist. Wenn der Türkontakt geöffnet wird, wird das System vollständig aktiviert.

ACHTUNG! Die vollständige Aktivierung des Systems über dieses mit einem Magnetkontakt verknüpfte Attribut erfolgt direkt, ohne Berücksichtigung eventueller im System vorhandener Fehler und ohne Aktivierung der Ausgangszeit.

- **24H:** Ist dies ausgewählt, wird der Alarm, ungeachtet des Aktivierungsstatus des Systems, immer generiert. Es ist möglich, den generierten Alarmtyp auszuwählen. Wird dieses Attribut ausgewählt, ist es nicht möglich, die Attribute für die anderen Status auszuwählen.
- **Deaktiviert:** Die Einstellung des Attributs (siehe unten) bestimmt das Verhalten des Systems im Status Deaktiviert. Wird zum Beispiel das Attribut Klingel ausgewählt, sendet die Zentrale im Status Deaktiviert jedes Mal einen Ton aus, wenn auf dem Melder ein Alarm vorliegt. Im Status Deaktiviert ist es nicht möglich, verzögerte Alarmer vorzusehen.
- **Vollständige Aktivierung:** Die Einstellung des Attributs (siehe unten) bestimmt das Verhalten des Systems im Status Vollständige Aktivierung. Wird zum Beispiel das Attribut Diebstahl Sofort ausgewählt, generiert die Zentrale jedes Mal einen Alarm, wenn auf dem Melder ein Alarm vorliegt.
- **Teilaktivierung A:** Die Einstellung des Attributs (siehe unten) bestimmt das Verhalten des Systems im Status Teilaktivierung im Bereich A. Wird zum Beispiel das Attribut Verzögert Zeit 1 ausgewählt, generierte die Zentrale jedes Mal einen Alarm, wenn auf dem Melder ein Alarm vorliegt.
- **Teilaktivierung B:** Die Einstellung des Attributs (siehe unten) bestimmt das Verhalten des Systems im Status Teilaktivierung im Bereich B. Wird zum Beispiel das Attribut Stiller Alarm ausgewählt, generiert die Zentrale jedes Mal einen stillen Alarm, wenn auf dem Melder ein Alarm vorliegt.
- **Teilaktivierung C:** Die Einstellung des Attributs (siehe unten) bestimmt das Verhalten des Systems im Status Teilaktivierung im Bereich C. Wird zum Beispiel das Attribut Keine Antwort ausgewählt, generiert die Zentrale KEINEN Alarm, wenn auf dem Melder ein Alarm vorliegt.
- **Trigger:** Parameter zur Steuerung der Home Automation (siehe entsprechende Anleitung).
- **Trigger wiederhergestellt:** Parameter zur Steuerung der Home Automation (siehe entsprechende Anleitung).
- **Alarmer im Ausgang:** Ist dies ausgewählt, werden während der Ausgangszeit keine Alarmer generiert.

Liste der Attribute der Melder

In der nachstehenden Tabelle werden die mit den Meldern Zeno verknüpfbaren Attribute gezeigt. Jedes Attribut bestimmt das Verhalten des Systems im Alarmfall in den verschiedenen Status (System deaktiviert, vollständig aktiviert, teilaktiviert).

IST DAS ATTRIBUT DES MELDERS:	VERHÄLT SICH DAS SYSTEM WIE FOLGT, WENN AUF DEM MELDER EIN ALARM EINTRITT:
KEINE ANTWORT	Es wird kein Alarm generiert
KLINGEL	Die Zentrale sendet einen Warnton aus
DIEBSTAHL SOFORT	Es wird ein unmittelbarer Alarm generiert
VERZÖGERT ZEIT 1	Am Ende der Verzögerungszeit 1 wird ein Alarm generiert, wenn das System nicht vorher deaktiviert wird.
VERZÖGERT ZEIT 2	Am Ende der Verzögerungszeit 2 wird ein Alarm generiert, wenn das System nicht vorher deaktiviert wird.
DIEBSTAHL WEG	Wenn auf dem Sensor im Status Vollaktivierung oder Teilaktivierung ein Alarm eintritt, wird ein umgehender Alarm generiert. Tritt auf dem Sensor während der Eingangszeit ein Alarm ein, wird am Ende der Verzögerungszeit ein Alarm generiert, wenn das System nicht vorher deaktiviert wird.
DIEBSTAHL AUSSEN	Es wird ein umgehender Alarm generiert, der als Außen identifiziert wird
DIEBSTAHL STILL	Es wird ein umgehender stiller Alarm generiert, d. h., ohne Aktivierung der akustischen Alarme (Innen- und Außensirene)

Hinweis

Im Menü des Displays der Zentrale sind die folgenden Attribute nicht vorhanden, die dagegen in der Tabelle angegeben sind: Diebstahl Weg, Diebstahl außen, Diebstahl still.

Sollten diese bei der Programmierung über PC ausgewählt werden, würden Sie auf dem Display nicht angezeigt, jedoch korrekt funktionieren.

5.3.2 Funksteuerung und Tastatur

Bedeutung der Felder

Gerät bearbeiten

Fernsteuerung

ID: **RF:038c6f00**

Version:

Reserviert:

Name:

Tag:

Gerät:

Attribut: ☐ Dauerhafter Ausschluss

Attribut: ☒ Latch report

Attribut: Paniktaste:

Attribut: Gesamt-Taste:

Attribut: Teil-Taste:

Attribut: Deaktivieren-Taste:

Attribute: Home Mode:

Oder [Löschen](#)

- **ID:** Geräteidentifizierung, nicht bearbeitbares Feld.
- **Version:** Nicht verfügbar. Für zukünftige Anwendungen.
- **Name:** Geben Sie den Namen für das Gerät ein. Es sind maximal 27 Zeichen zulässig.
- **Tag:** Nicht verfügbar. Für zukünftige Anwendungen
- **Zone:** Nummer des Geräts, normalerweise ist es nicht notwendig, diese zu ändern, ändern Sie sie nur bei besonderen Anforderungen.
- **Attribut: Ständiger Bypass (Umgehung):** Diese Option deaktiviert (Ausschluss) das ausgewählte Gerät, bis die Funktion wieder abgewählt wird. Die vom Gerät versendeten Meldungen der entladenen Batterie und der Sabotage werden in jedem Fall angezeigt. Um die Meldungen vollständig auszuschließen, muss das Gerät entfernt werden.
- **Attribut: Gespeichert:** Dieser Vorgang gestattet es, festzulegen, ob die Ereignisse in Bezug auf dieses Gerät unter den Systemereignissen gespeichert werden sollen. Es wird empfohlen, diese Option aktiviert zu lassen.
- **Attribut: Paniktaste:** Die Einstellung des Attributs (siehe unten) bestimmt das Verhalten der Panik-Taste der Funksteuerung oder der Fern tastatur. Wird zum Beispiel das Attribut Stiller Panikalarm ausgewählt, generiert das Betätigen derselben einen Panikalarm ohne Aktivierung der Sirenen.
- **Attribut: Voll-Taste:** Die werkseitigen Einstellungen (Standard) nur für Anwendungen der Home Automation ändern (siehe entsprechende Anleitung). Hinweis LUCA auf dem Display nicht vorhanden
- **Attribut: Teil-Taste:** Die werkseitigen Einstellungen (Standard) nur für Anwendungen der Home Automation ändern (siehe entsprechende Anleitung)
- **Attribut: Deaktivieren-Taste:** Die werkseitigen Einstellungen (Standard) nur für Anwendungen der Home Automation ändern (siehe entsprechende Anleitung). Hinweis LUCA auf dem Display nicht vorhanden
- **Attribut: Bereichsauswahl:** Diese Option gestattet es, festzulegen, welcher Bereich unter A, B oder C über die Teil-Taste aktiviert werden soll. Hinweis LUCA auf dem Display nicht vorhanden

Liste der Attribute der Panik-Taste der Funksteuerungen und der Tastaturen

Die nachstehende Tabelle zeigt die mit der Panik-Taste der Funksteuerung und der Zeno-Tastatur verknüpfbaren Attribute. Jedes Attribut bestimmt das Verhalten des Systems beim Betätigen der Taste.

IST DAS ATTRIBUT DER TASTE:	VERHÄLT SICH DAS SYSTEM BEI IHREM BETÄTIGEN WIE FOLGT:
DIEBSTAHLALARM	Es wird ein unmittelbarer Alarm generiert
RAUCHALARM	Es wird ein Rauchalarm generiert.
STILLER PANIKALARM	Im Fall der Aktivierungsanfrage unter Bedrohung wird ein Alarm ohne Aktivierung der Sirenen generiert
PANIKALARM	Im Fall eines Angriffs wird ein Alarm mit Aktivierung der Sirenen generiert

HINWEIS: Die auswählbaren, doch nicht in der Tabelle beschriebenen Attribute sind nicht operativ.

Hinweis

Im Menü des Displays der Zentrale sind die folgenden Attribute nicht vorhanden, die dagegen in der Tabelle angegeben sind: Diebstahl Weg, Diebstahl außen, Diebstahl still.

Sollten diese bei der Programmierung über PC ausgewählt werden, würden Sie auf dem Display nicht angezeigt, jedoch korrekt funktionieren.

Auch die Fernbedienung ist ein Gerät mit bidirektionaler Kommunikation: wenn ihre Steuerung von der Zentrale erkannt wird, bestätigt sie das Erkennen durch schnelles Blinken ihrer LED (grünes Blinken). Im Fall des nicht erfolgten Erkennens blinkt die Led dreimal langsam (rotes Blinken). Kontrollieren Sie im letzteren Fall ihre Programmierung und ihre Reichweite.

Soll die Diebstahlsicherung mit der Fernbedienung aktiviert werden, auch wenn Fehler im System vorliegen, muss die dafür vorgesehene Taste zweimal betätigt werden. Der Beginn der Zählung von Seiten der Zentrale, bestätigt, wenn vorgesehen, die erfolgte Systemaktivierung. Achten Sie auf den Ton der Zählung, um sicher zu sein, das System aktiviert zu haben und regulieren Sie eventuell im Menü „**Einstellungen Zentrale**“ die Lautstärke.

5.3.3 Geräte Foto/Video

Die Melder mit Kamera oder Videokamera und die IP-Kameras können im Untermenü „**Videogeräte**“ des Menüs „**Gerätesteuerung**“ verwaltet und konfiguriert werden



Bedeutung der Spalten und der Steuerungen

Geräte Foto/Video				
Gerät	Typ	Name		
5	IR m/Kamera		Bearbeiten Löschen	Abrufen Foto/Video Abrufen Foto/Video (No Flash)
6	IP Camera		Bearbeiten Löschen	Sehen Programmierung

- **Gerät:** Nummer der Geräteeingabe
- **Typ:** Gerätetyp
- **Name:** Name, der dem Gerät im Inneren des Systems zugeordnet werden kann
- **Bearbeiten:** Gestattet das Bearbeiten der Parameter und der Attribute des Geräts, die denen der IR-Melder entsprechen
- **Löschen:** Gestattet das Löschen des Geräts
- **Programmierung** (nur für IP-Kameras): Gestattet den Zugriff auf die Menüs der Programmierung der IP-Kamera
- **Foto-/Videoabruf:** Gestattet das Aufnehmen eines Fotos durch das Gerät, um die aufgenommenen Bilder kontrollieren zu können. Der Melder mit Kamera erfasst ein Bild, das in der Steuertafel „**Ereignisversand**“ angesehen werden kann.
- **Foto-/Videoabruf (no Flash):** Die Fotos werden ohne Hilfe des automatischen Blitzlichts aufgenommen (um die Gerätebatterien nicht zu verbrauchen)

Sollte die IP-Kamera gewählt werden, sind die aufgezeichneten Videos nach wenigen Augenblicken auf Portal, APP und lokaler Programmierschnittstelle der Kamera zu sehen. Sie sind jedoch nicht in der Ansicht „**Bildabruf**“ zu sehen.

Liste der Attribute der IP-Kameras

Gerät bearbeiten

IP Camera

ID: XF:001d940b3ddb

Version:

Reserviert:

Name:

Tag:

Gerät:

Attribut: ☐ Dauerhafter Ausschluss

Attribut: Trigger von Gerät:

Attribut: ☒ 24 STD:

Deaktivierung ->:

Vollaktivierung ->:

Heim Akt A ->:

Heim Akt B ->:

Heim Akt C ->:

Trigger-Aktivierung:

Reaktivierung:

Ausgang: ☒ Keine

OK Default Reset Oder [Löschen](#)

- **ID:** Geräteidentifizierung, nicht bearbeitbares Feld.
- **Version:** Nicht verfügbar. Für zukünftige Anwendungen.
- **Name:** Geben Sie den Namen für das Gerät ein. Es sind maximal 27 Zeichen zulässig.
- **Tag:** Nicht verfügbar. Für zukünftige Anwendungen.
- **Zone:** Normalerweise ist es nicht notwendig, die Nummer des Geräts zu ändern, ändern Sie es nur bei besonderen Anforderungen.
- **Attribut: Ständiger Bypass (Umgehung):** Diese Option deaktiviert (Ausschluss) das ausgewählte Gerät, bis die Funktion wieder abgewählt wird.
- **Attribut: Auslösung nach Zone:** Über diese 4 Optionen kann die Aufzeichnung eines Videos mit einem von 4 verschiedenen Meldern bzw. einem beliebigen in der Anlage vorhandenen Melder (Option Belieb) generierten Alarm verknüpft werden. Wählen Sie die Nummer des zu verknüpfenden Melders aus der Tabelle der Geräte oder wählen Sie Beliebig. Außer den Meldern kann eine Fernbedienung verknüpft werden: in diesem Fall wird das Video im Fall des Panikalarms versandt.
- **Attribut: 24H:** Ist dies ausgewählt, ist es jederzeit möglich, die Kamera standortfern anzuzeigen.

Sollte gewünscht werden, dass die IP-Kamera nur in bestimmten Status (deaktiviert, teilaktiviert A, B oder C, vollständig aktiviert) angezeigt werden kann, muss die Option **24H** abgewählt und das Attribut **DIEBSTAHL SOFORT** in den zuvor ausgewählten Status gewählt werden. Die anderen Attribute haben in diesem Fall keine Bedeutung.

Wird zum Beispiel die folgende Konfiguration verwendet:

Attribut: ☐ 24 STD:

Deaktivierung ->:

Vollaktivierung ->:

Heim Akt A ->:

Heim Akt B ->:

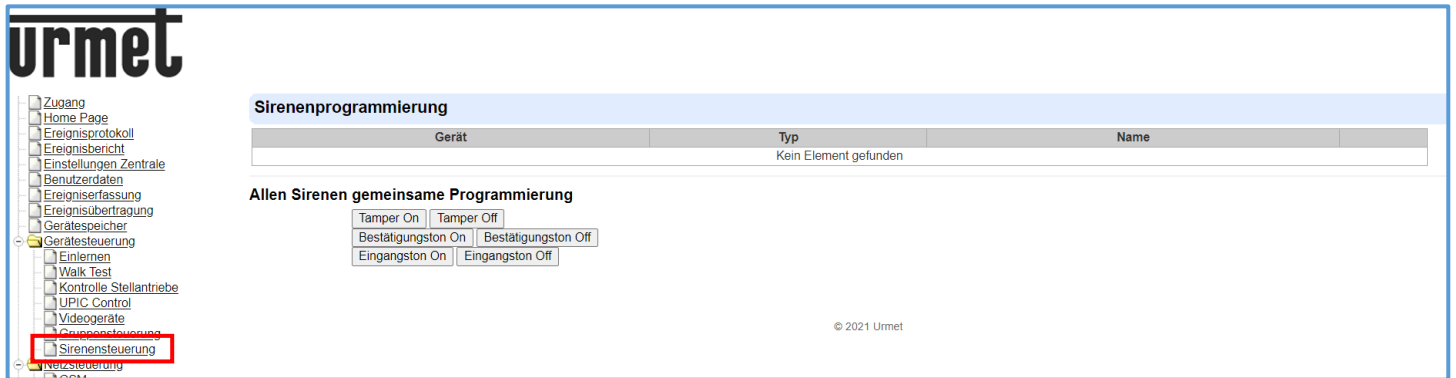
Heim Akt C ->:

ist die Kamera bei im Bereich B oder vollständig aktiven System zu sehen, während sie in den anderen deaktivierten oder aktivierten Status in den Bereichen A und C nicht zu sehen ist.

5.3.4 Sirenen

Die Sirenen können im Untermenü „**Sirenensteuerung**“ des Menüs „**Gerätesteuerung**“ verwaltet und konfiguriert werden.

Bedeutung der Spalten und der Steuerungen



- **Gerät:** Nummer der Geräteeingabe
- **Typ:** Gerätetyp
- **Name:** Name, der dem Gerät im Inneren des Systems zugeordnet werden kann
- **Tamper Ein:** Diese Option dient dem Aktivieren des Sabotageschutzes der Sirene.
- **Tamper Aus:** Diese Option dient dem Deaktivieren des Sabotageschutzes der Sirene.
- **Bestätigungston Ein:** Mit dieser Option kann entschieden werden, die Sirene einen Pfeifton als Hinweis aussenden zu lassen, wenn das System aktiviert oder deaktiviert wird.
- **Bestätigungston Aus:** Mit dieser Option wird der Hinweiston deaktiviert.
- **Eintrittston An:** Mit dieser Option kann entschieden werden, die Sirene während der Zählung der Eingangszeit einen Pfeifton als Hinweis aussenden zu lassen.
- **Eintrittston Aus:** Mit dieser Option wird der Hinweiston deaktiviert.

<Hinweise>

- ☞ Die Änderungen der Einstellung der Sirene erfolgen gleichzeitig auf allen im System vorhandenen, jedoch NICHT auf der im Inneren der Zentrale.
- ☞ Um einen versehentlichen Sabotagealarm beim Batteriewechsel oder der Änderung der Installationsposition zu vermeiden, muss zuvor der Tamper der Sirene deaktiviert werden, indem in der Änderungsansicht „Sirenen-Tamper OFF“ gewählt wird.
- ☞ Wird vergessen, den Tamper wieder zu aktivieren, wird die Erfassung in jedem Fall nach einer Stunde erneut aktiviert.

6 SYSTEMEINSTELLUNGEN

In diesem Kapitel werden die Menüs zur Basiskonfiguration des Systems behandelt.

Es wird empfohlen, bei der Systemkonfiguration die in diesem Kapitel dargestellte Reihenfolge der Ansichten einzuhalten.

6.1 ZUGANG - ALLGEMEINE INFORMATIONEN

In dieser Seite ist es möglich, die Daten der Zentrale anzuzeigen, insbesondere die Firmwareversion und die Mac Address.

Allgemeine Informationen

Firmware-Version	ML-PRO 0.0.2.28E BG_U-ITR-F1-BD_BL_A30.20201225 4.1.2.6.2
Firmware/RF-Version	BG_U-ITR-F1-BD_BL_A30.20201225
ZigBee-Version	4.1.2.6.2
Z-wave-Version	
GSM-Version	Quectel EC21EFAR06A03M4G
Öffentliche IP-Adresse	80.16.165.62
Private IP-Adresse	192.168.1.124
MAC Address	00:1D:94:12:EE:87

© 2021 Urmet

6.2 HOMEPAGE

In dieser Seite befinden sich alle Status und die wichtigsten Anlagensteuerungen.

Zugang

Home Page

Ereignisprotokoll

Ereignisbericht

Einstellungen Zentrale

Benutzerdaten

Ereigniserfassung

Ereignisübertragung

Gerätespeicher

Gerätesteuerung

Netzsteuerung

Systemsteuerung

Verlassen

Zentrale
Aktivierungsstatus: Deaktivierung

Status

Batterie	Tamper	ZigBee dongle	Störung	Stromnetz	GSM-Signal	RF-Geräusch
Batterie fehlt/leer	Normal	Normal	Normal	Normal	N/D	1

Fehlerstatus

Fehler	Meldungsdeaktivierung
SIM Non Insertita	☐ Nullstellen
Nessun segnale GSM	☐ Nullstellen
Nummer3 Tamper	☐ Nullstellen
Batterie Zentrale fehlt/entladen	☐ Nullstellen
Nummer5 Tamper	☐ Nullstellen

OK Reset

Aufladen

Gerätesteuerung

Gerät	Typ	Name	Zustand	Batterie	Tamper	Ausschluss	RSSI	Status	
1	IR	Sensore Sala				No	Stark, 9		Bearbeiten Löschen Ausschließen
2	Magnetkontakt	contatto cucina				No	Stark, 9	Tür geschlossen	Bearbeiten Löschen Ausschließen
3	IR				Tamper	No	Stark, 9		Bearbeiten Löschen Ausschließen
4	Temperatur					No	N/D		Bearbeiten Löschen Ausschließen

- **Aktivierungsstatus:** Aktivierungsstatus des Systems (aktiv/deaktiviert/teilaktiviert)

Zentrale
Aktivierungsstatus: Deaktivierung

- **Zentralenstatus:** In diesem Bereich werden die Status der Zentrale in Bezug auf Folgendes angezeigt:

Status

Batterie	Tamper	ZigBee dongle	Störung	Stromnetz	GSM-Signal	RF-Geräusch
Batterie fehlt/leer	Normal	Normal	Normal	Normal	N/D	1

- das Vorhandensein oder den Ladezustand der internen Backup-Batterie
- das korrekt geschlossene Gehäuse (Tamper)
- die korrekte Funktionsweise der Zigbee-Geräte
- das Vorliegen von Versuchen der Funkunterdrückung der Zentrale (Jamming-Interferenz)

- den Versorgungsstatus des Stromnetzes
- das Vorliegen einer GSM-Verbindung
- das Vorliegen von Funkgeräuschen in der Umgebung. Ein Wert von 0 bedeutet keine Störungen, ein Wert von 9 bedeutet ein Höchstmaß an Störungen. Der Wert muss daher niedrig bleiben, um die größte Systemzuverlässigkeit zu garantieren.
- **Fehlerstatus:** In diesem Bereich werden die eventuell im System vorliegenden Störungen aufgeführt. Da das System im Fall von vorliegenden Störungen zur Aktivierung des Systems eine doppelte Bestätigung verlangt, kann in dieser Ansicht auch festgelegt werden, ob die ausgewählten ignoriert werden und das System direkt ohne Notwendigkeit einer doppelten Bestätigung aktiviert werden soll (erneut eingegebener Code oder Zwangsaktivierung auf den Tastaturen oder erneutes Betätigen der Aktivierungstaste auf der Fernbedienung). Durch Auswahl von „Nullstellen“ und Betätigen der Taste „OK“ wird festgelegt, die Störung zu ignorieren.

Fehlerstatus	
Fehler	Meldungsdeaktivierung
SIM Non Inserita	☐ Nullstellen
Nessun segnale GSM	☐ Nullstellen
Nummer3 Tamper	☐ Nullstellen
Batterie Centrale fehlt/entladen	☐ Nullstellen
Nummer5 Tamper	☐ Nullstellen

OK Reset

- **Geräteliste:** In diesem Bereich werden die im System vorhandenen Geräte und ihre Eigenschaften aufgeführt. Es werden außerdem die Steuerungen Bearbeiten, Löschen, Umgehung und Identifizierung zur Verfügung gestellt:

Aufladen

➡

Geräteliste

Gerät	Typ	Name	Zustand	Batterie	Tamper	Ausschluss	RSSI	Status	
1	IR	Sensore Sala				No	Stark, 9		Bearbeiten Löschen Ausschließen
2	Magnetkontakt	contatto cucina				No	Stark, 9	Tür geschlossen	Bearbeiten Löschen Ausschließen
3	IR				Tamper	No	Stark, 9		Bearbeiten Löschen Ausschließen
4	Fernsteuerung					No	N/D		Bearbeiten Löschen Ausschließen
5	IR m/Kamera				Tamper	No	Stark, 9		Bearbeiten Löschen Ausschließen Identifizieren

- **Gerät:** Nummer der Geräteeingabe
- **Typ:** Gerätetyp
- **Name:** Name, der dem Gerät im Inneren des Systems zugeordnet werden kann
- **Zustand:** Betriebsstatus des Geräts (zum Beispiel wird angegeben, ob es außer Betrieb ist)
- **Batterie:** Batteriestatus (es wird angegeben, ob die Ladung schwach ist)
- **Schutz:** Sabotagestatus (Tamper) des Geräts
- **Umgehung:** Zeigt den Status der ständigen oder vorübergehenden Deaktivierung des Geräts an
- **RSSI:** Funksignalstärke, gemessen von 1 bis 9. Bei einer Stärke von unter 3 wird die Kommunikation noch garantiert, doch es wird empfohlen, eine Position zu suchen, die eine größere Reichweite garantiert
- **Status:** Informationen zum Gerätestatus (zum Beispiel der Status des Öffnens eines Kontakts)
- **Bearbeiten:** Gestattet das Bearbeiten der Einsatzparameter der Geräte (siehe Absatz 5.3 **Bearbeiten der Geräteeinstellungen**)
- **Löschen:** Gestattet das Löschen der Geräte (siehe unten)
- **Umgehen:** Gestattet das Umgehen der Geräte (siehe unten)
- **Identifizieren:** Gestattet das Feststellen einiger Gerätetypen (siehe unten)

Durch Auswahl von „Neu laden“ wird der Status der Geräte in Echtzeit aktualisiert.

Löschen eines Geräts

Um ein Gerät aus der Zentrale zu löschen, muss das entsprechende Feld ausgewählt und auf „**Löschen**“ geklickt werden: Das ausgewählte Gerät wird entfernt.

ACHTUNG! Aus Sicherheitsgründen deaktiviert die Funktion „Löschen“ die Sirenen nicht, auch wenn sie sie aus der Liste der Geräte und den Berichten der Fehlermeldungen ausschließt.

Zum Deaktivieren der Sirenen müssen diese von der Versorgung getrennt werden oder es muss ein Reset auf die werkseitigen Einstellungen erfolgen (siehe Geräteanleitung).

<Hinweis> Bleibt ein Gerät von der Zentrale getrennt, weist es einen höheren Stromverbrauch auf.

Um die Zigbee-Geräte zu löschen und für alle Geräte der Home Automation ist kein Löschbefehl erforderlich. Es genügt der Reset derselben auf die werkseitigen Werte.

Umgehen eines Geräts

Die Geräte können vorübergehend ausgeschlossen werden, indem das entsprechende Feld ausgewählt und auf „**Bypass**“ geklickt wird. Im Fall der Magnetkontakte wird das erste Eindringen vom System während der ersten Aktivierung ignoriert, alle weiteren Eindringversuche lösen dagegen den Alarm aus. Im Fall von IR-Meldern werden während des gesamten Aktivierungszeitraums keine Alarme generiert. Während dieses Zeitraums meldet das Gerät in jedem Fall eventuelle Situationen der entladenen Batterie oder Sabotage.

Diese Funktion kann verwendet werden, um versehentliche Sabotagealarme zu vermeiden, wenn die Batterien eines Geräts ersetzt werden oder seine Position verändert wird.

ACHTUNG! Die Vorübergehende Deaktivierung deaktiviert die IP-Kamera und die Geräte der Home Automation nicht. Für die Sirenen unterbindet der vorübergehende Bypass nur den Versand der Störungsmeldungsberichte. Für die Geräte der Home Automation werden die Meldungen der nicht erfolgten Überwachungen unterbunden. Für die Rauchmelder wird die Alarmmeldung auf der Zentrale jedoch nicht auf dem Gerät deaktiviert.

Identifizierung eines Geräts

Die Identifizierungsfunktion in der Ansicht der Gerätesteuerung steht nur für Zigbee-Melder und die Geräte der Home Automation zur Verfügung. Sie kann dazu verwendet werden, diese Geräte nach dem Einlernen festzustellen.

Die Identifizierungsfunktion darf innerhalb einer Minute nach dem Betätigen der Gerätetaste oder innerhalb drei Minuten nach dem Einlernen des Geräts NICHT verwendet werden. In diesen Fällen könnte das Gerät die Signale von der Zentrale nicht korrekt empfangen.

Schritt 1. Wählen Sie das Feld mit der Gerätenummer und klicken Sie unter der Liste auf „Identifizieren“.

Schritt 2. Empfängt das Gerät das Signal korrekt, blinkt die entsprechende Anzeige-Led zur Bestätigung 10 Mal. Blinkt die Geräte-Led nicht, bedeutet dies, dass das Gerät das Signal von der Zentrale nicht erhält.

- **Hinweise:** Bereich, indem es möglich ist, eigene Hinweise als Erinnerung über die Steuerung „**Bearbeiten**“ einzugeben.

Anmerkungen			
Nein.	Typ	Beschreibung	
#1			Bearbeiten
#2			Bearbeiten
#3			Bearbeiten
#4			Bearbeiten
#5			Bearbeiten

Die letzte Steuerung der Seite ([Reset Panel](#)) gestattet das Zurücksetzen der Zentrale, ohne jegliche der erfolgten Programmierungen zu ändern.

6.3 EREIGNISPROTOKOLL

In diesem Menü steht das Ereignisprotokoll der Zentrale zur Verfügung, darunter:

- ✓ Alle Alarmereignisse
- ✓ Alle Fehlerereignisse
- ✓ Alle Aktivierungs- und Deaktivierungsereignisse über Fernbedienung oder Tastatur mit den Benutzer betreffenden Informationen
- ✓ Alle Fernaktivierungs- und -deaktivierungsereignisse.

Ereignisübertragung						
Aufladen						
Uhrzeit	Gerät/Benutzer	Trigger / Restore	CID-Ereignis	Anmerkungen	Status Übertragungen	Kommentare
2024-03-19 10:48:30	0	Restore	137	Tafelsabotage Behebung	Erledigt	
2024-03-19 10:48:29	0	Trigger	137	Tafelsabotage	Erledigt	
2024-03-19 10:19:02	0	Restore	137	Tafelsabotage Behebung	Erledigt	
2024-03-19 09:47:38	0	Trigger	137	Tafelsabotage	Erledigt	
2024-03-19 09:33:48	0	Restore	137	Tafelsabotage Behebung	Erledigt	
2024-03-19 09:33:46	0	Trigger	137	Tafelsabotage	Erledigt	
2024-03-19 09:24:43	5	Trigger	383	Sabotage	Erledigt	
2024-03-19 09:23:55	0	Restore	137	Tafelsabotage Behebung	Erledigt	
2024-03-19 09:22:49	0	Trigger	602	Periodischer Test	Erledigt	
2024-03-19 09:19:41	0	Trigger	137	Tafelsabotage	Erledigt	
2024-03-19 08:38:34	0	Trigger	311	Tafel Batterie fehlt/entladen	Erledigt	
2024-03-19 08:34:38	3	Trigger	383	Sabotage	Erledigt	
2024-03-19 08:14:10	0	Restore	137	Temper. Zentrale Diagnostik	Erledigt	

- **Zeit:** Datum und Uhrzeit des Ereignisses.
- **Gerät:** Gerät, das das Ereignis ausgelöst hat.
- **Benutzer:** Benutzer, der den Vorgang in Bezug auf das Ereignis ausgeführt hat.
- **Ereignis:** Beschreibung des Ereignisses.

<Hinweis>

Die die IP-Kamera betreffenden Ereignisse stehen in dieser Ansicht nicht zur Verfügung.

6.4 EREIGNISBERICHT

In diesem Menü werden Daten angegeben, die nicht für den Benutzer, sondern für den Kundendienst bestimmt sind und zum Ausführen von Diagnosen auf der Anlage erforderlich sein können.

6.5 EINSTELLUNGEN ZENTRALE

In diesem Menü ist es möglich, einige die Zentrale und das System betreffende Einstellungen zu konfigurieren.

- **AC-Fehlerbericht:** In diesem Feld wird die Wartezeit der Zentrale angegeben, bevor im Anschluss an das Feststellen eines Stromausfalls eine Meldung generiert wird. Die werkseitige Einstellung beträgt **5 Minuten**.
- **Verzögerungszeit Energieeinsparung:** Bei einem Stromausfall begibt sich die Zentrale in den Energiesparmodus (siehe Absatz 2.4, Verwendung der aufladbaren Batterie). Diese Zeit legt fest, wie sehr der Start des Modus verzögert wird. Die werkseitige Einstellung beträgt **5 Sekunden**.
- **Staubericht** In diesem Feld wird angegeben, ob die Zentrale Funkfrequenzstörungen erfassen und in diesem Fall eine Meldung erstellen soll. Stellt die Zentrale eine Funkstörung fest, die in der Lage ist, die Kommunikationen mit den Geräten länger als 1 oder 2 Minuten zu unterbinden, meldet sie das Ereignis anhand der vorgesehenen Berichte. Der Alarm verschwindet, wenn die Störung länger als 1 oder 2 Minuten unterbleibt. Die werkseitige Einstellung beträgt **1 Minute**.
- **Auto-Check-in:** Diese Funktion gestattet die Konfiguration periodischer Tests der Zentrale intern und zu Berichtszwecken. Die werkseitige Einstellung beträgt **24 Stunden**.
- **Offset regelmäßiger Test:** Die Offset-Zeit gestattet es, festzulegen, nach wie viel Zeit der erste Bericht ab dem Einschalten der Zentrale versendet wird. Die werkseitige Einstellung beträgt **1 Stunde**.
- **Alarmbilderauflösung:** Mit dieser Funktion ist es möglich, die Einstellung der Alarmbildaufnahme der Melder mit Kamera zu bearbeiten. Folgende Optionen stehen zur Verfügung:
 - ☞ **640 x 480 x 3:** der Melder mit Kamera nimmt 3 Bilder mit Auflösung 640 x 480 auf, wenn er einen Einbruch feststellt.
 - ☞ **320 x 240 x 6:** der Melder mit Kamera nimmt 6 Bilder mit Auflösung 320 x 240 auf, wenn er einen Einbruch feststellt.
 - ☞ **320 x 240 x 3:** der Melder mit Kamera nimmt 3 Bilder mit Auflösung 320 x 240 auf, wenn er einen Einbruch feststellt.

feststellt (**Werkseitige Einstellung**)

- **Bilder in Graustufen für Außenbereiche:** Gestattet es, festzulegen, ob die Alarmbilder in Schwarz-Weiß aufgenommen werden sollen, um unter bestimmten Bedingungen ein besseres Videoergebnis zu erzielen. Die werkseitige Einstellung ist **Deaktiviert**
- **Interne Sirene:** Bei Aktivierung wird die in die Zentrale eingebaute Sirene aktiviert und sendet einen Alarmton aus, wenn ein Alarm generiert wird. Die werkseitige Einstellung ist **Aktiviert**
- **IP/4G-Defekt ignorieren:** Gestattet es, festzulegen, ob Fehlerereignisse in Bezug auf die Ethernet- oder G4-Funktion ignoriert werden sollen. Die ignorierten Fehlerereignisse werden in der lokalen Steuertafel angezeigt.
 - **Deaktiviert:** Wird Deaktiviert ausgewählt, werden keine Ereignisse ignoriert (Werkseitige Einstellung)
 - **IP:** Wird IP ausgewählt, werden die Ereignisse und die Störungen in Bezug auf die Ethernet-Funktion ignoriert.
 - **4G:** Wird 4G ausgewählt, werden die Ereignisse und Störungen in Bezug auf die Übertragung der 4G-Daten ignoriert.
 - **IP+4G:** Wird IP+4G ausgewählt, werden alle Ereignisse und Störungen in Bezug auf die Internetverbindung ignoriert.

ANMERKUNG: Die Umgehung aktiviert auch die Möglichkeit der IP- und GSM-Verbindungen

- **Sprache:** Gestattet die Auswahl der Verwendungssprache

Nachdem die vorangegangenen Einstellungen vorgenommen wurden zum Bestätigen der Änderungen die Taste „OK“ betätigen.

Weitere Einstellungen:

- **Letzte Tür:**
 - ☞ **Letzte Tür Ein:** Wird das System **Vollständig aktiviert** und ein mit dem Attribut **Verzögert** eingegebener Magnetkontakt wechselt von geöffnet auf geschlossen, wird das System aktiviert, ohne das Ende der Ausgangsverzögerung abzuwarten.
 - ☞ **Letzte Tür Aus:** Die oben beschriebene Funktion ist nicht aktiv. Die werkseitige Einstellung ist **Letzte Tür Aus**.
- **Akt.fehlertyp:**
 - ☞ **Bestätigen:** Bei dieser Einstellung wird, wenn die Aktivierung bei vorhandenen Fehlern versucht wird, eine doppelte Bestätigung zur Aktivierung des Systems verlangt (erneut eingegebener Code oder Zwangsaktivierung auf den Tastaturen oder erneutes Betätigen der Aktivierungstaste auf der Fernbedienung). Die werkseitige Einstellung ist **Bestätigen**.
 - ☞ **Direktaktivierung:** Bei dieser Einstellung erfolgt die Aktivierung des Systems bei vorhandenem Fehler direkt und ohne die Notwendigkeit einer doppelten Bestätigung.
- **Tamper:**
 - ☞ **Vollständig.** Die Sabotagealarme (Tamperalarme) werden nur im Status der vollständigen Aktivierung generiert (das Sabotageereignis wird in jedem Fall auch im Status der Teilaktivierung oder Deaktivierung gemeldet). Die werkseitige Einstellung ist **Vollständig**.
 - ☞ **Immer.** Der Sabotagealarm wird bei jedem Systemstatus generiert.
- **Überwachung:** Aktiviert/deaktiviert die Überwachung für die Zusatzgeräte. Wird innerhalb des für ein bestimmtes Gerät eingegebenen Zeitraums kein Überwachungssignal empfangen, meldet die Zentrale einen Überwachungsalarm, der dem Benutzer mitgeteilt wird. Die werkseitige Einstellung ist **Ein**.

ACHTUNG: Um den Überwachungsmodus und den damit verbundenen Alarm im Fall des nicht erfolgten Empfangs des Signals eines Geräts von Seiten der Zentrale zu nutzen, muss das Gerät mit aktiviertem Überwachungstest eingelesen werden.

Zeiteinstellung:

- **Timer Überwachung:** Gibt den Überwachungstimer für Zubehörgeräte ein. Die werkseitige Einstellung beträgt **12 Stunden**.
- **Verzögerung Eintritt 1 Voll:** Legt die Zeit fest, die dem Benutzer zur Verfügung steht, um das vollaktivierte System zu deaktivieren, wenn Alarme von den Meldern generiert werden, die die Verzögerungen von Eingang 1 vorsehen. (Für weitere Informationen siehe Absatz **5.3. Bearbeiten der Geräteeinstellungen**). Die werkseitige Einstellung beträgt **20 Sekunden**.
- **Verzögerung Eintritt 2 Voll:** Legt die Zeit fest, die dem Benutzer zur Verfügung steht, um das vollaktivierte System zu deaktivieren, wenn Alarme von den Meldern generiert werden, die die Verzögerungen von Eingang 2 vorsehen. (Für weitere Informationen siehe Absatz **5.3. Bearbeiten der Geräteeinstellungen**). Die werkseitige Einstellung beträgt **20 Sekunden**.
- **Verzögerung Verlassen Gesamt:** Legt die zur Vollaktivierung des Systems notwendige Zeit fest. Die werkseitige Einstellung beträgt **30 Sekunden**.
- **Verzögerung Eintritt 1 Teil:** Legt die Zeit fest, die dem Benutzer zur Verfügung steht, um das teilaktivierte System

zu deaktivieren, wenn Alarme von den Meldern generiert werden, die die Verzögerungen von Eingang 1 vorsehen. (Für weitere Informationen siehe Absatz **5.3. Bearbeiten der Geräteeinstellungen**). Die werkseitige Einstellung beträgt **20 Sekunden**.

- **Verzögerung Eintritt 2 Teil:** Legt die Zeit fest, die dem Benutzer zur Verfügung steht, um das teilaktivierte System zu deaktivieren, wenn Alarme von den Meldern generiert werden, die die Verzögerungen von Eingang 2 vorsehen. (Für weitere Informationen siehe Absatz **5.3. Bearbeiten der Geräteeinstellungen**). Die werkseitige Einstellung beträgt **20 Sekunden**.
- **Verzögerung Verlassen Teil:** Legt die zur Teilaktivierung des Systems notwendige Zeit fest. Die werkseitige Einstellung beträgt **30 Sekunden**.
- **Dauer Alarmaktivierung:** Bei der Aktivierung eines Alarms senden sowohl die Sirene der Zentrale als auch die Außensirene einen Alarm basierend auf der Einstellung der in diesem Feld definierten Alarmdauer aus. Die werkseitige Einstellung beträgt **3 Minuten**.

<HINWEIS> Überprüfen Sie gleichzeitig die Konfiguration der Alarmdauer der Außensirene. Wurden für lokale Steuertafel und Sirene andere Zeiten eingegeben, gilt die kürzere Zeitdauer.

Toneinstellung

Die Von der Zentrale bei den Ereignissen generierten Töne können deaktiviert (**Aus**), bei **Niedriger** Lautstärke oder **Hoher** Lautstärke ausgegeben werden:

- ☞ **Klingel:** Bei Aktivierung sendet die Zentrale einen kurzen Ton aus, wenn ein Alarm auf einem Melder mit der Klingelfunktion bei System im deaktivierten Zustand generiert wird. (Für weitere Informationen siehe Absatz **5.3 Bearbeiten der Geräteeinstellungen**.)
- ☞ **Eintrittakt.:** Bei Aktivierung sendet die Zentrale bei vollständiger Aktivierung während der Eintrittszeit Pfeiftöne aus.
- ☞ **Verl. Akt.:** Bei Aktivierung sendet die Zentrale für die vollständige Aktivierung während der Ausgangszeit Pfeiftöne aus.
- ☞ **Eintritt Home:** Bei Aktivierung sendet die Zentrale bei Teilaktivierung während der Eintrittszeit Pfeiftöne aus.
- ☞ **Verl. Home:** Bei Aktivierung sendet die Zentrale für die Teilaktivierung während der Ausgangszeit Pfeiftöne aus.
- ☞ **Bestätigung Aktivierung/Deaktivierung:** Bei Aktivierung sendet die Zentrale im Moment der Aktivierung und der Deaktivierung einen Ton aus.
- ☞ **Warnung:** Bei Aktivierung sendet die Zentrale alle 30 Sekunden Pfeiftöne aus, wenn im System ein Fehler vorliegt.
- ☞ **Tondauer Zeiten Eingang/Ausgang:** Es ist möglich, festzulegen, wie viele Sekunden lang die Zentrale während der Aktivierungen und Deaktivierungen Pfeiftöne aussendet.

<HINWEIS> Die Sirenen, die im Fall eines von einem Rauchmelder generierten Brandalarms aktiviert werden, haben einen anderen Klang als der Einbruchalarm und ertönen intermittierend.

Nachdem die vorangegangenen Einstellungen vorgenommen wurden, zum Bestätigen der Änderungen die Taste „**OK**“ betätigen.

6.6 BENUTZERDATEN

In dieser Ansicht werden die Namen der zur Benutzung des Systems freigeschaltete Benutzer angezeigt, die über APP oder das Portal eingegeben wurden. Auf dieser Seite können keine neuen Benutzer eingegeben, sondern diese nur angezeigt werden.

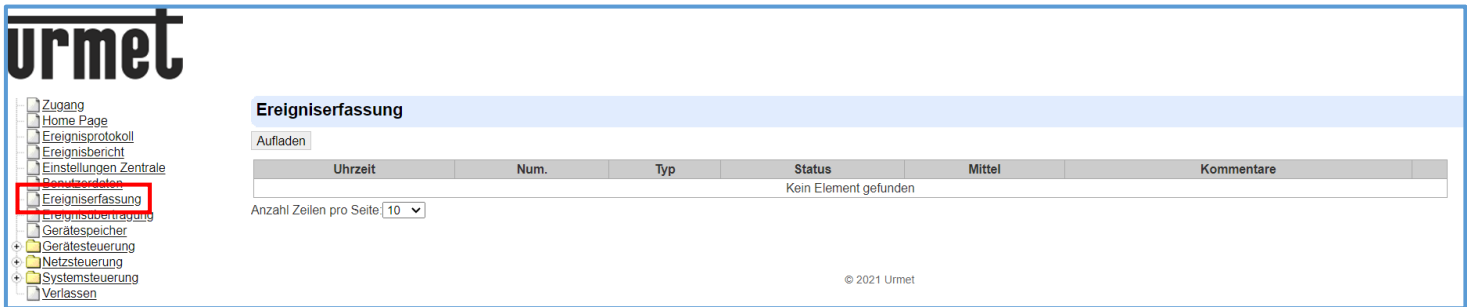
Nr.	Benutzercode	Benutzername	Sperrung	Löschen
1.	user		☒	☐
2.			☐	☐
3.			☐	☐
4.			☐	☐
5.			☐	☐
6.			☐	☐
7.			☐	☐

Aus Sicherheitsgründen werden die persönlichen Codes der Benutzer nicht angezeigt. Der werkseitige Code für den Benutzer 1 lautet **1234**.

Das Feld „**Gespeichert**“ wird verwendet, um festzulegen, ob die Aktivierungs- und Deaktivierungsvorgänge des Benutzers in der Liste der Ereignisse angegeben werden. Durch Ankreuzen des Felds wird die Aufzeichnung der Ereignisse aktiviert. Das Feld „**Löschen**“ gestattet das Löschen eventueller zusätzlicher Codes.

6.7 EREIGNISERFASSUNG

In dieser Ansicht werden die von den Meldern mit Kamera und Videokamera aufgenommenen Bilder und Videos angezeigt. Es werden nur Bilder und Videos der letzten Ereignisse gespeichert.



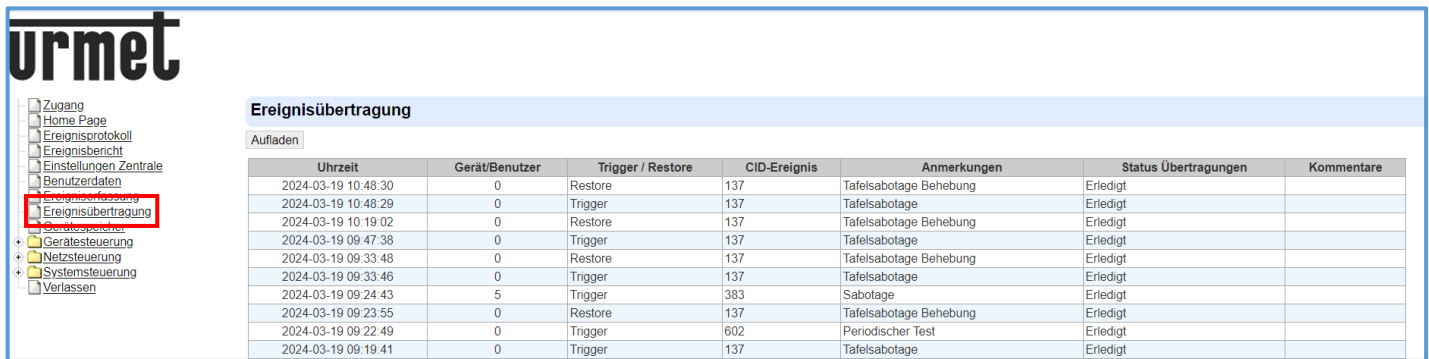
- **Zeit:** Datum und Uhrzeit der Aufnahme des Bildes/Videos.
- **Gerät:** ID-Nummer des Melders, der das Bild oder das Video geliefert hat.
- **Typ:** Typ der im Anschluss an einen Alarm oder auf Anfrage gespeicherten Bilder oder Videos.
- **Status:** Der Status des erfassten Ereignisses kann die folgenden Werte aufweisen.
 - **In Erwartung der Mediendatei:** Der Melder mit Foto- oder Videokamera hat das Bild/Video erfasst und sendet dieses an die Zentrale, sobald die Datei bereit ist. Für die Alarmbilder/-videos werden, wenn die Zentrale in diesem Status deaktiviert wird, die erfassten Bilder und Videos gelöscht und nicht versandt.
 - **In Erwartung der Erfassung:** Der Melder mit Foto- oder Videokamera versendet das erfasste Bild/Video an die Zentrale. Für Alarmbilder/-videos werden, wenn die Zentrale in diesem Status deaktiviert wird, die erfassten Bilder und Videos gelöscht und nicht versandt.
 - **Geladen:** Der Melder mit Foto- oder Videokamera hat den Versand des Bilds/Videos an die Zentrale abgeschlossen. Die Zentrale lädt nun das Bild/Video unter der programmierten Zieladresse.
 - **Verfügbar:** Die Zentrale hat das Laden des Bilds/Videos abgeschlossen.
 - **Fehlgeschlagen:** Der Melder mit Foto- oder Videokamera konnte das erfasste Bild/Video nicht an die Zentrale senden. Überprüfen Sie, ob die Foto-/Videokamera nicht defekt und ob ihre Batterie nicht entladen ist (Foto- und Filmaufnahmen benötigen viel Energie) und führen Sie dann einen Walk Test durch, um die Signalstärke zu kontrollieren.
 - **Timeout:** Der Melder mit Foto- oder Videokamera hat nicht auf die Abfrage reagiert. Überprüfen Sie, ob die Foto-/Videokamera nicht defekt und ob ihre Batterie nicht entladen ist (Foto- und Filmaufnahmen benötigen viel Energie) und führen Sie dann einen Walk Test durch, um die Signalstärke zu kontrollieren.
- **Medien:** Anzeige der gespeicherten Videos und Fotos. Klicken Sie auf das Bild oder auf den Download des Videos, um die Datei anzuzeigen.
- **Kommentare:** Status der Datenübertragungen.
- **Löschen:** Löscht das Video oder Foto aus dem internen Speicher der Zentrale

<Hinweise>

- ☞ Wird ein Alarm eines Melders mit Foto- oder Videokamera bei aktivem System generiert, deaktivieren Sie das Alarmsystem nicht, bevor der Status „Geladen“ oder „Verfügbar“ angezeigt wird. Andernfalls wird die Bilder/Videos gelöscht und nicht an die Zentrale und den Systemserver versandt.
- ☞ Die von der IP-Kamera aufgezeichneten Videos stehen in dieser Ansicht nicht zur Verfügung.

6.8 EREIGNISÜBERTRAGUNG (MENÜ FÜR SPEZIALISIERTE BENUTZER)

In diesem Menü werden alle Ereignisse aufgelistet, die während des normalen Betriebs der Zentrale nacheinander aufgetreten sind und die an den Systemserver versandt wurden:



Ereignisübertragung						
Aufladen						
Uhrzeit	Gerät/Benutzer	Trigger / Restore	CID-Ereignis	Anmerkungen	Status Übertragungen	Kommentare
2024-03-19 10:48:30	0	Restore	137	Tafelsabotage Behebung	Erledigt	
2024-03-19 10:48:29	0	Trigger	137	Tafelsabotage	Erledigt	
2024-03-19 10:19:02	0	Restore	137	Tafelsabotage Behebung	Erledigt	
2024-03-19 09:47:38	0	Trigger	137	Tafelsabotage	Erledigt	
2024-03-19 09:33:48	0	Restore	137	Tafelsabotage Behebung	Erledigt	
2024-03-19 09:33:46	0	Trigger	137	Tafelsabotage	Erledigt	
2024-03-19 09:24:43	5	Trigger	383	Sabotage	Erledigt	
2024-03-19 09:23:55	0	Restore	137	Tafelsabotage Behebung	Erledigt	
2024-03-19 09:22:49	0	Trigger	602	Periodischer Test	Erledigt	
2024-03-19 09:19:41	0	Trigger	137	Tafelsabotage	Erledigt	

Die Zentrale zeichnet insgesamt 250 gemeldete Ereignisse mit den im Anschluss beschriebenen Informationen auf:

- **Zeit:** Datum und Uhrzeit des Ereignisses.
- **Gerät/Benutzer:** Die Nummer des mit dem Ereignis verbundenen Geräts wird angezeigt.
- **Trigger/Wiederherstellung:** Definiert den Ereignistyp.
- **CID-Ereignis:**
 - Der CID-Code des Ereignisses wird in einem Format mit 4 Ziffern aufgezeichnet, bestehend aus „Kennzahl + Ereigniscode“
 - Kennzahl: „1“ steht für die auftretenden Ereignisse. „3“ steht für die Behebung der Ereignisse.
 - Ereigniscode: CID-Code des Ereignisses mit 3 Ziffern. Zum Beispiel: „1302“ bedeutet „Batterie entladen“ und „3302“ bedeutet „Wiederherstellung der entladenen Batterie“.
- **Beschreibung:** Beschreibung des Ereignisses.
- **Status:** Zeigt die erfolgte Übertragung des Ereignisses an.

<HINWEIS>

Die die IP-Kamera betreffenden Ereignisse stehen in dieser Ansicht nicht zur Verfügung.

6.9 GERÄTESPEICHER HA

In diesem Menü steht das Ereignisprotokoll der Zentrale in Bezug auf die Home Automation zur Verfügung.

7 NETZSTEUERUNG

In den Untermenüs des Menüs **Netzsteuerung** können die Netzwerkverbindungen konfiguriert werden.

7.1 GSM

In diesem Menü kann der Status des GSM kontrolliert und es können die 4G-Netzwerkeinstellungen konfiguriert werden.



- **Status:** In diesem Feld wird der Status des 4G-Moduls angezeigt (vorhandene SIM-Karte und Reichweite).
 - **IMEI:** In diesem Feld wird der IMEI-Code des 4G-Moduls angezeigt.
 - **Verbindungsbeschränkung:** Sollte das IP-, LAN- oder WLAN-Netzwerk sich als nicht verbunden erweisen und die Zentrale nur über 4G verbunden sein, ist es möglich, festzulegen, wie lange die Verbindung bei 4G bleibt, bevor wieder versucht wird, die Verbindung mit LAN oder WLAN herzustellen. Klicken Sie auf die Taste „OK“, um die eingeegebene Einstellung zu aktualisieren.
HINWEIS: „Keine Beschränkung“ ist nur zu verwenden, wenn die einzige verfügbare Verbindung 4G ist (kein LAN und kein WLAN).
 - **4G:** Um die 4G-Verbindung als Back-up-Verbindung nutzen zu können, muss dieser Abschnitt programmiert werden, um die Kommunikationen mit den Ferngeräten zu garantieren.
- ☞ **APN-Name (Zugangspunkt).** Der Name eines Zugangspunkts für 4G. Der APN-Name muss beim Telefondienstanbieter angefordert werden. Hier die APN der häufigsten Anbieter:
- **TIM:** wap.tim.it
 - **Vodafone:** mobile.vodafone.it; web.omnitel.it; m2m.vodafone.bis
 - **Vodafone HO:** web.ho-mobile.it
 - **Wind:** internet.wind; internet.wind.biz
 - **Fastweb:** apn.fastweb.it

Sobald der APN-Name eingegeben wurde, kann das System sich mit dem Internet verbinden.

☞ **Benutzer:** Der vor dem Zugriff auf die 4G-Funktionen einzugebende Zugangsname Diese Information muss, wenn erforderlich, beim Telefondienstanbieter angefordert werden.

☞ **Passwort:** Das vor dem Zugriff auf die 4G-Funktionen einzugebende Benutzer-Passwort. Diese Information muss, wenn erforderlich, beim Telefondienstanbieter angefordert werden.

- **SMS-Versand:** Die Steuerung gestattet das Versenden einer Probe-SMS.

Klicken Sie, nachdem alle Informationen eingegeben wurden, auf die Taste „OK“, um die erfolgten Einstellungen zu aktualisieren.

- **GSM-Reset.** Diese Taste dient dem Rücksetzen des in der Zentrale enthaltenen 4G-Moduls.

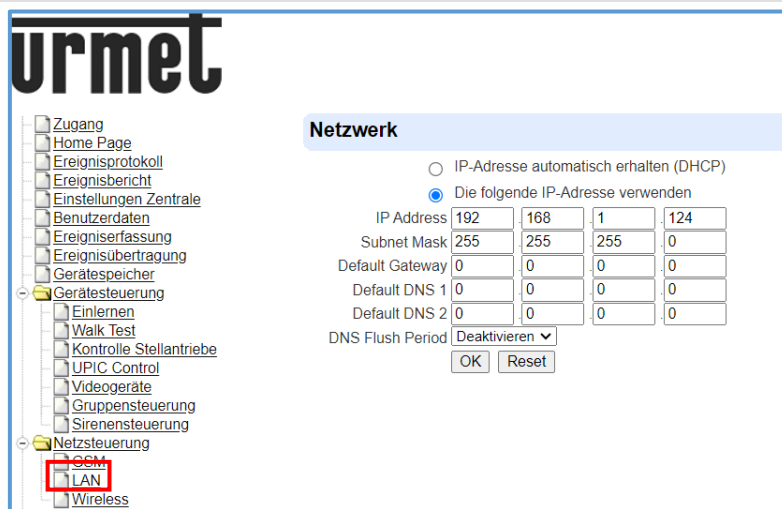
<HINWEISE>

1. Beseitigen Sie die Abfrage des PIN-Codes von der SIM-Karte (verwenden Sie ein Handy).

2. Verwenden Sie SIM-Karten mit Daten- und Gesprächsaktivierung und überprüfen Sie das Ablaufdatum.
3. Da es sich um eine Sicherungsanlage handelt wird für die SIM-Karte empfohlen, ein Abonnement abzuschließen, bei dem nicht die Gefahr besteht, kein Guthaben mehr zu haben.
4. Sollten Prepaid-SIM-Karten verwendet werden, ist regelmäßig zu überprüfen, ob die SIM-Karte ausreichend Restguthaben aufweist, um den Betrieb des GSM-Moduls zu gewährleisten.
5. Es wird empfohlen, eine Prepaid-SIM-Karte oder einen Vertrag zu aktivieren, die einen Datenverkehr von nicht weniger als 100 MB/Monat vorsehen. Der durchschnittliche Verbrauch für ADSL- und 4G-Verbindungen beläuft sich auf:
 - 50 MB/Monat für eine Verbindung mit dem Server „Always ON“ (24 Stunden täglich für alle Tage des Monats)
 - 90-140 KB für jedes Video
 - 25 KB für jedes Foto mit höchster Auflösung

URMET haftet nicht für die vorübergehende oder dauerhafte Nichtverfügbarkeit des GSM-Mobilfunknetzes, die den Versand der programmierten Informationen beeinträchtigen kann.

7.2 LAN



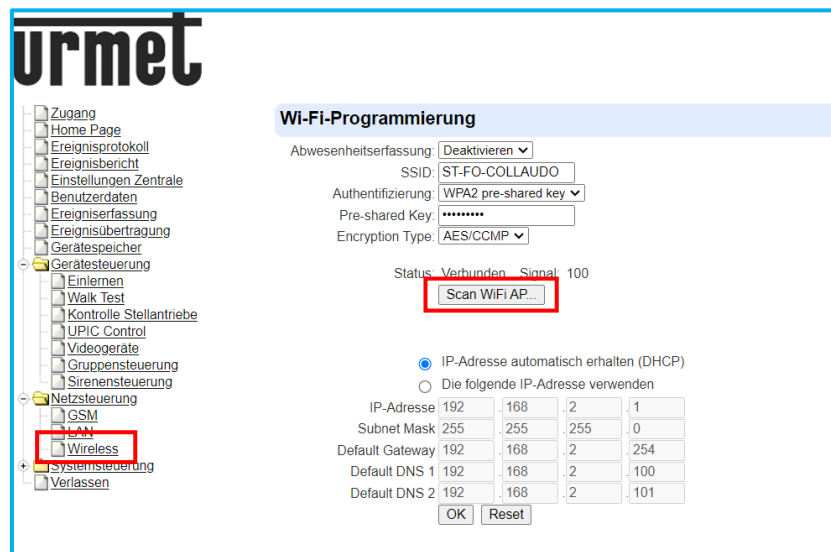
In diesem Menü ist es möglich, die Parameter der LAN-Verbindung zu konfigurieren.

- **DHCP:**

- ☞ **Ein.** Ist DHCP mit Ein eingegeben, erhält die Zentrale die IP-Adresse vom DHCP-Server des Netzwerks automatisch. Es sind daher keinerlei Einstellungen vorzunehmen.
- ☞ **Aus:** Ist DHCP mit Aus eingegeben, müssen die Informationen für IP-Adresse, Subnetzmaske, Gateway und DNS manuell eingegeben werden. Überprüfen Sie zuvor, ob Sie über alle notwendigen Daten für Ihre Netzwerkumgebung verfügen. Für weitere Informationen wenden Sie sich an den Betreiber des lokalen Netzwerks.

7.3 WLAN

In diesem Menü ist es möglich, die Parameter der WLAN-Verbindung zum Router zu konfigurieren.



- **Ausfallerfassung:** Wenn gewünscht wird, dass eine eventuelle Unterbrechung des WLAN in den Status und Ereignissen des Systems angegeben wird „Aktivieren“ auswählen.
- **SSID:** Name des ausgewählten Netzwerks.
- **Authentifizierung:** Für die Verbindung mit dem Router verwendete Authentifizierungsmethode.
- **Passwort:** Passwort des Routers.
- **Encryption:** Vom Router verwendete Verschlüsselungsart.

Die Taste „Scan WiFi AP“ betätigen, um das **WLAN**-Netzwerk zu suchen, mit dem die Verbindung erfolgen soll. Wählen Sie aus der Liste der verfügbaren **WLAN**-Netzwerke (Beispiel unten) das Netzwerk von Interesse durch Betätigen der Taste „Einstellen“ am Ende der Zeile aus. Durch Anklicken der Taste „X“ WiFi Aps wird die Tabelle der WLAN-Netzwerke gelöscht.

WiFi Aps						
SSID	MAC	Authentifizierung	Encryption	Signalniveau	Kanal	
ST-FO-COLLAUDO	08:55:31:53:8a:05	WPA2PSK	AES	100	9	Einstellen
UDOMUS_new	e8:ed:d6:dd:14:30	WPA2PSK	AES	100	6	Einstellen
UDOMUS_new	e8:ed:d6:dd:79:90	WPA2PSK	AES	44	1	Einstellen

Zum Bestätigen der eingegebenen Daten die Taste „OK“ betätigen. Nachdem die Seite des Browsers aktualisiert wurde, kann die erfolgte Verbindung in der Zeile **Status** überprüft werden.

Alternativ dazu ist es möglich, die Daten unter Verwendung der Adressierung mit statischer IP manuell einzugeben.

Sobald die Verbindung konfiguriert ist, zur Nutzung der drahtlosen Verbindung das Netzkabel von der Zentrale entfernen. Nach ca. einer Minute erneut anschließen und den Verbindungsstatus überprüfen.

Wird es dagegen vorgezogen, erneut die Verbindung über Kabel herzustellen, die Versorgung unterbrechen, das Netzkabel anschließen und die Versorgung wieder herstellen.

ACHTUNG: Stets nur einen Verbindungstyp verwenden, entweder mit Kabel oder mit WLAN.

8 SYSTEMSTEUERUNG

In den Untermenüs des Ordners **Systemsteuerung** ist es möglich, die Systemparameter zu konfigurieren.

8.1 PASSWORTÄNDERUNG

In diesem Menü können Benutzername und Passwort für den Zugriff auf die Steuertafel der Zentrale eingegeben werden.

- ☞ **Benutzername:** dies ist der beim Zugriff auf die lokale Steuertafel zu verwendende Benutzername. Der voreingestellte Name ist „**admin**“. Soll der Benutzername geändert werden, geben Sie einen neuen Namen in das Feld ein. Die maximale Zeichenanzahl beträgt 20.
- ☞ **Neues Passwort:** soll das Passwort geändert werden, geben Sie das neue Passwort in dieses Feld ein. Die maximale Zeichenanzahl beträgt 20.
- ☞ **Wiederh Passwort:** geben Sie das neue Passwort in dieses Feld ein.

8.2 HOME AUTOMATION

Siehe entsprechende Anleitung

8.3 SZENARIEN

Siehe entsprechende Anleitung

8.4 BERICHT

In diesem Menü kann eingegeben werden, wohin die Berichte versandt werden sollen. Es stehen bis zu 8 Adressen für die Übertragung der Informationen zur Verfügung.

urmet

Bericht

#	Berichtadresse	Filter	Gruppe 1	Gruppe 2	Gruppe 3	Gruppe 4	Gruppe 5
1	ip://127038320263@www.myzeno.urmet.com	Alle Ereignisse	☒	☐	☐	☐	☐
2		Alle Ereignisse	☐	☒	☐	☐	☐
3		Alle Ereignisse	☐	☐	☒	☐	☐
4		Alle Ereignisse	☐	☐	☐	☒	☐
5		Alle Ereignisse	☐	☐	☐	☐	☒
6		Alle Ereignisse	☒	☐	☐	☐	☐
7		Alle Ereignisse	☒	☐	☐	☐	☐
8		Alle Ereignisse	☒	☐	☐	☐	☐
9		Alle Ereignisse	☒	☐	☐	☐	☐
10		Alle Ereignisse	☒	☐	☐	☐	☐
11		Alle Ereignisse	☒	☐	☐	☐	☐
12		Alle Ereignisse	☒	☐	☐	☐	☐
13		Alle Ereignisse	☒	☐	☐	☐	☐
14		Alle Ereignisse	☒	☐	☐	☐	☐
15		Alle Ereignisse	☒	☐	☐	☐	☐
16		Alle Ereignisse	☒	☐	☐	☐	☐

- **Berichttyp:**

Die Zentrale Zeno unterstützt die folgenden Berichtstypen:

- ☞ **Report IP/GPRS im Format CID/SIA DC09:**

Zieladressenformat des Berichts: `ip://account@xxx.xxx.xxx.xxx:port/CID_SIA/SES`

Zum Beispiel: `ip://account@59.124.123.22:8765/CID_SIA/SES`

ip://	6543	59.124.123.23	:8765	/CID_SIA
Berichtstyp	Account	IP-Adresse des Servers	Port-Nummer	Berichtformat

- ☞ **IP/GPRS-Bericht im Format CID:**

Zieladressenformat des Berichts: `ip://Account@Server IP:Porta/CID`

Zum Beispiel: ip://6543@59.124.123.22:8765/CID

ip://	6543	@59.124.123.23	:8765	/CID
Berichttyp	Account (4-8 Ziffern)	IP-Adresse des Servers	Port-Nummer	Berichtformat

☞ IP/GPRS-Bericht im Format SIA:

Zieladressenformat des Berichts: ip://Account@Server IP:Porta/SIA

Zum Beispiel: ip://6543@59.124.123.22:8765/SIA

ip://	6543	@59.124.123.23	:8765	/SIA
Berichttyp	Account (4-8 Ziffern)	IP-Adresse des Servers	Port-Nummer	Berichtformat

☞ Sprachanrufbericht:

Zieladressenformat des Berichts: voice://Tel-Nummer.

Zum Beispiel: voice://00391234567890

voice://	0039	1234567890
Berichttyp	Internationale Vorwahl	Telefonnummer

<Hinweise>

- Die Adresse 1 wird bei der ersten Verbindung mit dem Server automatisch konfiguriert

ACHTUNG! Die Parameter der gesamten Zeile dürfen nie geändert werden! Im Fall von Wartungseingriffen oder der versehentlichen Änderung dieses Parameters, muss der Vorgang des Konfigurationsversands über das Portal MyZeno verwendet werden (siehe entsprechende Anleitung).

- Die Berichtart muss in Kleinbuchstaben eingegeben werden.
- Die Statuswechsel können nicht mittels Sprachanruf mitgeteilt werden.
- Der Versand der E-Mails kann nur auf dem Portal oder auf der APP eingegeben werden.

● Filter:

Durch Auswahl des Filters können Meldungen unterschiedlicher Ereignisse definiert werden:

- ☞ Alle Ereignisse: Die Zentrale meldet den Berichtempfängern die Alarmer, Fehler und Statuswechsel des Systems betreffenden Ereignisse.
- ☞ Alarmereignisse und Statuswechsel: Die Zentrale meldet den Berichtempfängern die die Alarmer und Statuswechsel betreffenden Ereignisse.
- ☞ Alarmereignisse ohne Statuswechsel: Die Zentrale meldet den Berichtempfängern nur die die Alarmer betreffenden Ereignisse.
- ☞ Statusereignisse: Die Zentrale meldet den Berichtempfängern nur die die Statuswechsel betreffenden Ereignisse. Von der Verwendung dieses Filters wird vor allem auf Adresse 1 abgeraten, da dies die Meldung der Alarmer an die Ferngeräte unterdrückt.

HINWEIS: Die Verwaltung der Berichte mittels Benachrichtigungen an ein Mobiltelefon kann unabhängig auf den APPs definiert werden.

● Gruppe:

Die Zieladressen der Berichte können verschiedenen Gruppen zugeordnet werden. Die Berichtgruppen unterliegen den folgenden Regeln:

- ☞ Die Priorität des Versands der Berichte wird von der der Gruppe zugeordneten Nummer definiert. Die Gruppe 1 hat im Verhältnis zu den nachfolgenden Nummern Priorität. Von Gruppe 1 → Gruppe 2 → Gruppe 3 →usw.
- ☞ Sind einer Gruppe mehrere Berichtzieladressen zugeordnet, unterbricht das System, wenn ein Bericht erfolgreich

an eine der Zieladressen gesandt wird, den Versand der Berichte an die restlichen Zieladressen der Gruppe und geht zum Bericht für die nachfolgende Gruppe über.

Gelingt es der Zentrale nicht, den Bericht an die erste Zieladresse einer Gruppe zu versenden, geht sie zur nächsten Zieladresse über. Gelingt es ihr nicht, den Bericht an eine der Zieladressen der Gruppe zu versenden, versucht die Zentrale noch zweimal bevor sie zur nächsten Gruppe übergeht.

Gelingt es ihr nicht, den Bericht an eine der Gruppen zu versenden, beginnt die Zentrale wieder mit dem Versand des Berichts von Gruppe 1 aus, bis mindestens eine Gruppe den Bericht erhält.

- ◆ Für die „**SPRACH**“-Berichte wählt die Zentrale, wenn der Anruf nicht zustande kommt, jede Telefonnummer dreimal erneut, bis zu maximal neun Versuchen insgesamt.

☞ Beispiel: Um sowohl die Benachrichtigungen an ein Mobiltelefon (ebenfalls bezüglich des Berichts von Zeile 1) als auch die telefonischen Sprachnachrichten im Alarmfall zu erhalten, zwei verschiedene Gruppe verwenden, eine für jeden Nachrichtentyp. Möchte man dagegen nur eine Art Nachricht erhalten, wird dieselbe Gruppennummer für Sprachanrufe und Benachrichtigungen verwendet. In diesem letzteren Fall geht der Sprachanruf nur ein, wenn die Benachrichtigung auf dem Mobiltelefon nicht erfolgreich war.

BEISPIELE

Beispiel	Konfiguration	Verhalten
A	1) IP-Benachrichtigung -> Gruppe 1 2) Rufversand -> Gruppe 1	Die Zentrale versendet nur eine Benachrichtigung an das Smartphone, wenn diese korrekt empfangen wird. Dagegen wird ein Sprachanruf versandt, wenn die Benachrichtigung nicht empfangen wird (z. B. wegen Ausfall des Datennetzwerks der Zentrale oder des Smartphones).
B	1) IP-Benachrichtigung -> Gruppe 1 2) Rufversand -> Gruppe 2	Von der Zentrale erfolgen stets sowohl Benachrichtigung als auch Sprachanruf.
C	1) IP-Benachrichtigung -> Gruppe 1 2) Rufversand -> Gruppe 2 3) Versand digitaler Bericht -> Gruppe 2	Von der Zentrale erfolgen stets sowohl Benachrichtigung als auch Telefonanruf. Ist der Telefonanruf nicht erfolgreich, wird auch eine Nachricht über digitales Protokoll versandt (z. B. an eine Überwachungszentrale).
D	1) IP-Benachrichtigung -> Gruppe 1 2) Versand digitaler Bericht -> Gruppe 2 3) Telefonanrufversand -> Gruppe 2	Von der Zentrale erfolgen stets sowohl Benachrichtigung als auch Versand des digitalen Berichts. Ist der Versand des digitalen Berichts nicht erfolgreich, erfolgt auch ein Telefonanruf.

<HINWEIS>

Die Zieladresse für den Versand der Berichte in Bezug auf die IP-Kameras muss in der lokalen Schnittstelle der jeweiligen Kamera programmiert werden (siehe entsprechende Anleitung).

- **Essentiell/Optional**

Essentiell: Die Zentrale versendet die Meldungen an alle als „**Essentiell**“ konfigurierten Gruppen. Die Zentrale versucht den Versand der Meldungen weiter, bis mindestens eine davon erfolgreich versandt wird. Die Gruppe 1 ist immer Essentiell.

Optional: Die Zentrale versendet die Meldungen an die als „**Optional**“ konfigurierten Gruppen nur dann, wenn die Meldungen der vorangegangenen Gruppe nicht erfolgreich waren. Zum Beispiel: Wenn Gruppe 3 Optional ist, versendet die Zentrale die Meldungen dieser Gruppe nur, wenn die der Gruppe 2 nicht erfolgreich waren.

- **1 Retry/ 3 Retry/ 5 Retry/ 10 Retry/ 99 Retry:**

Wenn die Meldungen einer Gruppe nicht erfolgreich sind, versucht die Zentrale die Übertragung mit der mit diesem Parameter festgelegten Häufigkeit.

8.5 SMS-BERICHT

In diesem Menü ist es möglich, die Verwendung der von der Zentrale versandten SMS einzustellen.

SMS-Bericht

	Berichtsadresse	Filter
1.		Alle Ereignisse
2.		Alle Ereignisse
3.		Alle Ereignisse
4.		Alle Ereignisse
5.		Alle Ereignisse

Hinweise: 1. SMS im Format CID, z. B.: sms://account@Telefonnr.
2. SMS im Textformat, z. B.: sms://Telefonnr./TEXT

OK Reset

© 2021 Urmet

☞ **SMS-Bericht im Textformat (nur wenn die Zentrale über SIM-Karte verfügt):**

Zieladressenformat des Berichts: sms://numero di cellulare/TEXT

Zum Beispiel: sms://00393476064587/TEXT

sms://	00393476064587	/TEXT
Berichtstyp	Handynummer	Berichtformat

<HINWEIS>

Wenn die SMS in diesem Menü definiert werden, werden sie immer versandt.

Sollte die Priorität der SMS-Nachrichten mit den Kriterien der im vorangegangenen Menü definierten Kriterien verwaltet werden sollen, die gleiche für dieses Menü definierte Zeichenfolge in die Zeilen der Berichte der Tabelle des vorangegangenen Menüs anstatt in dieses Menü einfügen.

8.6 UPLOAD VIDEO

Dieses Menü gestattet die Eingabe der Zieladresse des Versands von von den Meldern mit Foto- oder Videokamera aufgenommenen Bildern/Videos.

Server Upload Foto/Video

URL 1: xhttp://www.myzeno.urmet.com:8090/up-post.js

URL 2:

URL 3:

URL 4:

URL 5:

Prefix: 127038320263

☐ Die Ereignisse nach ihrem Versand löschen

Hinweise: 1. IP (Ethernet oder 4G) im FTP-Protokoll, z. B.: ftp://user:password@server/path
2. IP (Ethernet oder 4G) im HTTP-Protokoll, z. B.: http://server/path
3.
4.

OK Reset

- **Adresse 1:** bei der ersten Verbindung mit dem Server automatisch konfigurierte Adresse.

ACHTUNG! Dieser Parameter darf nie geändert werden!

Im Fall von Wartungseingriffen oder der versehentlichen Änderung dieses Parameters, geben Sie diesen wie folgt erneut ein:

Adresse 1: <http://www.myzeno.urmet.com:8080/up-post.php>

- **Adressen 2~5:** geben Sie FTP-Adressen ein.

☞ Format FTP: <ftp://user:password@IP address:port/folder>

- **Prefix:** ID für den Zugriff auf die Zentrale

<HINWEIS>

Die Zieladresse für den Versand von von den IP-Kameras aufgenommenen Bildern/Videos muss in der lokalen Schnittstelle der jeweiligen Kamera programmiert werden (siehe entsprechende Anleitung).

8.7 XMPP

In diesem Menü werden Daten angegeben, die nicht für den Benutzer, sondern für den Kundendienst bestimmt sind und zum Ausführen von Diagnosen auf der Anlage erforderlich sein können.

ACHTUNG! Diese Parameter dürfen nie geändert werden!

Im Fall von Wartungseingriffen oder der versehentlichen Änderung dieser Parameter, geben Sie diese wie folgt erneut ein:

- **XMPP:** www.myzeno.urmet.com
- **Port :** 522
- **Domäne:** elkron-home-portal
- **Buddy:** security_admin

8.8 DATUM UND UHRZEIT

Dieses Menü gestattet die Eingabe von Datum und Uhrzeit auf der Zentrale.

urmet

Datum und Uhrzeit

Data - 2024/03/19 20 (jjjj/mm/tt)

Uhrzeit 13 13 (hh:mm) Now

OK Reset

Zeitzone

Zeitzone (GMT+01:00) Brussels, Copenhagen, Madrid, Paris

OK Reset

Weltzeituhr

☐ Automatisch mit der Weltzeituhr auf dem NTP-Server synchronisieren

Server pool.ntp.org

OK Reset

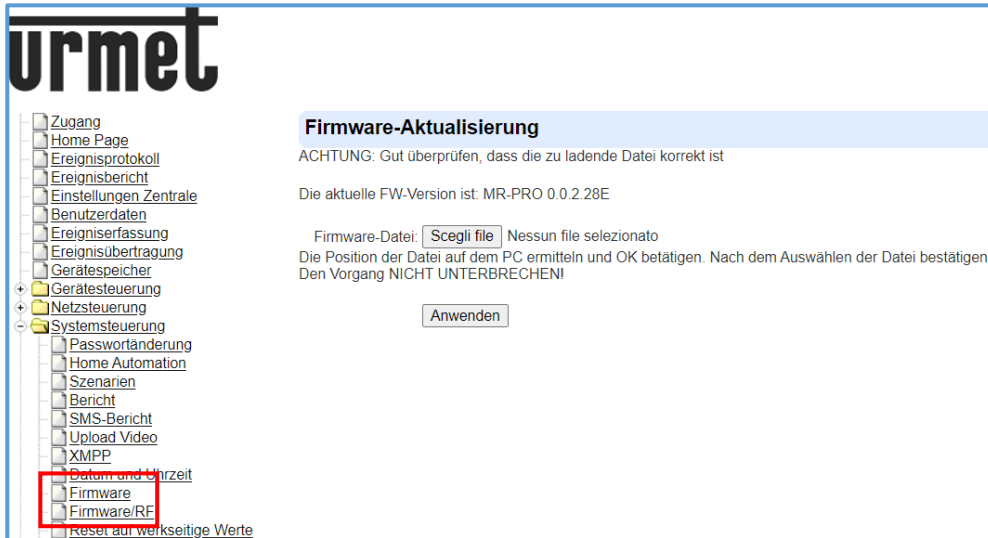
Navigation:

- Zugang
- Home Page
- Ereignisprotokoll
- Ereignisbericht
- Einstellungen Zentrale
- Benutzerdaten
- Ereigniserfassung
- Ereignisübertragung
- Gerätespeicher
- Gerätesteuerung
- Netzsteuerung
- Systemsteuerung
 - Passwortänderung
 - Home Automation
 - Szenarien
 - Bericht
 - SMS-Bericht
 - Upload Video
 - XMPP
 - Datum und Uhrzeit**
 - Firmware
 - Firmware/RF

- **Datum & Zeit:** Gestattet die Einstellung von Datum und Uhrzeit.
Nach dem Einstellen von Zeitzone und Datum und Uhrzeit muss zum Bestätigen der Änderungen die Taste „OK“ betätigt werden.
- **Zeitzone:** Gestattet die Einstellung der lokalen Zeitzone.
- **Weltzeituhr:** Wird die automatische Synchronisierung gewählt, wird die interne Uhr mit dem vom Internet über einen auswählbaren NTP-Server angebotenen Service synchronisiert. Es wird empfohlen, diesen Parameter nicht zu ändern.

8.9 FIRMWARE & FIRMWARE RF

In diesen Menü ist es möglich, die Firmware der Zentrale für die Verwaltung der Daten und der RF-Geräte zu aktualisieren.



Schritt 1. Wählen Sie die Firmware-Datei im Computer aus.

Schritt 2. Klicken Sie auf „Übernehmen“, um die Firmware-Datei in die Zentrale zu laden.

Schritt 3. Der Ladevorgang ist in nur wenigen Minuten abgeschlossen. Schalten Sie die Zentrale während des Vorgangs **NICHT** aus. Nach Abschluss der Aktualisierung sendet die Zentrale 2 Pfeiftöne aus und kehrt in ihren ursprünglichen Status zurück.

Schritt 4. Klicken Sie nach dem Abschluss des Vorgangs auf die Taste „Zugriff“ und überprüfen Sie das Vorhandensein der neuen FW-Version.

8.10 RESET AUF WERKSEITIGE EINSTELLUNGEN

Dieses Menü gestattet das Löschen aller Informationen und der in der Zentrale gespeicherten Einstellungen und wieder zu den werkseitigen Einstellungen zurückzukehren. Warten Sie den Neustart der Zentrale ca. 30 Sekunden ab.



Es ist möglich:

- die Netzwerkparameter nicht zu ändern, indem das Feld „**Netzwerkeinst erhalten**“ ausgewählt wird
- die Konfiguration der bereits eingelernten Geräte nicht zu verlieren, indem das Feld „**Geräteeeinstellungen erhalten**“ ausgewählt wird.

<Hinweis>

Für den Reset auf werkseitige Einstellungen ist es auch möglich, die Tastatur der Zentrale zu verwenden, die auch die Netzwerk- und Geräteeinstellungen löscht. Um den Reset auszuführen, wie folgt vorgehen:

- unterbrechen Sie die Netzversorgung und stellen Sie den Batterieschalter auf OFF;

- stellen Sie die Netzversorgung her und betätigen Sie innerhalb von 30 Sekunden nach dem Einschalten die Taste ▲. Das Display zeigt einen alphanumerischen Text mit Angabe der Firmwareversion an;
- betätigen Sie die folgende Tasten nacheinander: ▼▲▼▲▼▲▼ OK. Auf dem Display erscheint folgende Anzeige: *FACTORY RESET*;
- betätigen Sie erneut die Taste OK.

Nun kann die Taste losgelassen und der Batterieschalter erneut auf ON gestellt werden. Warten Sie den Neustart der Zentrale ca. 30 Sekunden ab.

ACHTUNG! Nachdem der Reset auf die Werkseinstellungen ausgeführt wurde, ist die Zentrale nicht mehr in der Lage, den Upload und die Berichte zu verwalten, da auch die Server-Adresse gelöscht wird. Die Wiederherstellung und erneute Aktivierung dieser Funktionen ist unerlässlich. Hierzu wird der Vorgang des Versands der Konfiguration über das Portal verwendet (siehe entsprechenden speziellen Leitfaden).

8.11 BACKUP & RÜCKSTELLEN

Dieses Menü gestattet den Speichervorgang und die Wiederherstellung der Konfigurationsdaten der Zentrale. Dieser Vorgang muss nach Besprechung mit dem Kundendienst erfolgen.

8.12 SYSTEMPROTOKOLL

In diesem Menü werden Daten angegeben, die nicht für den Benutzer, sondern für den Kundendienst bestimmt sind und zum Ausführen von Diagnosen auf der Anlage erforderlich sein können.

9 TECHNISCHE EIGENSCHAFTEN DER ZENTRALE

Wichtigste Leistungsmerkmale

- Bidirektionale Kommunikationen mit Funkfrequenz mit allen Geräten.
- Funkfrequenzanbindung von bis zu 80 Geräten.
- Anschluss von bis zu 6 IR-Meldern mit Kamera oder Videokamera für die Videoüberprüfung der Alarme.
- Anschluss von bis zu 4 IP-Kameras.
- Verwaltung von 3 Teilaktivierungsbereichen und Vollaktivierung.
- Maximal 20 konfigurierbare Benutzer (Codes und Fernbedienungen).
- Maximal 20 Aktivierungs-/Deaktivierungs-/Teilaktivierungs-codes konfigurierbar.
- Speicherkapazität von bis zu 200 Ereignissen
- Aufzeichnung von 4 oder 6 Fotos und 10 Sekunden Video bei jedem Alarm 30 Sekunden Videoaufzeichnung im Fall der IP-Kamera, mit der Möglichkeit, auch die Videoaufzeichnung vor dem Alarmereignis zu erhalten.
- Aktivierungen/Deaktivierungen über Funksteuerungen, Tastaturen, PC, Smartphone, für die Aktivierungen/Deaktivierungen und Szenarien/Regeln der Home Automation konfigurierte Kontakte.
- Verbindung zum Router mittels Ethernet- oder WLAN-Kabel (alternativ).
- Alarm-/Bild-/Videoversand auf HTTP/FTP-Server, per E-Mail, Telefonanruf und SMS (nur wenn die Zentrale mit SIM-Karte ausgestattet ist), Push-Nachrichten, CID- und SIA-Protokolle.
- Umgebungsabhörung über IP-Kamera.
- Alarmübertragung mittels:
 - CID/ SIA over TCP/IP (DC09), über Ethernet oder 4G (nur wenn die Zentrale mit SIM-Karte ausgestattet ist)
 - SMS auf GSM (nur wenn die Zentrale mit SIM-Karte ausgestattet ist),
 - Videos und Bilder über E-Mail/ FTP over Ethernet oder 4G (nur wenn die Zentrale mit SIM ausgestattet ist)
- Fernsteuerung über WEB-Portal oder APP (iOS und Android).
- Messung Wireless- und 4G-Signale.
- Überwachung aller Geräte mit Ausnahme der Fernbedienung und der Tastatur
- Erfassung von Störungen der Funkfrequenz (Anti-Jamming)
- Eingebaute Sirene
- Konform mit den Zertifizierungen EN 50131 Grad 2, Klasse II

Technische Daten:

- GSM Quadband 900/1800/850/1900 MHz
- Wireless-Verbindungen über:
 - 4G
 - ZigBee HA 1.2
 - 868 MHz Narrowband
 - WiFi 2,4 GHz
- Ethernet-Verbindung 10/100 Mbit
- Interne Versorgung über 9V 1A
- Max. Verbrauch: 30 mA bei 230 VAC
- Wiederaufladbare interne Backup-Batterie: 4,8 V Ni-Mh, 1100 mAh
- Dauer der Backup-Batterie: durchschnittl. 15 Stunden
- Funkfrequenzband: 868,600-868.700 MHz
- Max. Sendeleistung: +15 dBm
- Schallpegel der internen Sirene: 95 dB bei 1 m
- Betriebstemperatur: von -10 °C bis +45 °C
- Abmessungen: 260 x 176 x 30 mm
- Gewicht: 600 g

10 FERNSTEUERUNGSGERÄTE

Das System Urmet Zeno kann über Smartphone und PC ferngesteuert werden. Urmet stellt eine dedizierte App und ein Multi-Browser-Web-Portal zur Verfügung, auf die der Benutzer mit den gewählten vertraulichen Anmeldedaten zugreifen kann.

Das **Portal** ist über die folgende Adresse erreichbar: <https://www.myzeno.urmet.com/home>. Der erste Vorgang besteht darin, sich als *Neuen Benutzer* zu registrieren (ein Vorgang mit Anleitung gibt die auszuführenden Schritte an). Sobald die Registrierung erfolgt ist, ist über das Portal Folgendes möglich:

- Aktivierung/Teilaktivierung/Deaktivierung der Anlage
- Anzeigen des Status der im System vorhandenen Geräte
- Anzeigen der letzten 200 Ereignisse
- Konfiguration neuer Benutzer und neuer Codes, Anzeigen der bereits als Master vorhandenen
- Anzeigen der Basisinformationen des Systems
- Konfiguration einiger Geräteparameter (darunter der ständige Bypass einiger Melder)
- Ändern des Hauptpassworts
- Konfiguration der E-Mails und Push-Nachrichten, an die die Berichte versandt werden sollen
- Anzeigen der von der IP-Kamera 1051/004 aufgenommenen Bilder in Echtzeit.

Die Bedienungsanleitung des Portals ist auf der Website von Urmet im Bereich *Produkte-Einbruchsicherung* verfügbar. Für den Zugriff auf die Website verwenden Sie den Link auf der nächsten Seite.

Die Benutzer-APP „**MyZeno**“ kann auf dem jeweiligen Smartphone installiert werden, indem man sich zu **App Store** (für iPhone) oder **Google Play** (für Android) begibt. Die Applikation gestattet Folgendes:

- Aktivierung/Teilaktivierung/Deaktivierung der Anlage
- Anzeigen des Status der im System vorhandenen Geräte
- Anzeigen der letzten 200 Ereignisse
- Anzeigen der Basisinformationen des Systems
- Ändern des Hauptpassworts
- Konfiguration der E-Mails und Push-Nachrichten, an die die Berichte versandt werden sollen
- Konfiguration von Benachrichtigungen für die APPs und E-Mails
- Ausführen der Anmeldung der Zentrale und des damit verbundenen Benutzers
- Generieren eines Codes für den Technikerzugriff
- Anzeigen der von den IP-Kameras aufgenommenen Bilder in Echtzeit

<WICHTIGE HINWEISE>

- Der Benutzer muss eine Internetverbindung über ein ADSL-Modem oder eine SIM-Karte vorsehen, die mit den Systemgeräten kompatibel sind und einen Vertrag über einen Internetzugang unterzeichnet haben.
- Der Zugriff auf Portal und App und dem Empfang von Benachrichtigungen und E-Mails sehen vor, dass die Zentrale Zeno ununterbrochen mit dem Internet verbunden ist.
- Die Installation und die Konfiguration der Telekommunikationsgeräte, die den Internetzugang gestatten, erfolgen unter der alleinigen Verantwortung von Urmet.

- Das Unternehmen warnt den Benutzer vor der potentiellen Gefahr von Unterbrechungen der Internetverbindung, die den Zugang und die Funktionsweise des Portals und der App und den Empfang von Benachrichtigungen und E-Mails teilweise oder vollständig beeinträchtigen könnten.
- Das Unternehmen haftet nicht im Fall von Funktionsstörungen oder der Unmöglichkeit des Zugriffs auf das Portal und die App und den Empfang von Benachrichtigungen und E-Mails aufgrund der Unterbrechung der Internetverbindung des Benutzers.
- Sowohl über App als auch über das Portal ist jeweils nur die Verbindung einer Sitzung zulässig. Eine Verbindung schließt die andere aus.
- Während der Installationsschritte oder anschließender Wartungsvorgänge über die lokale Steuertafel wird von der gleichzeitigen Verwendung von App und Portal für eventuelle Systemtests oder für die Interaktion mit dem System abgeraten. Trennen Sie nach Abschluss der Installations- und Wartungsvorgänge den lokalen PC von der Verbindung.
- Überprüfen Sie, sollten die E-Mails nicht empfangen werden, die Ordner für Spam und unerwünschte Post.
- Sowohl das Portal als auch die App begrenzen aus Sicherheitsgründen die Dauer einer Sitzung auf eine zeitliche Höchstgrenze.
- Es wird empfohlen, für Portal und App Passwörter mit mindestens 8 Zeichen zu wählen.
- Eine Sabotage (Tamper) bei aktivem System wird in der Historie von App und Portal sowohl als Sabotage (Tamper) als auch als Einbruchalarm aufgezeichnet.

11 ANHÄNGE

11.1 TYPOLOGIEN DER IM SYSTEM GENERIERTEN ALARME UND EREIGNISSE

EINBRUCHALARM	
Wird ausgelöst, wenn	Ein Einbruchsversuch erfolgt
Die Zentrale aktiviert	- Die im System vorhandenen Abschreckvorrichtungen, d. h., die Außensirenen und/oder die Innensirene der Zentrale, außer im Fall von stillen Alarmen, für die nur die Benachrichtigungen aktiviert werden - Das Pop-up-Fenster „Neues Ereignis“ auf dem Portal - Wenn aktiviert, den Versand der E-Mail mit der entsprechenden Einbruchalarmmeldung - Wenn aktiviert, den Versand von SMS mit der entsprechenden Einbruchalarmmeldung über das GSM/4G-Modul (nur wenn die Zentrale über eine SIM-Karte verfügt) - Wenn aktiviert, die Benachrichtigung mit entsprechender Einbruchalarmmeldung auf der dedizierten APP - Wenn aktiviert, den Versand von Alarmen an die Überwachungszentren (CID, SIA usw.)
Der Alarm wird gemeldet	- Auf der Zentrale mit der Anzeige „Alarm!“ auf dem Display - Auf den Tastaturen (Einzelheiten siehe jeweilige Bedienungsanleitungen)
Der Alarm wird gespeichert	- in der Zentrale, im Menü Historie - in der Benutzer-APP und im Portal, im Menü Ereignisse
Der Alarm dauert	Für die programmierte Dauer des Einbruchsalarms
Der Alarm wird unterbrochen durch	- Eingabe eines gültigen Codes über die Tastatur und den anschließenden Deaktivierungsbefehl - Eingabe eines gültigen Codes auf Portal oder APP und den anschließenden Deaktivierungsbefehl - Einen Deaktivierungsbefehl der Funksteuerung - Einen Statuswechsel über den als Aktivieren/Deaktivieren programmierten Magnetkontakt

Wird ausgelöst, wenn	Ein Tamper bei dem Versuch eines unerlaubten Eingriffs auf einem Gerät des Systems geöffnet wird (Zentrale, Tastaturen oder Geräte wie DC, IR, Sirenen). Die Erfassung hängt von der Tamper-Programmierung im Menü „Einstellungen Zentrale“ ab
Aktiviert	- Die im System vorhandenen Abschreckvorrichtungen (Außensirenen und/oder Sirene im Inneren der Zentrale) - Das Pop-up-Fenster „Neues Ereignis“ auf dem Portal - Wenn aktiviert, den Versand der E-Mail mit der entsprechenden Tamperalarmmeldung - Wenn aktiviert, den Versand der SMS mit der entsprechenden Tamperalarmmeldung - Die Benachrichtigung auf der dedizierten APP mit der entsprechenden Tamperalarmmeldung - Wenn aktiviert, den Versand von Alarmen an die Überwachungszentren (CID, SIA usw.)
Der Alarm wird gemeldet	Auf der Zentrale mit der Anzeige „Alarm!“ auf dem Display
Der Alarm wird gespeichert	- Im Portal, im Menü Ereignisse - In der Benutzer-APP, im Menü Ereignisse - In der Zentrale, im Menü Historie, mit dem Hinweis auf das Problem mit der eingeschalteten gelben Led
Der Alarm dauert	Für die programmierte Dauer des Alarms
Wird gestoppt durch	- Eingabe eines gültigen Codes über die Tastatur und den anschließenden Deaktivierungsbefehl - Betätigen des Deaktivierungsbefehls auf dem Portal oder der APP und durch Eingabe eines gültigen Codes - Den Deaktivierungsbefehl über Funksteuerung - Einen Statuswechsel über den als Aktivieren/Deaktivieren programmierten Magnetkontakt

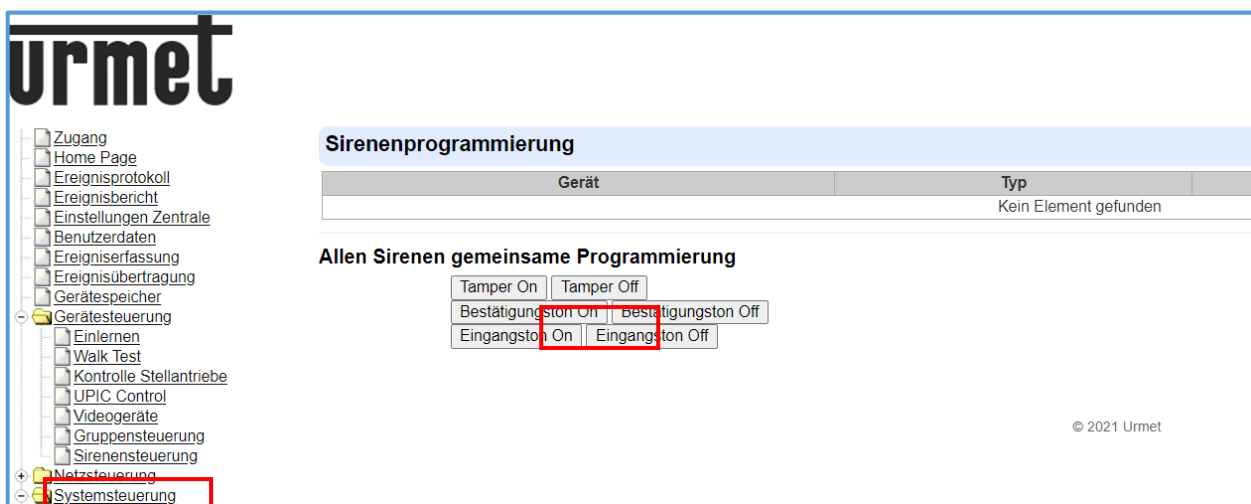
11.2 ANWEISUNGEN ZUM ERSETZEN UND ENTSORGEN DER BATTERIEN

Allgemeine Vorgehensweise

1. Vor dem Ersetzen der Batterien jeglicher Komponenten des Systems **Zeno** sicherstellen, dass die Zentrale sich im deaktivierten Zustand befindet.
2. Verbinden Sie sich mit der *Lokalen Steuertafel* der Zentrale oder mit der *Techniker-App*, um die bestehende Konfiguration zu überprüfen und diese eventuell zu ändern, wie unter Punkt 3 für die Geräte und die Sirene beschrieben.
3. Für die Zusatzgeräte: Im Inneren des Menüs „**Einstellungen Zentrale**“ die Auswahl **Tamperalarm** → **Fern Akt** treffen. Auf diese Weise generiert das Öffnen der Geräte zum Wechseln der Batterien keinen Einbruchalarm.



Für die Sirene: Im *Geräte/Sirenenprogrammierung* den Sabotageschutz der Sirene deaktivieren, indem **Aus** auf „**Sirenen-Tamper**“ ausgewählt und auf die Taste geklickt wird, um die Auswahl zu bestätigen (die Sirene wird nach einer Stunde wieder aktiviert, auch wenn der Tamper in dieser Ansicht nicht wieder aktiviert wird).



4. Befolgen Sie die im Anschluss beschriebenen Vorgehensweisen für den Batteriewechsel für jedes einzelne Gerät und die Sirene.
5. Nachdem der Vorgang des Batteriewechsels ausgeführt wurde, in der Ereignisliste das Schließen des Tampers überprüfen

Eventuelle Aktualisierungen der Dokumentation und weiterer Ressourcen und Vertiefungen sind auf der Website www.urmet.com im Bereich Produkte → Einbruchssicherung oder unter dem folgenden Link zu verfügbar:



In diesem Bereich können Sie auch Folgendes finden:

- Die Anleitung für Bedienung und Programmierung der Zentrale über Tastatur
- Die Bedienungsanleitung des Portals und der APP **MyZeno**
- Die Anweisungen für die Installation von Wireless-Anlagen
- Den technischen Leitfaden zum Ersetzen und Entsorgen der Batterien der Geräte des Systems Zeno.

VEREINFACHTE EU-KONFORMITÄTSERKLÄRUNG

Der Hersteller, URMET S.p.A., erklärt, dass der Funkgerätetyp:
DRAHTLOSE ZENTRALE MIT IP-, WLAN- UND 4G-NETZWERK Artikelnummer 1051/020 mit der Richtlinie 2014/53/EU konform ist.

Der ungekürzte Text der EU-Konformitätserklärung steht auf der folgenden Website zur Verfügung:
www.urmet.com

RICHTLINIE 2012/19/EU DES EUROPÄISCHEN PARLAMENTS UND DES RATS vom 4. Juli 2012 über Elektro- und Elektronik-Altgeräte (WEEE).



Das auf dem Gerät oder seiner Verpackung angebrachte Symbol des durchgestrichenen Abfallcontainers weist darauf hin, dass das Produkt am Ende seiner Lebensdauer getrennt von anderem Abfall gesammelt werden muss. Es liegt daher in der Verantwortung des Benutzers, das Gerät am Ende seiner Lebensdauer einer geeigneten Sammelstelle für das Recycling für Elektro- und Elektronik-Altgeräte zuzuführen. Alternativ zur eigenständigen Entsorgung kann das zu entsorgende Gerät im Moment des Kaufs eines Neugerät gleichwertigen Typs beim Händler abgegeben werden.

Bei Händlern von Elektronikprodukten mit einer Verkaufsfläche von mindestens 400 m² ist außerdem die kostenlose Abgabe ohne Kaufverpflichtung von zu entsorgenden Elektronikprodukten mit einer Größe von maximal 25 cm möglich. Die korrekte Abfalltrennung für die anschließende Zuführung in Recycling, Aufbereitung und umweltfreundliche Entsorgung trägt dazu bei, eventuelle negative Auswirkungen auf Umwelt und Gesundheit zu vermeiden und fördert die Wiederverwendung und/oder das Recycling der Werkstoffe, aus denen das Gerät besteht.