



EkoSecure Hub

DIN VDE V 0825-1 compliant

Product Part Number: EKSHUB

# Administrator Guide

Document Part Number: 9262-0119

Issue Number: 1

Release: 23/02/2022

# Contents

<b>0</b>	<b>Preface</b>	<b>7</b>
0.1	About this document	7
0.2	Intended readers	7
0.3	Warranty	7
0.4	Compliance	7
0.5	Company liability	8
0.6	Data protection	8
0.7	Safety	8
	0.7.1 Installation notes	9
	0.7.2 Connection of power supplies	9
	0.7.3 Servicing	9
0.8	Limitations	10
0.9	Feedback	10
0.10	Version control	10
<b>1</b>	<b>Introduction</b>	<b>11</b>
<b>2</b>	<b>Front panel</b>	<b>11</b>
2.1	Overview	11
2.2	Indicators	12
	2.2.1 LCD Display screen	12
	2.2.2 Timing synchronisation with Timing Master	12
	2.2.3 Radio beacon transmission active	13
	2.2.4 Configuration installed	13
	2.2.5 EkoTek logo	13
2.3	Removing the lower front panel	13
	2.3.1 IP Address Reset button	14
<b>3</b>	<b>Powering the device</b>	<b>15</b>
3.1	Powering up the device	16
3.2	Powering down the device	16
	3.2.1 Changing the on-board batteries	17
3.3	Failure of the external power supply	18
	3.3.1 Total power failure	18
<b>4</b>	<b>Software interface</b>	<b>18</b>

4.1	Connecting a viewing device to the Hub	19
4.2	Accessing the web interface	19
4.2.1	Logging in to the web portal	20
4.2.2	Logging out of the web portal	20
<b>5</b>	<b>Konfiguration menu</b>	<b>21</b>
5.1	System settings	21
5.1.1	System Clock	22
5.1.2	Hub IP settings	23
5.1.3	Connecting to external systems	24
5.1.4	Remote logging	25
5.1.5	LAN 227	
5.2	Funk	28
5.2.1	Netzkennung	28
5.2.2	Synchronisation PTP domain	29
5.2.3	Frequenzsprung	29
5.2.4	Autoregistrierung Gerät	31
5.2.5	Autoregistrierung Name	31
5.3	Geräte	32
5.3.1	Manually adding a new device	33
5.3.2	Editing an existing device	35
5.3.3	Removing a device	35
5.4	Geräteprofil	35
5.4.1	Abstellruf settings [Fob devices]	37
5.4.2	Akustischer Alarm (drop-down list)	37
5.4.3	Alarm löschen settings [Pager devices]	37
5.4.4	Alarm Wiederholung – Intervall (text field)	38
5.4.5	Alarmbetrieb settings [Call Point devices]	38
5.4.6	Alarmbetrieb settings [Fob devices]	40
5.4.7	Anwesenheit settings	41
5.4.8	Assistenzalarm settings	42
5.4.9	Auf Netzwerk fixieren	42
5.4.10	Bereichsalarm settings	43
5.4.11	Bewohnerruf settings	44
5.4.12	Downstream-Kanal (drop-down list)	45
5.4.13	Freigabe zur Alarmlöschung (checkbox)	46
5.4.14	Funk (checkbox)	47
5.4.15	Kanal (drop-down list)	47
5.4.16	Kontakteingabe settings	48
5.4.17	Lagealarm settings	49
5.4.18	Lokalisierungsbereich (drop-down list)	50
5.4.19	Manueller alarm settings	51
5.4.20	Notruf settings [EkoCare Units]	52
5.4.21	Nur Long-Range / Konvertor (radio buttons)	53
5.4.22	Reißleine settings	54

5.4.23	Relais-Betrieb settings	55
5.4.24	Schwesternruf settings [EkoCare Units]	56
5.4.25	Schwesternrufbetrieb settings [Call Point and Fob devices]	57
5.4.26	Upstream-Kanal (drop-down list)	58
5.4.27	Zeitalarm settings	60
5.5	Pagergruppen	60
5.5.1	Managing Pager Groups	61
5.6	Alarmregeln	63
5.6.1	Adding a new Alert Rule	65
5.6.2	Editing an existing Alert Rule	66
5.7	EkoCare Regeln	67
5.8	Zurücksetzen	67
5.9	Alles Löschen	68
5.10	Passwörter	69
5.10.1	Editing the account passwords	70
5.10.2	Access based on user account	70
5.11	Datensicherung	71
5.11.1	Creating an archive	71
5.11.2	Restoring an archive into the system	72
5.12	Aktualisierung	72
5.13	Herunterfahren	74
5.14	Nachrichtenformat	75

## 6 Hauptmenu 76

6.1	Tag / Nacht – Setting the current Shift	76
6.1.1	Manuelle Auswahl	76
6.1.2	Automaticsh	77
6.1.3	Extern	77
6.2	Ereignisprotokoll	78
6.2.1	The Event Log table	79
6.2.2	Adding records	80
6.2.3	Exporting the Event Log data	80
6.3	Nachricht senden	80
6.4	Nachrichtenprotokoll	81
6.4.1	The Nachrichtenprotokoll table	82

## 7 Systeminfo menu 83

7.1	Gerätestatus	83
7.1.1	Device Details page	84
7.2	Netzwerk-Baum	86
7.2.1	Searching the Network Tree	87
7.3	Verkehr	88
7.4	Rangfolge der Nachrichten	89

<b>8</b>	<b>Operating the hardware interface</b>	<b>90</b>
8.1	Default display	90
8.2	Raising and clearing alarms	91
8.2.1	Raising an alarm from the Hub	91
8.2.2	Clearing an alarm raised by the Hub	92
8.2.3	Alarm escalation	92
8.3	Receiving messages	92
8.3.1	Responding to a message	92
8.3.2	Messages listed on the default display	93
8.3.3	Receivable message types	93
8.4	Zeitalarm prompts	94
8.5	Hub operation menu	94
8.5.1	Hauptfunktionen	94
8.5.2	Zusatzfunktion	96
<b>9</b>	<b>Upgrading the Hub software</b>	<b>98</b>
<b>10</b>	<b>Servicing</b>	<b>99</b>
<b>11</b>	<b>Additional support</b>	<b>99</b>
	<b>Appendices</b>	<b>100</b>
A	EkoSecure principles	100
A.1	The radio network mesh	100
A.2	Beacons	101
A.2.1	Main Beacon	101
A.2.2	Location Beacon	103
A.3	Devices	104
A.3.1	The Hub	104
A.3.2	Static devices	105
A.3.3	Portable devices	106
A.3.4	External devices and systems	106
A.4	Device Modes overview	107
A.5	Network Zones overview	108
A.6	Alarms	108
A.6.1	Alarm types	108
A.6.2	Alarm escalation	109
A.6.3	Information included in alarm messages	109
A.6.4	Alert Rules overview	110
A.7	Maintenance Messages	110
B	Compliance with DIN VDE V 0825-1	111
B.1	Response times	111
B.2	Pager identification in alarms	112

B.3	Monitoring and technical alarms	112
B.4	Pager operation	112
B.5	Alarm type test on Pager activation	113
B.6	Notification of personal alarms by the Hub	113
B.7	Manual clearance of audible and visible alerts	114
B.8	Internal and external logging of alarms	114
B.9	Independent power supplies	115
B.10	Fail-over power capability	115
B.11	Indication of external power failure	115
B.12	Product labelling	116
B.13	Enclosed user information	116
B.14	Electrical safety	117
C	Remote logging output	117

<b>Index</b>	<b>119</b>
--------------	------------

---

## 0 Preface

### 0.1 About this document

This document covers the full operational function and device management of the EkoSecure DIN VDE V 0825-1 compliant Hub as part of a complete EkoSecure system once installed and commissioned for use. Guidance on editing the system configuration is also included.

The Hub contains a range of settings and features intended for use when EkoSecure is integrated with a wider EkoTek system, which are covered in this document. Where EkoSecure is installed as a self-contained system, these features do not apply.

For user guidance limited to basic operation of the hardware interface at Operator level for daily team use, see the dedicated Operator Guides, document numbers 9262-0116 (German) and 9262-0117 (English).

For documentation concerning the installation of the devices, see the dedicated system Installation & Setup Guide, document number 9261-9708.

For information on the role of other Devices within an EkoSecure system, see the dedicated EkoSecure system documentation, available from Multitone upon request.

### 0.2 Intended readers

This document is intended for use by users with administrative and management responsibilities relating to the EkoSecure system and access to the browser interface of the EkoSecure Hub. Some technical knowledge and familiarity of the system is required.

### 0.3 Warranty

This Multitone system is supplied with a 12-month warranty beginning upon receipt of the solution. Please see Multitone's standard terms and conditions of purchase.

### 0.4 Compliance

#### EU Territories

This product complies with the requirements of the following EU Directives:

**Radio Equipment Directive (RED) 2014/53/EU**  
**RoHS-2 Directive 2011/65/EU (Decision 768/2008/EC**  
**Annex II, Module A)**



Product accreditation is also inclusive of certification by the German DGUV authority to the following standards:

**Surveillance systems - Radio staff protection systems  
for Lone Workers, DIN VDE V 0825-1;  
Use of personal emergency signal systems,  
DGUV Regel 112-139**



A complete copy of the associated Declaration of Conformity for this and other Multitone products may be obtained upon request from [info@multitone.de](mailto:info@multitone.de) or [supportdesk@multitone.com](mailto:supportdesk@multitone.com). Alternatively, please contact your Multitone representative.

This equipment contains low power radio devices and has been tested for compliance with the recognised operational performance and personnel safety working limits specified for such equipment. Should any problems arise in relation to interference affecting signals both to and from the equipment, the apparatus may require repositioning or the fitting of additional filtering components, such as ferrite absorbers or in-line filters. Should such action be deemed necessary, contact either Multitone or their authorised agents.

#### **PRODUCT DISPOSAL WEEE DIRECTIVE & 2012/19/EU**

At the end of its serviceable life, this product should not be treated as household or general waste. It should be handed over to the applicable collection point for the recycling of electrical and electronic equipment, or returned to Multitone or their agent, for disposal.



## 0.5 Company liability

This document has been compiled for guidance only and the content checked for technical accuracy. The user should ensure that the correct issue of the document is used, as Multitone Electronics plc will not accept any liability for inaccuracies or errors resulting from its use.

In line with Multitone's policy of continued technical advancement, technical specifications are subject to change without notice. The products and services offered may be subject to availability and differ from those described, or illustrated, in this document.

## 0.6 Data protection

As the equipment user or controller, you may collect and manage personnel data. In this instance, you must be in compliance with any local privacy protection laws and regulations that protect the rights and interests of other people, by implementing measures which include but are not limited to: handling such data securely and only for a period of time that is reasonably required for its intended use.

## 0.7 Safety

The following information applies to both operating and servicing personnel. General Warnings and Cautions will be found throughout the manual where they apply.



**WARNING statements identify conditions or practices that could result in personal injury.**

**CAUTION statements identify conditions or practices that could result in physical damage to the product or loss of data.**

All the safety and operating instructions should be read before the equipment is connected and operated and retained for future reference. All warnings marked on the equipment should be strictly adhered to. No attempt should be made to remove any designated safety covers, as these areas contain voltages of a sufficient magnitude to constitute a risk of electric shock to personnel.

This package contains small parts that may be hazardous if mismanaged.

To attract attention, this equipment emits loud alert tones. Repeated exposure to such sounds at close range can result in permanent hearing loss or damage. Users should avoid putting their ears against the sounder opening on the front panel.

### 0.7.1 INSTALLATION NOTES

The installation and servicing of this product must only be carried out by suitably qualified personnel.

This equipment is rated for use in the temperature range 0 - +40 °C and is ingress-rated to IP20. The equipment should be positioned away from sources of heat and so that there is no interference to the flow of air around the front and sides of the unit.

This equipment has been designed to conform to the relevant Safety and EMC performance standards, but it may be necessary to take additional precautions during installation, to ensure continued compliance.

### 0.7.2 CONNECTION OF POWER SUPPLIES

This equipment is intended to be primarily powered by an external Power-over-Ethernet (PoE) injector power supply. This should be connected to a nearby 100-240 V AC, 50 Hz power source using the power cable supplied; see section 3.

This equipment also contains a re-chargeable backup battery installation. Any replacement of these batteries should only be undertaken by designated service personnel.

### 0.7.3 SERVICING

This equipment should only be serviced at a Multitone approved service facility.

Other than the batteries, none of the components of this equipment can be replaced or repaired by users. Only authorised dealers or service centres may dismantle the product.

If any parts of your product require replacement for any reason, including normal wear and tear or breakage, contact your dealer.

## 0.8 Limitations

In accordance with the requirements stipulated by DIN VDE V 0825-1, some features and settings relating to this model of the EkoSecure Hub are pre-configured or disabled by default and cannot be changed. Information relating to these requirements is included in Appendix B.

## 0.9 Feedback

Multitone welcomes feedback relating to this document and the product(s) described. Please direct any comments to [supportdesk@multitone.com](mailto:supportdesk@multitone.com) or to Multitone's Head Office:

**Germany:**

Multitone Elektronik  
International GmbH  
Roßstraße 11  
D-40476 Düsseldorf  
Deutschland

**GB:**

Multitone Electronics plc  
Multitone House  
Shortwood Copse Lane  
Kempshott  
Basingstoke  
Hampshire  
RG23 7NL  
United Kingdom

## 0.10 Version control

Version 1      23/02/2022      First release

# 1 Introduction

The EkoSecure Hub is a high-capacity control centre for EkoSecure systems through which the network and connected devices can be managed, providing a radio network interface to EkoSecure repeaters and a pair of LAN interfaces to TCP/IP-based equipment. The device is powered by either PoE or 12 V DC, with failover to rechargeable batteries capable of covering power outages of 30 minutes or more.

## 2 Front panel

### 2.1 Overview

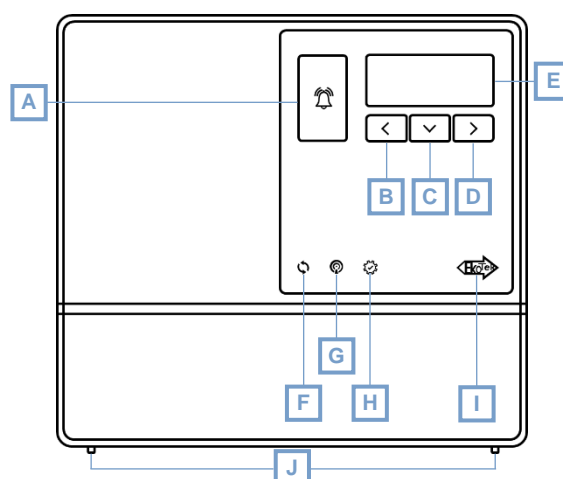


Fig. 1 The EkoSecure Hub interface

The following controls are available on the front panel interface:

- |                                 |                                |
|---------------------------------|--------------------------------|
| <b>A</b> Emergency Alarm button | <b>C</b> Scroll button         |
| <b>B</b> Back button            | <b>D</b> Select / Enter button |

The following indicators are located on the front panel interface:

- |  |   |
|--|---|
| <b>E</b> LCD display screen                        | <b>H</b> Configuration installed                          |
| <b>F</b> Timing synchronisation with Timing Master | <b>I</b> Active power supply via PoE or 12 V DC connected |
| <b>G</b> Radio beacon transmission active          |   |

Use the Cover Release Clips **J** to open the front panel of the Hub; see section 2.3.

## 2.2 Indicators

The indicators on the front panel of the device convey the following information.

### 2.2.1 LCD DISPLAY SCREEN








Fig. 2 The LCD display default screen

The LCD display shows all messages received by the Hub and any available response options. The number of message previews shown simultaneously on the display is limited to 4.

The LCD will not illuminate until an active external power supply is connected and the on-board batteries have charged to a level sufficient to complete a controlled power-down procedure when the external supply is disabled.

#### Status icons

The following icons are displayed in the top-right corner of the Hub LCD display:

-  Connected to an active external power supply
-  Powered by the on-board battery
  - An approximate indication of the current level of charge is indicated through the icon
-  An audible alert will be triggered when alarms and messages are received
-  The system configuration is currently using the **Tag** Shift settings
-  The system configuration is currently using the **Nacht** Shift settings


#### Device Operation Status indicator

The separator between the hours and minutes value of the display clock indicates correct functionality of the Hub:

- **00 : 00** – The Hub is functioning correctly
- **00 ! 00** – The Hub processor has encountered a problem and the system is inoperable
  - Contact your Multitone Agent for assistance

### 2.2.2 TIMING SYNCHRONISATION WITH TIMING MASTER

Where multiple systems are installed in close proximity, the radio signals of each system must be assigned a separate PTP domain in order to prevent message conflicts and overlaps between systems. Within each system, one Hub must be designated the Timing Master to manage the signal timing for that system. This is managed in the Configuration

settings; see section 5.2.2 for more information. This is configured by the system Administrator. The Hub's status as a Timing Master or Slave is indicated by the  LED.

The Timing Synchronisation indicator illuminates in the following modes:

- **On** – The Hub is configured as the system Timing Master, or is configured as a slave device that is synchronised to a Timing Master within the system
- **Flashing** – The Hub is configured as a slave device but is currently acting as the Timing Master
- **Off** – The Hub is configured as a slave device but is not synchronised to a Timing Master within the system

The Timing Synchronisation indicator temporarily changes illumination mode to recognise a press of the IP Address Reset button. After 60 seconds, the indicator returns to its original mode.


### 2.2.3 RADIO BEACON TRANSMISSION ACTIVE

The radio beacon transmission is indicated by the  icon.


During normal operation, this icon will flash to indicate that the Hub is creating and broadcasting the system network. The icon will only remain unlit in the following circumstances:

- A factory reset or controlled power-down has been initiated
- A system Archive is being restored
- The device has suffered an error and is not operating correctly

### 2.2.4 CONFIGURATION INSTALLED

Illumination of the  icon indicates that the Hub has received and applied its configured settings. This occurs during start-up and the indicator should illuminate within 60 seconds of the device powering on. The indicator remains illuminated during normal operation.

### 2.2.5 EKOTEK LOGO

When  is illuminated, the device is connected to an active external power supply. When powered only by the on-board batteries, this indicator is not lit.

## 2.3 Removing the lower front panel

To access the hardware interface connections, the lower front panel of the device casing must be removed.

To remove the front panel:

- a) Press the two Cover Release Clips  inwards towards the device interior
- b) Push the clips upwards and lift the front panel away from the device

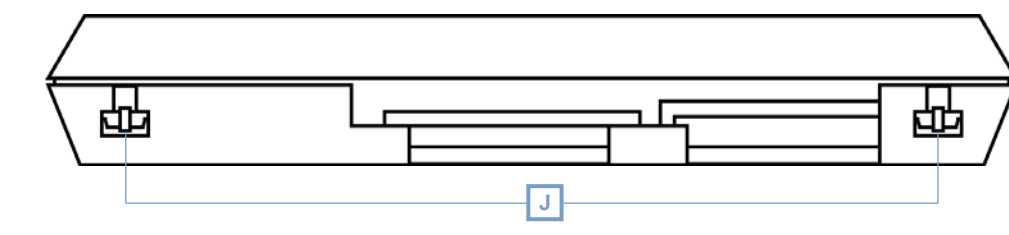


Fig. 3 Locating the Cover Release Clips

To replace the front panel, align and insert the casing tabs along the upper edge and press the bottom of the panel to lock it in place.

### 2.3.1 IP ADDRESS RESET BUTTON

The button **K** located between the two RS232 data ports beneath the removable lower front panel can be used for the following purposes:

- Resetting the IP address of the Hub
- Performing a controlled power-down procedure

When pressed, the illumination of the Timing Synchronisation indicator changes for 60 seconds to acknowledge the action; see section 2.2.2.

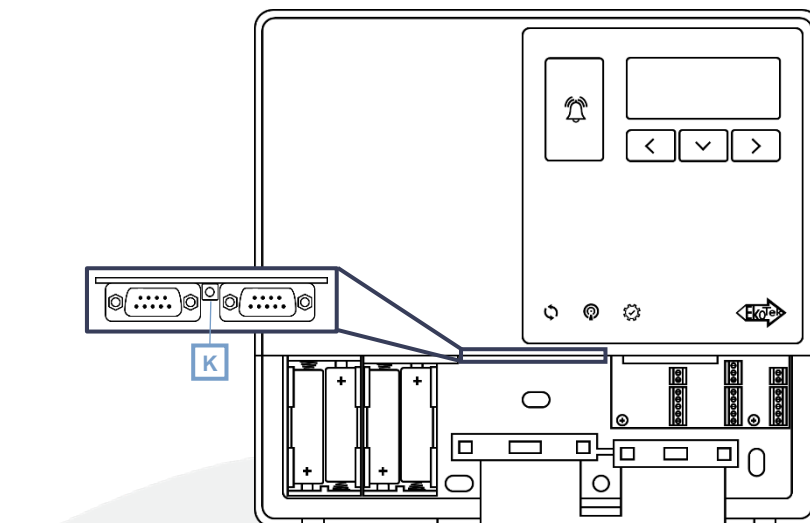


Fig. 4. Locating the IP Reset button beneath the removable front panel

**PLEASE NOTE:** Pressing the IP Address Reset button may disrupt the EkoSecure system. It should only be pressed when safe to do so and when any disruption can be managed accordingly.

#### Resetting the IP address of the Hub

To reset the IP address of the Hub to the default value of 192.168.1.2:


- Press and hold the reset button for approximately 1 second
- When **User 'super' enabled** is shown on the LCD display, press and hold the reset button for another 2 seconds
- The default IP address is shown on the LCD display

Once reset, the Hub can be accessed at its default address. The IP address of the device adaptor used to access the Hub must be within the same range as this address.

An additional press of the IP address reset button after its use to reset the Hub's IP address will restore the Hub to its previously configured address. The configured address is displayed on the LCD display.

#### Powering down the Hub using the IP Address Reset button

Pressing and holding the IP address reset button for at least 5 seconds will initiate a controlled power-down of the device. **Herunterfahren** is shown on the LCD display when the process is initiated. Once the message has appeared, wait for the power down process to complete. This may take up to 30 seconds.

**PLEASE NOTE:** If the IP address reset button is used to power down the device, the LCD display will switch off but the EkoTek logo  will remain illuminated in order to indicate an active external power supply. Removing and restoring the external power will restart the device.

## 3 Powering the device

The EkoSecure Hub can be powered by a Power over Ethernet connection or through a 12 V DC supply. PoE can be provided over Cat5e cabling by the supplied PoE Injector or a PoE-equipped network switch.

The device must also have 4 Ni-MH AA rechargeable cells with a minimum capacity of 2.4 Ah installed as an emergency supply in the event of external power failure. The device will only power on once the AA batteries have reached enough charge to independently power the device long enough for a controlled power-down procedure to be completed.

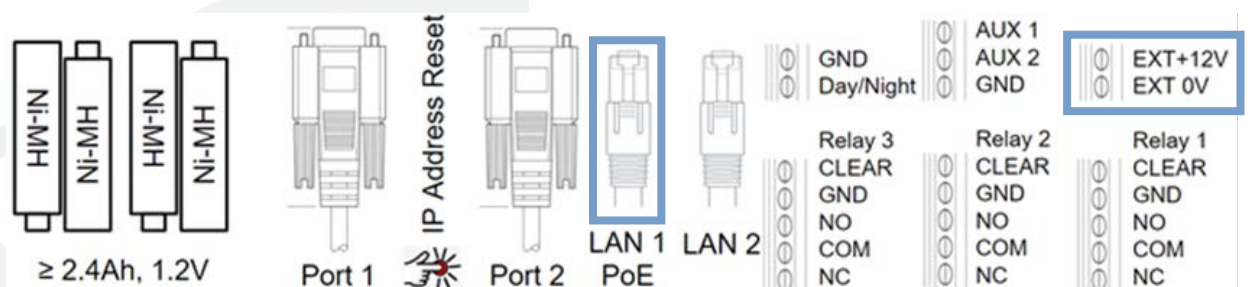





Fig. 5 The connections available beneath the lower front panel of the Hub, with potential external power connections highlighted

**CAUTION:** Installed batteries **MUST** be Nickel-metal hydride with a minimum of 2.4 Ah capacity. **DO NOT** install non-rechargeable batteries into the device. All 4 batteries must be installed before the device can be used.

The Hub's power connections can be accessed by removing the lower front panel.

## 3.1 Powering up the device

In the event that power must be manually restored to the Hub:

- a) Press the Cover Release Clips and remove the lower front panel
- b) Ensure that the 4 on-board batteries are installed
- c) Identify the Hub's external power source:
  - i) If the Hub is powered using Power over Ethernet (PoE):
    1. Unplug and reconnect the Ethernet cable connected to the **LAN 1** port
  - ii) If the Hub is powered using 12 V DC via the **EXT** Contacts:
    1. Ensure the DC power connection is connected via a 12 V DC power adapter to a mains power outlet
    2. Switch on the mains power
- d) The  logo on the front panel illuminates when an active power supply is connected
- e) The front panel display illuminates once the on-board batteries have reached enough charge to support a complete power-down procedure
  - i) If the on-board batteries are not sufficiently charged when external power is connected, the Radio Beacon  and Configuration  indicators will flash alternately while the device tests the battery state

## 3.2 Powering down the device

In the event that the Hub must be turned off, a controlled power-down procedure must be initiated.

**PLEASE NOTE:** Powering down the Hub will disable the EkoSecure network.

To perform a controlled power-down procedure:

- a) If the Hub web browser interface can be accessed easily:
  - i) Navigate to the Hub IP address and log in
  - ii) Navigate to **Konfiguration > Herunterfahren**; see section 5.13
  - iii) Select **System Neustart** or **Herunterfahren** from the drop-down menu as appropriate
  - iv) Press **BESTÄTIGEN** to confirm the action
- b) If the Hub web browser interface cannot be accessed easily:
  - i) Either:



1. Press and hold the IP address reset button until the LCD display shows **Herunterfahren**
  - A. See section 2.3.1
- ii) Or:
  1. Disconnect or disable the PoE or 12 V DC power supply
    - A. The lower front panel must be removed to disconnect an external power supply at the Hub interface; see section 2.3
  2. Allow the on-board battery charge to be exhausted
    - A. This will take at least 30 minutes
  3. When the battery charge is nearly exhausted, the Hub will autonomously trigger a controlled power-down procedure

**CAUTION: DO NOT** remove the on-board batteries while the device is still powered if there is no other power supply to the Hub. This will prevent the completion of a controlled power-down procedure and may result in data corruption. The batteries should only be removed when the device is no longer switched on.

### 3.2.1 CHANGING THE ON-BOARD BATTERIES

Over time the performance of the on-board backup batteries may deteriorate due to age or frequent use. The batteries must be replaced by Nickel-metal hydride rechargeable AA battery cells with a minimum capacity of 2.4 Ah, as supplied by Multitone.

To replace the on-board batteries:

- a) Ensure that the Hub is connected to an active external power supply
  - i) The device must remain powered throughout the battery change process to ensure that the new batteries are sufficiently charged to support a power failure
- b) Remove the front panel of the device
- c) Remove **ONLY** the 2 batteries from the left-hand holder and replace with new cells
- d) Remove **ONLY** the 2 batteries from the right-hand holder and replace with new cells

It is recommended that the batteries are replaced every **24 months** to ensure sufficient charge to support a power failure of at least 30 minutes.

**CAUTION: NEVER** install non-rechargeable batteries into the EkoSecure Hub. This may cause damage to the device and render it unsafe. Replace all 4 batteries at the same time. Always dispose of used batteries responsibly.

### 3.3 Failure of the external power supply

In the event that the primary power supply of PoE or 12 V DC becomes inactive during normal operation, the Hub performs the following actions:

- **Stromausfall** is displayed on the Hub's front panel display
- A Stromausfall message is sent to all devices in Pager Group 1

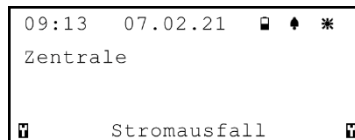


Fig. 6 Hub external power failure as indicated on the LCD display

This message is accompanied by an audio tone from the Hub, if enabled in the LCD display menu.

As the battery back-up power supply depletes, **Batterie NIEDRIG** messages are presented on the Hub front panel display.

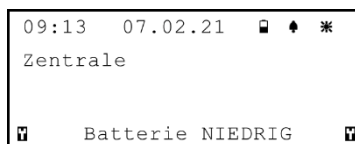


Fig. 7 Low charge remaining in the Hub's on-board batteries as indicated on the LCD display

If the external power supply is not restored, the Hub will perform a controlled power-down procedure to ensure that the system is switched off correctly.

#### 3.3.1 TOTAL POWER FAILURE

In the event that both the external power supply fails and the on-board batteries are exhausted, the Hub will perform a controlled power-down procedure. This will safely switch off the device, but will disable the EkoSecure network until power is restored.

## 4 Software interface

The EkoSecure Hub can be configured and managed through a web interface accessible by any browser-enabled device on the same network.

Functions such as adding system Devices, managing Alert Rules, and Hub maintenance must be completed via the web interface. Initial configuration is completed during installation by the system Engineer.

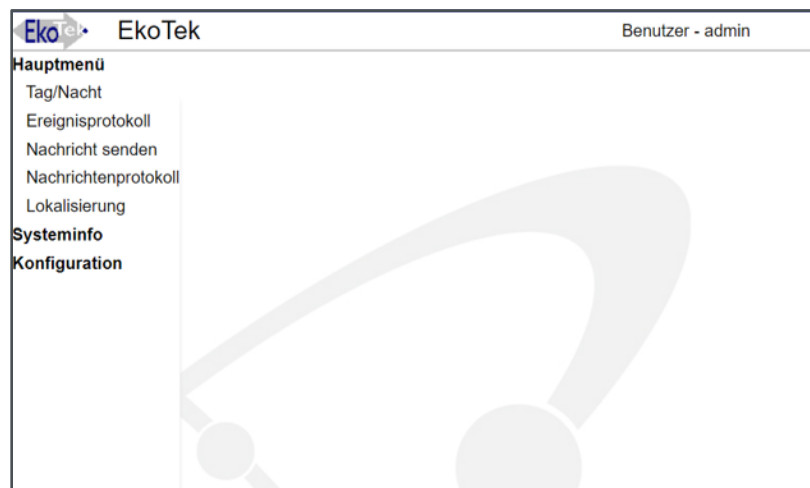


Fig. 8 The EkoSecure browser interface after login

## 4.1 Connecting a viewing device to the Hub

To view the EKSHUB web interface, the device used for access must have an IP address within the same network subnet as the Hub itself. The Hub has two individually configurable LAN ports to which a static IP address can be assigned; see section 5.1.

Where the Hub is installed as part of a wider LAN or WAN, other devices on that network may be able to access the Hub browser interface automatically through the network connection.

Where the Hub is not installed as part of a wider LAN or WAN, a wired connection must be made between the device used to access the web interface and one of the Hub's LAN ports. In this instance, the **IPv4** settings of the Ethernet Adapter of the accessing device may need to be manually set by the user. The **IP Address**, **Subnet Mask**, and **Default Gateway** settings must be configured so that they are within the same range as those configured for the connected Hub LAN port.

**PLEASE NOTE:** The Hub's LAN 2 port can only be used if enabled in the system configuration; see section 5.1.5.

## 4.2 Accessing the web interface

To access the Hub's web interface, enter the IP address of the connected Hub LAN port into the URL field of a browser on a device connected to the same network.

**PLEASE NOTE:** The default address of the Hub's LAN 1 port is **192.168.1.2**. This may have been changed during initial configuration. To view the currently configured IP address of the Hub, see section 8.5.1.

#### 4.2.1 LOGGING IN TO THE WEB PORTAL

Login credentials are required when accessing the web portal during a new browser session.



Fig. 9 The EkoSecure login page on the browser interface

The Hub is configured with two user accounts by default, each with differing levels of access privilege. See section 5.10 for login credentials and access restrictions.

#### 4.2.2 LOGGING OUT OF THE WEB PORTAL

To log out of the web portal, either:

- Click on the account name in the page header of the web portal interface
  - The browser returns to the portal log in page
- Close the web browser fully on the viewing device
  - The browser will prompt for a new log in when the browser reconnects to the Hub IP address

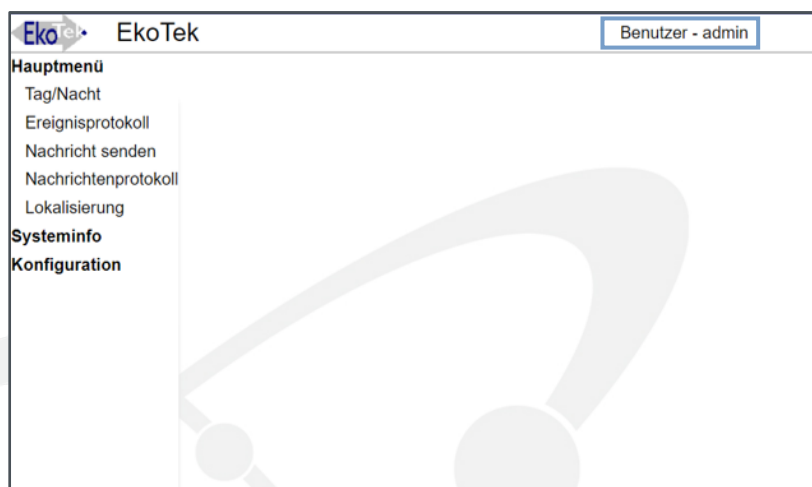


Fig. 10 To log out of the web interface, click the username at the top of the screen or fully close the web browser on the device

**PLEASE NOTE:** Automatic logout only occurs when the browser is no longer running on the device. If only the active tab or window is closed but the browser continues to run, the web portal will still be accessible without the need to log in.

## 5 Konfiguration menu

The EkoSecure Hub is configured through the web interface. Initial configuration is usually completed upon installation by the system Engineer, but the system settings can be managed and updated at any time by users logged in to the interface **admin** account.

To access the Hub configuration pages, click **KONFIGURATION** in the menu on the left of the screen. The following pages are available from the menu, and are only accessible by users logged in to the web portal with the username **admin** unless otherwise stated.

For guidance on accessing the Hub's web interface, see section 4.

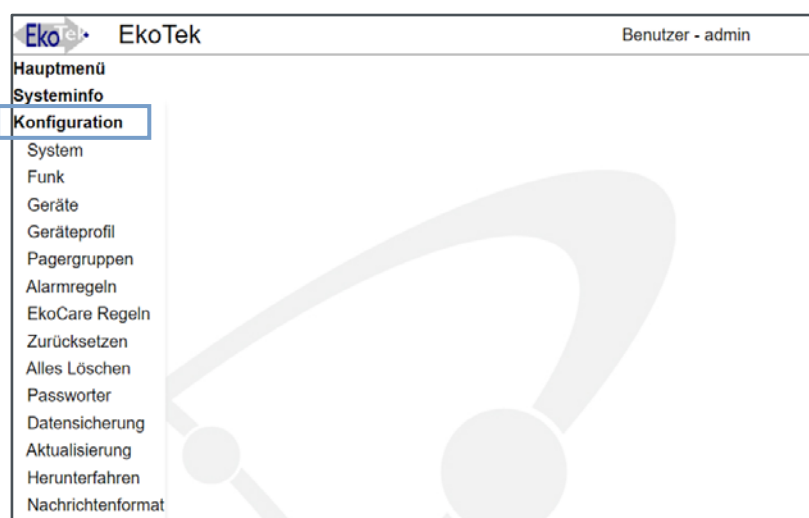


Fig. 11 To access the configuration pages, click the option in the left-hand menu

### 5.1 System settings

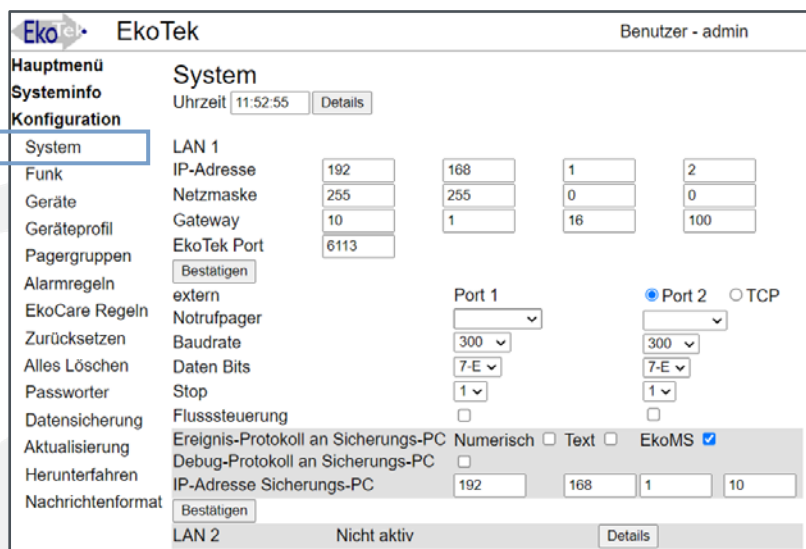


Fig. 12 The Hub System settings page

The Hub interface settings are configured in the System settings page of the interface menu. To edit the system settings, navigate to **Konfiguration > System**.

**PLEASE NOTE:** This page is also accessible by users logged in to the web interface with the **benutzer** account credentials, but only the **Uhrzeit** and **LAN 2** settings may be changed.

### 5.1.1 SYSTEM CLOCK

The **Uhrzeit** settings govern the internal clock of the entire EkoSecure system. If JavaScript is enabled for the active browser, the current time will update in real-time. If it is not enabled, the page will show the system time when the System settings page was loaded.

To configure the clock settings, click **DETAILS** beside the current time field.

Uhrzeit	Jahr	Monat	Tag	Stunden	Minuten
<input type="radio"/> manuell	2021	05	14	11	54
<input checked="" type="radio"/> NTP-Server	79	135	97	79	Offen

Datumsformat: tt/mm/jjjj  
 UTC-Zeitabstand: + 0 :00  
 Sommerzeit: EU

Bestätigen

Fig. 13 The Hub Uhrzeit settings

To apply changes to the clock settings, click **BESTÄTIGEN** beside the **Sommerzeit** parameter.

#### Clock modes

The system clock can be set manually or synchronised with an NTP server. Select the appropriate radio button to enable the desired mode.

If **Manuell** mode is selected, enter the appropriate values into the date and time fields.

**PLEASE NOTE:** If **Manuell** mode is selected, the system time will be set exactly at the value specified when **BESTÄTIGEN** is clicked. If the time is submitted considerably later than the value was entered, it may have become out of date. Ensure that the date and time values are correct when the changes are applied.

If an invalid value is submitted when **Manuell** mode is enabled, the changes are not applied and the page retains the settings from the last successful save.

If **NTP-server** is selected, enter the IP address of the NTP server from which the system time will be determined. If a connection to the NTP server is established, **Gültig** is displayed beside the address.

**PLEASE NOTE:** In the event that a Hub configured in NTP server mode does not receive a response to a request for the current time within 30 seconds, the Hub will continue with its current time data and send a new request in 24 hours. If the request is rejected by the NTP server, the Hub will no longer send requests to the NTP server and will display a **Abgelehnt** message beside the NTP server address.

### Datumsformat

The date format defined in the Hub determines the display format in the following locations:

- The LCD display on the Hub itself
- The display on Pagers connected to the system

The date can be displayed as either **tt/mm/jjjj** or **mm/tt/jjjj**. To apply the desired format, select the appropriate setting from the **Datumsformat** drop-down menu and click **BESTÄTIGEN**.

**PLEASE NOTE:** The timestamp logged for each record in the system Event Log, Pager Log, and Device Status pages are printed in **jjjj-mm-tt** format. This cannot be changed.

### UTC Zeitabstand

The **UTC Zeitabstand** setting can be used to adjust the configured system time according to global time zones and is intended to offset time data received from an NTP server.

Select an option from the UTC Zeitabstand drop-down menus to adjust the system time by the configured value and click **BESTÄTIGEN** to apply.

### Sommerzeit

To apply a Sommerzeit schedule to the Hub system time, select the appropriate region from the drop-down list. The system time will automatically adjust to accommodate the time changes on the appropriate date.

Click **BESTÄTIGEN** to apply.

## 5.1.2 HUB IP SETTINGS

The primary IP settings of the Hub are configured in the **LAN 1** section of the system settings page.

Hub devices are configured with the default IP address off **192.168.1.2**. To change this, enter a new address into the **IP-Adresse** fields.

LAN 1				
IP-Adresse	<input type="text" value="192"/>	<input type="text" value="168"/>	<input type="text" value="1"/>	<input type="text" value="2"/>
Netzmaske	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Gateway	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
EkoTek Port	<input type="text" value="6113"/>			
<input type="button" value="Bestätigen"/>				

Fig. 14 The Hub LAN 1 IP settings

If the Hub is to be connected to an external network via ethernet, ensure that the **IP-Adresse**, **Netzmaske** and **Gateway** parameters are set within the appropriate range. It is advised to leave the **EkoTek port** number at the default value of **6113** unless this conflicts with another network application. The LAN 1 settings apply to the PoE port beneath the removable front panel of the device; see sections 2.3 and 3.

To apply changes to the IP configuration, click **BESTÄTIGEN** beneath the **EkoTek port** parameter. If an invalid value is entered into the **IP-Adresse** fields, the changes are not applied and the settings stored at the last successful save are retained.

**PLEASE NOTE:** If the LAN 1 IP address of the Hub is changed and later restored to its default value using the IP address reset button, the configured LAN 1 IP address value is retained on the **System** page for future reference. To restore the configured IP address, press the IP address reset button again.

The Hub can only be accessed at the IP addresses assigned to LAN ports 1 and 2. If the IP address of the LAN 1 port is not known, it can be obtained from the display on the device itself; see section 8.5.1. For more information on the LAN 2 port settings, see section 5.1.5.

### 5.1.3 CONNECTING TO EXTERNAL SYSTEMS

The EkoSecure Hub can integrate with external and third-party systems via the two RS232 serial ports located on the device main pcb. Connections can use either TAP or ESPA 4.4.4 protocols and can be configured in the **Extern** region of the System settings page. Messages to and from external systems may be truncated according to their format.

	Port 1	<input checked="" type="radio"/> Port 2 <input type="radio"/> TCP
Extern		
Notrufpager	TAP aus ▼	▼
Baudrate	300 ▼	300 ▼
Daten Bits	7-E ▼	7-E ▼
Stop	1 ▼	1 ▼
Flusssteuerung	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Fig. 15 The Hub settings for external connections

**Port 1** can be used as an interface for the following:

- ESPA input (maximum 128 characters)
- ESPA output (maximum 128 characters)
- TAP input (maximum 138 characters)
- TAP output (maximum 138 characters)

**Port 2** can be used as an interface for the following:

- ESPA input (maximum 128 characters)
- TAP input (maximum 138 characters)



Select the interface type using the appropriate **Notrufpager** drop-down list.

**PLEASE NOTE:** The **Port 2** radio button must be selected in order to enable the port.

Once the port interface type is selected, configure the connection settings to match the external system:

- **Baudrate** – The data rate should be set to match the link speed (bits per second) of the external system
- **Daten Bits** – The format of the link data (7 bit even parity or 8 bit no parity)
- **Stop** – The number of stop bits per byte
- **Flusssteuerung** – Enabled or disabled as defined in the external system

To enable a TCP connection, select the **TCP** radio button; this disables Port 2 on the device and it cannot be configured. Selecting TCP enables the receipt of incoming TAP messages over a TCP connection through Port 1. The appropriate TCP port number must be entered into the **Port** text field.

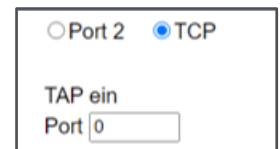


Fig. 16 Enabling a TCP connection over Port 1

Messages to external systems are triggered when an alarm message is sent to a Pager Group that includes a configured **External Notrufpager** in its listed devices.

Incoming messages can be addressed in the following ways:

- **0** – Sent to all Pagers in the EkoSecure system
- **[1 – 120]** – Sent to a specified Pager Group according to the numerical identifier
- **[HHNNNNNNNN]** – Sent to a specific Device according to the device identifier:
  - **HHH** – The Device Type hardware prefix
  - **NNNNNNN** – The Device serial number

**PLEASE NOTE:** In EkoSecure systems, only one Alarm Rule can be configured to send paging messages to an external system via the RS232 ports.

To save any changes to the external connections, click **BESTÄTIGEN** beneath the **IP-Adresse Sicherungs-PC** setting.

#### 5.1.4 REMOTE LOGGING

System event records, as stored in the Pager and Event logs, and paging messages transmitted and received through the network, can be shared with and stored in real-time by external logging systems if required. This can be used to enable the application of

additional software to extend system functionality or to assess and diagnose network performance faults.

Once the remote logging settings are configured, click **BESTÄTIGEN** beneath the **IP-Adresse Sicherungs-PC** setting to apply.

Fig. 17 The Hub settings for remote logging functionality

**PLEASE NOTE:** Sharing of this information directly from the Hub can only be configured to **one** external system or an integrated EkoMS server if present. Sharing with additional external systems may be configured through EkoMS, if available.

### Remote event logging

To enable remote storage of the Event log, select the required output type in the **Ereignis-Protokoll an Sicherungs-PC** field as appropriate for the external device. Multiple outputs can be selected. To enable sharing with an EkoMS server, enable the **EkoMS** option.

The logging output from the Hub includes the following message types:

- **Paging messages** – Output generated each time a Paging message or response is sent
- **Personal Security alarms** – Output each time a system alarm is raised
- **Maintenance messages** – Output each time maintenance messages are sent from devices

Remote logging information is sent within a transmission of SysLog formatted messages to UDP Port 514 of the configured **IP-Adresse Sicherungs-PC**. No validation of this address is performed.

For more information on the format and content of remote logging information, see Appendix C.

### Debug-Protokoll an Sicherungs-PC

The Remote debug logging function sends a record of every radio message from the system network to a remote machine. To enable the setting, select the **Debug-Protokoll an Sicherungs-PC** checkbox.

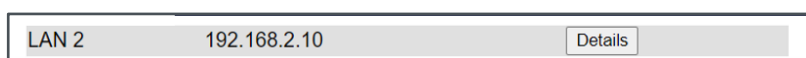
**PLEASE NOTE:** For standard operation, this setting should be disabled.

### IP-Adresse Sicherungs-PC

To identify the remote device with which the logging records will be shared, enter the device IP address in the **IP-Adresse Sicherungs-PC** fields. If sharing with an EkoMS server, the server address should be entered here.

### 5.1.5 LAN 2

For optimal performance, EkoSecure systems should be installed with a dedicated Local Area Network to which other network devices do not have access. This ensures that extraneous network activity is segregated from the system and does not impact on system performance.



LAN 2	192.168.2.10	Details
-------	--------------	---------

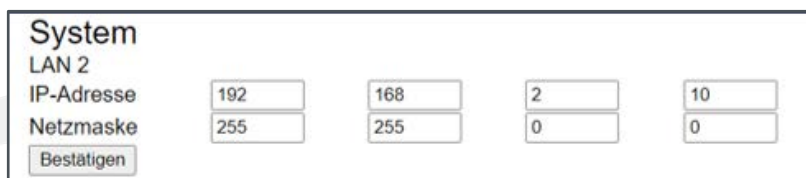
Fig. 18 The Hub LAN 2 IP settings

When the Hub is configured in this way, the LAN 1 port is used to connect any wired IP Slave Hub and SER devices. The LAN 2 port can then be configured with an additional IP address at which the web browser interface of the Hub can be accessed by remote devices. The LAN 2 port must be configured with an IP address that falls within a different subnet range to that of the LAN 1 port configuration.

**PLEASE NOTE:** The LAN 2 port is disabled by default and must be configured before it can be used to access the Hub browser interface.

To configure and access an additional IP address for the Hub:

- a) Click **DETAILS** in the **LAN 2** configuration area
- b) Enter a unique IP address and netmask into the appropriate fields
  - i) If the subnet range entered for the LAN 2 port matches the LAN 1 IP configuration, it will be rejected by the Hub and the original configuration maintained



<b>System</b>				
<b>LAN 2</b>				
IP-Adresse	192	168	2	10
Netzmaske	255	255	0	0
<b>Bestätigen</b>				

Fig. 19 Configuring the Hub LAN 2 IP settings on the Details page

- c) Click **BESTÄTIGEN** to apply the configuration
- d) Disable the WiFi capability of the remote device through which the new Hub IP address will be accessed
- e) Configure the Ethernet Adapter IPv4 settings of the remote device so that they are within the same range as the LAN 2 IP address of the Hub
  - i) For information on this process, see section 4.1

- f) Connect an ethernet cable between the remote device and the LAN 2 port of the Hub
  - i) Connection may also be made via a network switch
- g) Navigate to the LAN 2 IP address through a browser on the remote device

Once enabled, the LAN 2 port cannot be disabled. Entry of invalid IP credentials causes the page to refresh and retain the values from the last successful save.

## 5.2 Funk

The Hub radio communication configuration is managed in the Funk page of the interface menu. To edit the Radio settings, navigate to **Konfiguration > Funk**.

To confirm any changes to settings on the Funk page, click **BESTÄTIGEN**. All unsaved changes are lost.

EkoTek		Benutzer - admin	
<b>Hauptmenü</b>	<b>Funk</b>		
<b>Systeminfo</b>	Netzkennung	18	
<b>Konfiguration</b>	Synchronisation PTP domain	0	Master ▼
System	Frequenzsprung	Aus ▼	
<b>Funk</b>	Autoregistrierung Gerät	Aus ▼	
Geräte	Autoregistrierung Name	Zentrale ▼	
Geräteprofil			Bestätigen
Pagergruppen			Details
Alarmregeln			
EkoCare Regeln			
Zurücksetzen			
Alles Löschen			
Passwörter			
Datensicherung			
Aktualisierung			
Herunterfahren			
Nachrichtenformat			

Fig. 20 The Hub Funk settings page

### 5.2.1 NETZKENNUNG

In the event that several EkoSecure systems, each with their own Hub, are located in close proximity to each other, the Hub of each system should be given a numerical Network Identifier in order to differentiate between systems. This allows system devices to identify the network with which they are associated.

Some system devices can be configured to lock to the network to which they are registered in order to prevent migration to neighbouring systems. Using unique network identifiers for each system can assist devices locked to a system in ignoring messages from outside their intended network. For more information on locking devices to systems, see section 5.4.9.

To define a Network Identifier, enter a value into the **Netzkennung** field on the Funk configuration page. Only numeric characters are permitted.

**PLEASE NOTE:** Where multiple networks are installed within close proximity to each other, it is **STRONGLY** recommended that each network is configured with a unique Netzkenennung value. Devices should be locked to their intended network as appropriate.

### 5.2.2 SYNCHRONISATION PTP DOMAIN

Where multiple systems are installed on the same site, radio signal transmission within each system should be synchronised. This helps to avoid signal conflicts between systems, caused by simultaneous message delivery within overlapping networks.

Synchronisation is achieved via PTP. Each system must be synchronised to its own PTP domain, with one Hub in each system assigned as the system Timing Master. Other synchronisable devices are designated as Slave devices.

In the event that the Timing Master device develops an issue, one of the Slave devices automatically assumes the role of Master. The identity of this device is determined internally by the system. When the Timing Master device is restored and stable, it will resume the role of Master.

To apply Timing Synchronisation to a device and assign Timing Master or Slave status:

- a) Enter a numerical value into the text field
  - i) The default value is **0**
  - ii) Values **1-3** assign pre-set PTP configurations
  - iii) Values **4-127** can be used for user-defined configurations
- b) Select the synchronisation status of the device as either a **Master** or **Slave**
  - i) Only 1 device per system may be designated a Master; designating a second device as Master will change the original Master device into a Slave

Successful synchronisation as either a Timing Master or Slave is indicated by the Timing Synchronisation LED on the front panel of each Hub device; see section 2.2.2.

### 5.2.3 FREQUENZSPRUNG

The **Frequenzsprung** setting determines whether the 2.4 GHz Main Beacon channels of the system network broadcast over a single frequency or alternate between several frequencies as configured by the user. This setting is disabled by default, and in most instances is not required, but can be used to alleviate intermittent bursts of interference that occasionally cause disruption across the radio signal band. Most potential radio interference is identified during the site survey prior to installation and the system can be initially configured to accommodate the findings.

If required, Frequency Hopping can be enabled by selecting **Ein** from the drop-down list and clicking **BESTÄTIGEN**.

**PLEASE NOTE:** This setting **ONLY** affects the 2.4 GHz Main Beacon signal; the frequency of any 863-870 MHz signal is managed by the Hub's Adaptive Frequency Agility and Listen Before Talk capabilities.

In self-contained EkoSecure systems using only 860 MHz band frequencies for the Main Beacon, this setting has no effect.

If Frequency Hopping is disabled, devices within the system network will broadcast a 2.4 GHz signal over the singular channel frequency as assigned in the Device Mode configuration **ONLY**. Disabling Frequency Hopping is appropriate for environments with minimal 2.4 GHz radio traffic or where ambient 2.4 GHz signals are confined to specific frequencies. All frequencies are available as channels for Device Mode configurations.

If Frequency Hopping is enabled, a checkbox representing each of the 16 frequencies available to the 2.4 GHz band are added to the page. Use the checkboxes to select the frequencies over which the system 2.4 GHz signal will be broadcast; the signal will alternate between the chosen frequencies in a pre-configured order. Take note of the number of frequencies that are enabled.

Each frequency enabled defines a new 2.4 GHz network channel available for the Device Mode configurations. Each channel is numbered from 1 to a maximum of 16, based on the number of frequencies enabled, and defines the first frequency at which 2.4 GHz signals from devices assigned to that radio channel are broadcast. The sequence of the frequencies over which the 2.4 GHz signals are broadcast remains the same for each Channel, but is offset by the starting frequency as determined by the specific channel.

If some of the 16 available frequencies are disabled using the checkboxes, those frequencies do not define a new broadcast channel. The values available in the drop-down list of the Device Mode **Kanal** settings correspond to the number of the channel and **NOT** the number of the frequency that was selected.

**EXAMPLE:** The **Frequenzsprung** setting is enabled and the following frequencies are selected:

Frequenzen															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

The values in the drop-down list of the **Kanal** setting in the Device Mode configuration represent the following starting frequencies:

- **Kanal setting value 1** – Frequency 3
- **Kanal setting value 2** – Frequency 7
- **Kanal setting value 3** – Frequency 8
- **Kanal setting value 4** – Frequency 11
- **Kanal settings value 5-16** – Void

Enabling Frequency Hopping may be beneficial in environments with increased 2.4 GHz radio traffic or where other 2.4 GHz signals are not confined to specific frequencies.

**PLEASE NOTE:** The Channel checkboxes only appear after the Frequency hopping setting has been enabled and **BESTÄTIGEN** has been clicked. **BESTÄTIGEN** must then be clicked again to confirm the selected frequencies.

#### 5.2.4 AUTOREGISTRIERUNG GERÄT

The Hub can be instructed to automatically import device data from any new devices detected within the system mesh. New devices are registered automatically until the maximum number of system devices has been reached.

Devices imported automatically are given default names as defined by the **Autoregistrierung Name** setting; see section 5.2.5.

To enable automatic registration of devices, select **Ein** from the drop-down list. If this setting is disabled, devices must be added manually to the system through the **Geräte** page; see section 5.3.

Devices registered automatically are given the following settings by default:

- **Name** – As defined under **Autoregistrierung Name**
- **Benutzergruppe** – 1
- **Geräte zone** – 1
- **Geräteprofil** – 1

Any devices with a display are automatically added to Pager Group 1 until the maximum number of devices in the group is exceeded.

**PLEASE NOTE:** Where multiple systems are installed within close proximity to each other, it is **STRONGLY** recommended that the Device Auto-Register setting is disabled.

#### 5.2.5 AUTOREGISTRIERUNG NAME

This setting defines the names assigned to new devices that are automatically imported into the system when the **Autoregistrierung Gerät** setting is enabled. Each Device Type is pre-populated with a default value that can be customised as required. The serial number of the device can also be included, if preferred.

If the auto-register setting is not enabled, this setting does not apply.

To define custom names for Device Types:

- a) Select the required Device Type from the drop-down list and click **DETAILS**



Fig. 21 Select a Device Type from the drop-down list

- b) Enter a standard device name into the text field
  - i) All new devices of this type will be assigned this name when automatically registered into the system
- c) To include the device serial number in the device name when registered, select **Seriennummer**

Fig. 22 The Device Type auto-register details fields

- d) Click **BESTÄTIGEN** to confirm

**PLEASE NOTE:** Changes made apply only to the Device Type selected. Each Device Type must be configured separately.

## 5.3 Geräte

The Geräte page lists every system device recognised by the Hub, including both static and portable units. If the **Autoregistrierung Gerät** setting is enabled, this page is automatically populated. New devices can also be added manually through this page. To view and manage the Device list, navigate to **Konfiguration > Geräte**.

Gerät	Name	Geräteprofil	Benutzergruppe	Zone	Schwesteranruf
005-4885731	Hub - Foyer	1	1		
020-0037286	Pager 37286 - Cardiac 1	1	2	1	
020-0048892	Pager 48892 - Cardiac 2	1	2		
020-0035216	Pager 35216 - Cardiac 3	1	2		
020-0034461	Pager 34461 - Reception 1	1	3		
020-0037111	Pager 37111 - Reception 2	1	3		
020-0048814	Pager 48814 - Reception 3	1	3		
020-0049362	Pager 49362 - Security 1	2	4		
020-0045726	Pager 45726 - Security 2	2	4		
020-0039117	Pager 39117 - Security 3	2	4		
032-1802501	Repeater - Cardiac WR	1	2	2	
032-1830299	Repeater - Cardiac West Hall	1	2	2	
032-1802525	Repeater - Cardiac North Hall	1	2	2	
032-1803352	Repeater - Stairwell	1	1	1	
032-1813006	Repeater - Security Office	1	4	4	

Fig. 23 The Hub Device configuration page

The Devices table can be filtered using the search field at the top of the page, and the visibility of device information can be toggled using the checkboxes relating to the table columns. The following data can be viewed in the table:



- **Geräte** – The serial number of the device, including the Device Type prefix
  - This field cannot be edited
  - For a full list of Device Types that may be registered as part of an EkoSecure system and their corresponding serial number prefixes, see Appendix A.3
- **Name** – The user-friendly name assigned to the device
  - If **Autoregistrierung Gerät** is enabled under the **Funk** settings, this field is automatically populated with the configured value; see section 5.2.5
- **Geräteprofil** – The pre-configured operating mode assigned to the device
  - If **Autoregistrierung Gerät** is enabled under the **Funk** settings, new devices are automatically assigned Device Mode 1
  - For more information on configuring Device Modes, see section 5.4
- **Benutzergruppe** – Typically a reference to the personnel group to which the device is assigned
  - This may be used to group devices according to characteristics of the personnel that will carry them, e.g., role, shift pattern, etc.
  - This is used as an input condition for Alert Rules; see section 5.6
  - This is only applicable to Hub, IP Slave Hub, EkoCare Wall Units, and portable devices
  - This is **NOT** the Pager Group to which the device is assigned
- **Zone** – Use the Zone numbers to create areas within the network that can be used to identify parts of the system environment and locations in which specific device are not permitted to travel
  - This is only applicable to static devices
  - Zones are used as an input condition for Alert Rules; see section 5.6
- **Schwesternruf** – Linkage between applicable Zimmerfunkmodule
  - Bathroom Call Points can be linked to Nurse Call Wall Units and Flursignallampes
  - Flursignallampe devices can be linked together to illuminate in the same colours when alarms are raised
  - Up to 8 devices can be linked to the same Flursignallampe

**PLEASE NOTE:** The system does not distinguish between mains-powered and battery-powered variants of the same Device Type.

Only ESREP and ESPAG/IS devices may be used in EkoSecure regions of a system network.

### 5.3.1 MANUALLY ADDING A NEW DEVICE

To add a new device to the system manually:

- a) Click **NEU** at the top of the screen

- b) Select the appropriate Device Type from the drop-down list
- c) Ensure that the device number prefix shown matches the start of the serial number shown on the device, unless instructed otherwise in the dedicated device manual
- d) Enter the remainder of the serial number into the field
  - i) The remaining device number must be 7 digits in length
  - ii) Each device must have a unique serial number when registered
- e) Type a user-friendly **Name** to identify the device
  - i) It is recommended to include the Device Type and location in the device name
- f) Select the appropriate **Geräteprofil** from the drop-down list
  - i) Device Modes must be configured as appropriate for devices in each system
  - ii) For more information on Device Modes, see section 5.4
- g) Select the appropriate **Benutzergruppe** from the drop-down list
  - i) For more information on Groups, see section 5.5
- h) Select the appropriate **Zone** from the drop-down list
  - i) Zones can be used to define areas of the network to which different devices do not have access permissions
  - ii) Zones are defined by the static devices to which they are assigned
- i) If the new device is a Call Point, EkoCare Wall Unit, or Overdoor Light, it can be linked to an EkoCare Unit or Overdoor Light that has already been registered in the system using the **Schwesternruf** drop-down list
- j) Click **BESTÄTIGEN** to confirm

Fig. 24 Adding a new device

The new device is added to the list on the main Geräte page and can be edited by clicking directly in the table. All new devices with a built-in display (Hub devices, Pagers, etc.) are automatically added to Pager Group 1 provided the maximum group capacity of 35 devices has not been exceeded.

**PLEASE NOTE:** If the new device is entered with a serial number that already exists within the system, the existing device is updated to reflect the new details.

### 5.3.2 EDITING AN EXISTING DEVICE

To edit the settings of an existing device:

- a) Click any editable value relating to the required device within the table
  - i) All available fields can be edited, excluding the **Geräte** column
  - ii) Some fields are not available to all devices
- b) Enter or select the new value
- c) Click **BESTÄTIGEN** at the end of the row to confirm

Gerät	Name	Geräteprofil	Benutzergruppe	Zone	Schwesternruf	Bestätigen
005-4885731	Hub - Foyer	1	1	1		
020-0037286	Pager 37286 - Cardiac 1	1	2			
020-0048892	Pager 48892 - Cardiac 2	1	2			
020-0035216	Pager 35216 - Cardiac 3	1	2			
020-0034461	Pager 34461 - Reception 1	1	3			
020-0037111	Pager 37111 - Reception 2	1	3			
020-0048814	Pager 48814 - Reception 3	1	3			
020-0049362	Pager 49362 - Security 1	2	4			
020-0045726	Pager 45726 - Security 2	2	4			
020-0039117	Pager 39117 - Security 3	2	4			
032-1802501	Repeater - Cardiac WR	1	2	2		
032-1830299	Repeater - Cardiac West Hall	1	2	2		
032-1802525	Repeater - Cardiac North Hall	1	2	2		
032-1803352	Repeater - Stairwell	1	1	1		
032-1813006	Repeater - Security Office	1	4	4		

Fig. 25 Editing a device profile through the Devices list

### 5.3.3 REMOVING A DEVICE

To remove a device from the system:

- a) Click the serial number relating to the required device in the **Geräte** column of the table
- b) Click **ENTFERNEN** at the end of the row

**PLEASE NOTE:** Once removed, devices no longer function as part of that system network. Devices must be re-registered in order to rejoin the system.

## 5.4 Geräteprofil

Each device is assigned a Device Mode that defines the way in which it operates within the system. Up to 32 Device Modes may be configured for each Device Type, allowing specific devices to behave in different ways if required.

When first registered to the system, each device is assigned to Device Mode **1** by default, unless the maximum number of devices per Group has been reached. Device Modes can be manually assigned to each device on the **Geräte** page.



Fig. 26 The Device Mode configuration page

To configure Device Modes for each Device Type:

- Navigate to **Konfiguration > Geräteprofil** and identify the appropriate Device Type
- In the appropriate row, select the Device Mode to be viewed or edited from the drop-down list
- Click **DETAILS** in the appropriate row

The name of the selected Device Mode is displayed beside the Device Type at the top of the Details page and can be edited.



Fig. 27 Changing the name of a Device Mode

**PLEASE NOTE:** Renaming a Device Mode changes only the user-friendly identifier assigned to that Mode. Although the new name is displayed throughout the browser interface, each Device Mode is still managed by the system according to its original number. Regardless of any name changes, drop-down lists will always display Device Modes in numerical order according to their original number. Where multiple Device Modes are configured, it is recommended to use Device Mode names that identify the purpose of each Mode.

The configurable settings available for Device Modes vary between Device Types and are listed below in alphabetical order.

Once the settings for a Device Mode have been configured, click **BESTÄTIGEN** to apply. Where any invalid value is submitted, the setting will retain its last acceptable value.

**PLEASE NOTE:** In self-contained EkoSecure systems, only EKSHUB, ESREP, and ESPAG/IS devices may be used. Device Mode settings relating to other Device Types do not apply.

#### 5.4.1 ABSTELLRUF SETTINGS [FOB DEVICES]

These settings determine whether the Fobs in this mode may manually clear Emergency alarms that they themselves have raised, and how this is displayed on other devices. This setting is permanently disabled for this model of Hub.

**PLEASE NOTE:** Fob devices are not compatible with a DIN VDE V 0825-1 compliant system.

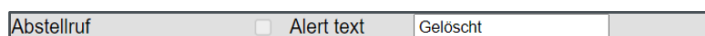


Fig. 28 The Abstellruf settings, as available for Fob Device Modes

#### Clearance (checkbox)

This setting is permanently disabled for this model of Hub.

#### Alert text (text field)

This defines the message that is displayed by Pagers and other devices with a screen when any alarm raised by a Fob in this Device Mode is cleared. This is set as **Gelöscht** by default.

As the **Clearance** setting is disabled, the **Alert text** value has no impact.

#### 5.4.2 AKUSTISCHER ALARM (DROP-DOWN LIST)

This setting determines whether devices in this Mode will sound an audible tone when an alarm is raised using that device.

When set as **Ein**, the audible tone will sound when an alarm is raised on that device; when set as **Aus**, alarms are raised silently on that device. If set to **Tag**, the audible alert will only sound when the system Shift setting is set to Tag; see section 6.1.



Fig. 29 The Akustischer Alarm setting

#### 5.4.3 ALARM LÖSCHEN SETTINGS [PAGER DEVICES]

These settings determine whether the Pagers in this Device Mode may manually clear Emergency alarms that they themselves have raised, and how this is displayed on other devices. This setting is permanently disabled for this model of Hub.

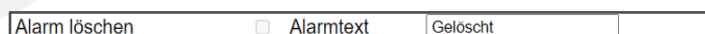


Fig. 30 The Alarm Löschen settings, as available for Pager Device Modes

**Clearance (checkbox)**

This setting is permanently disabled for this model of Hub.

**Alert text (text field)**

This defines the message that is displayed by other Pagers and devices with a screen when any alarm raised by a Pager in this Device Mode is cleared. This is set as **Gelöscht** by default.

As the **Clearance** setting is disabled, the **Alert text** value has no impact.

**5.4.4 ALARM WIEDERHOLUNG – INTERVALL (TEXT FIELD)**

This setting defines the length of time, in minutes, after which an active alarm raised by a device in this Mode is escalated if it has not been cleared. This is set at 1 minute by default.

When escalated, an alarm is resent with a **Hoch** escalation level. Alert Rules can be configured to handle alarms in specific ways based on their escalation level, allowing different or additional recipients to be contacted upon escalation if required; see sections 5.6 and 5.7.

Alarm Wiederholung	Intervall	1	(Minuten)
--------------------	-----------	---	-----------

Fig. 31 The Alarm Wiederholung setting

**5.4.5 ALARMBETRIEB SETTINGS [CALL POINT DEVICES]**

These settings enable Call Point Devices to be used to raise Manual alarms. These are raised when the **RED** button on the Device is pressed or the **ACTIVATE** and **GND** contacts are closed, as configured in the **Contact input** setting.

To enable Alarm Operation for Call Points in this Device Mode, click the **Alarmbetrieb** radio button. This disables the **Schwesternrufbetrieb** settings and Patient Call alarms cannot be raised; see section 5.4.25.

**PLEASE NOTE:** The contact inputs cannot be used as an alarm input if the device is configured to raise Patient Call alarms.

If a Call Point is linked to an EkoCare Unit for which the Anwesenheit setting has been enabled and is currently active (i.e., the **GREEN** button has been pressed to indicate Nurse Presence at an earlier alarm), all alarms raised by the Call Point until the Nurse Presence has been cleared (i.e., the **GREEN** button has been pressed a second time to clear the original alarm) are treated as an Emergency Alarm. Alarms raised by the Call Point during this time inherit the message code configured in the **Notruf – Alarm Text** setting of the linked EkoCare Unit.

The following settings are applied to devices in this Device Mode if **Alarmbetrieb** is enabled.

<b>Alarmbetrieb</b>		<input checked="" type="radio"/>
Manueller Alarm aktiv	<input type="checkbox"/>	Alarmtext <input type="text" value="Druckalarm"/>
		Betriebsart <input type="text" value="Einzelklick"/>
Alarm akustisch	<input type="checkbox"/>	
Kontakteingabe	<input type="checkbox"/>	Alarmtext <input type="text" value="Druckalarm"/>
		Betriebsart <input type="text" value="Umschaltung"/>
Alarm Wiederholung	<input type="checkbox"/>	Intervall <input type="text" value="1"/> (Minuten)
Abstellruf		Alert text <input type="text" value="Gelöscht"/>

Fig. 32 The Alarmbetrieb settings as available for Call Point devices

#### Manueller Alarm aktiv (checkbox)

This setting determines whether Manual alarms can be raised by pressing the alarm button on the device when the Alarmbetrieb settings have been enabled. Alarms raised via the contact inputs are configured separately.

#### Alarmtext (text field)

This setting defines the message text that is sent to other devices when a Manual alarm is raised from devices in this Mode. This is set as **Druckalarm** by default. The **Manueller Alarm aktiv** setting must be enabled for this setting to apply.

To customise this message, enter an alphanumeric string into the text field (maximum 20 characters).

#### Betriebsart (drop-down list)

This setting determines whether the alarm button on the device must be pressed once or twice in order to raise a Manual alarm. The **Manueller Alarm aktiv** setting must be enabled for this setting to apply.

#### Alarm akustisch (checkbox)

If enabled, the Call Point will sound an audible alert when an alarm is raised manually using the button on the device or via the contact inputs.

#### Kontakteingabe (checkbox)

See section 5.4.16.

#### Alarm Wiederholung (checkbox)

When enabled, the Call Point will escalate an alarm if it has not been cleared within the specified period of time. This applies to both manual and contact input alarms.

When escalated, an alarm is resent with a **Hoch** escalation level. Alert Rules can be configured to handle alarms in specific ways based on their escalation level, allowing different or additional recipients to be contacted upon escalation if required; see sections 5.6 and 5.7. To enable alarm escalation, ensure that the checkbox is selected.



**Intervall (text field)**

This setting defines the length of time, in minutes, after which an active alarm raised by a device in this Mode is escalated if it has not been cleared. This is set at 1 minute by default and applies to both Manual and contact input alarms.

**Alarm löschen – Alert text (text field)**

This defines the message that is displayed by Pagers and other devices with a screen when any alarm raised from the Call Point is cleared, and is set as **Gelöscht** by default.

**5.4.6 ALARMBETRIEB SETTINGS [FOB DEVICES]**

These settings enable standard alarm functionality for Fobs in this Device Mode. Alarms are raised automatically or by pressing the appropriate buttons on the device, according to their purpose.

To enable Alarm Operation for Fobs in this Device Mode, click the **Alarmbetrieb** radio button. This disables the **Schwesternrufbetrieb** settings and Patient Call alarms cannot be raised; see section 5.4.25.

The following settings are applied to devices in this Device Mode if **Alarmbetrieb** is enabled.

**PLEASE NOTE:** Fob devices are not compatible with a DIN VDE V 0825-1 compliant system.

<b>Alarmbetrieb</b>		<input checked="" type="radio"/>
Manueller Alarm aktiv	<input checked="" type="checkbox"/>	Alarmtext Druckalarm
		Betriebsart Einzelklick ▾
Alarm akustisch	<input checked="" type="checkbox"/>	
Alarm vibrieren	<input checked="" type="checkbox"/>	
Zeitalarm aktiv	<input type="checkbox"/>	Alarmtext Zeitalarm
Start Zeitalarm nach		30 (Minuten)
Quittierungszeit		5 (Sekunden)
Assistenzalarm aktiv	<input type="checkbox"/>	Alarmtext Assistenzalarm
		Betriebsart Einzelklick ▾
Permanent Eingeschaltet	<input type="checkbox"/>	

Fig. 33 The Alarmbetrieb settings as available for Fob devices

**Manueller Alarm aktiv enable (checkbox)**

This setting determines whether Manual alarms can be raised by pressing the **RED** alarm button on the device when the Alarmbetrieb settings have been enabled.

**Alarmtext (text field)**

This setting defines the message text that is sent to other devices when a Manual alarm is raised from devices in this Mode. This is set as **Druckalarm** by default. The **Manueller Alarm aktiv enable** setting must be enabled for this setting to apply.



To customise this message, enter an alphanumeric string into the text field (maximum 20 characters).

#### Betriebsart (drop-down list)

This setting determines whether the alarm button on the device must be pressed once or twice in order to raise a Manual alarm. The **Manueller Alarm aktiv enable** setting must be enabled for this setting to apply.

#### Alarm akustisch (checkbox)

If enabled, the Fob will sound an audible alert when an alarm is raised manually using the buttons on the device.

#### Alarm vibrieren (checkbox)

When enabled, the Fob will vibrate when an alarm is raised manually using the buttons on the device.

#### Zeitalarm aktiv settings

See section 5.4.27.

#### Assistenzalarm settings

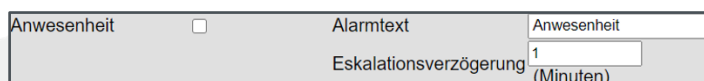
See section 5.4.8.

#### Permanent Eingeschaltet (checkbox)

When enabled, the device cannot be manually powered down using the **GREY** button.

### 5.4.7 ANWESENHEIT SETTINGS

These settings enable use of the **GREEN** Nurse Present button to indicate the presence of a responder when an alarm has been raised. When enabled, the Emergency and Nurse Assist buttons raise Patient Call alarms until the Nurse Present button has been pressed. Once Nurse Present has been pressed, the Emergency and Nurse Assist buttons both raise Emergency alarms until the Nurse Present button has been pressed a second time, clearing the alarms.



Anwesenheit <input type="checkbox"/>	Alarmtext	Anwesenheit
	Eskalationsverzögerung	1 (Minuten)

Fig. 34 The Anwesenheit settings as available on EkoCare Wall Units

#### Anwesenheit (checkbox)

When enabled, the **GREEN** Nurse Present button may be used to indicate the presence of a responder when an alarm has been raised. The button must be pressed a second time to clear an active alarm.

If the Attendance setting is disabled, each press of the Nurse Present button clears an active alarm raised from the device.

**Alarmtext (text field)**

This setting defines the message text that is sent to other devices when the Nurse Present button is pressed to indicate the presence of a responder. This is set as **Anwesenheit** by default. The **Anwesenheit** setting must be enabled for this setting to apply.

To customise this message, enter an alphanumeric string into the text field (maximum 20 characters).

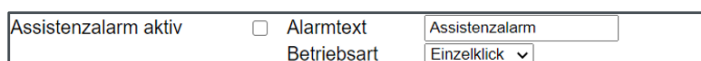
**Eskalationsverzögerung (text field)**

This setting defines the length of time, in minutes, by which escalation of the active alarm is delayed when the Nurse Present button is pressed to indicate attendance. The **Anwesenheit** setting must be enabled for this setting to apply.

This is set as 1 minute by default.

**5.4.8 ASSISTENZALARM SETTINGS**

These settings determine whether Assistenzalarm alarms can be raised manually by pressing the **BLUE** button on devices in this Mode, and how other devices display these alarms when received. These settings apply to Pager and Fob devices.



Assistenzalarm aktiv <input type="checkbox"/>	Alarmtext	Assistenzalarm
	Betriebsart	Einzelklick ▼

**Fig. 35** The Assistenzalarm settings

**Assistenzalarm aktiv (checkbox)**

When enabled, Assist alarms can be raised on devices in this mode by pressing the blue button.

**Alarmtext (text field)**

This setting defines the message text that is sent to other devices when an Assistenzalarm is raised from devices in this Mode. This is set as **Assistenzalarm** by default. The **Assistenzalarm aktiv** setting must be enabled for this setting to apply.

To customise this message, enter an alphanumeric string into the text field (maximum 20 characters).

**Betriebsart (drop-down list)**

This setting determines whether the alarm button on the device must be pressed once or twice in order to raise an Assist alarm. The **Assistenzalarm aktiv** setting must be enabled for this setting to apply.

**5.4.9 AUF NETZWERK FIXIEREN**

Where **Autoregistrierung Geräte** is enabled under the **Funk** settings (see section 5.2.4), the Hub will adopt any device within range of its network broadcast and register them as part of that system. In environments where system networks overlap, detection of the Main

Beacon from a neighbouring network may cause devices to defect to that system, preventing messages sent within the original system from being received on those devices.

Enabling the **Auf Netzwerk Fixieren** settings causes devices in that Mode to ignore any Main Beacon broadcasts from outside their registered system, ensuring that they do not join other networks without permission.

The **Auf Netzwerk Fixieren** setting is **disabled** by default. Where systems are installed in isolation and there is no interference or overlap from peripheral EkoFamily systems, or it is desirable for devices to migrate between cohabiting systems, it is not necessary to enable this setting. Where it is not desirable for devices to migrate between systems and there is a risk that this may occur, ensure that this setting is **enabled**.



Fig. 36 The Auf Netzwerk Fixieren setting

**PLEASE NOTE:** Static devices such as Repeaters and Call Points should not be permitted to migrate between systems as this will continually disrupt the network mesh. This will increase traffic over the network, interfere with Location Data, and cause additional power consumption by battery-powered devices. Ensure that **ALL** Device Modes relating to static devices are configured with the **Lock to network** setting **enabled**.

If a device that is locked to a network does not receive a signal from that network for a period of several hours, its locked status is overridden. This occurs in order to avoid circumstances in which a device is restricted to a specific network that is no longer reachable or does not exist.

**PLEASE NOTE:** When powered on, devices that are locked to a network use the parent system's **Netzkennung** value to determine the system to which they should connect. To ensure that devices are able to identify the correct network where several systems have been installed within close proximity to each other, the main Hub of each system should be configured with a unique Netzkennung value. For more information, see section 5.2.1.

#### 5.4.10 BEREICHSALARM SETTINGS

These settings identify any network areas into which portable system devices are not permitted to travel, and the way in which the resulting alarms are displayed by other devices.

Each static device is assigned to a network Zone, visible on the **Geräte** page; see section 5.3. Zones can be used to differentiate between areas of the network and to identify any areas into which specific portable devices are not permitted to be carried. The Zone from which an alarm is raised can be used as a parameter when configuring Alert Rules; see sections 5.6 and 5.7.

Bereichsalarm aktiv	<input type="checkbox"/>	Alarmtext	<input type="text" value="Wandern"/>												
Bereichsalarm akustisch	<input type="checkbox"/>														
Bereichsalarm vibrieren	<input type="checkbox"/>														
Verbotene Zone															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Fig. 37 The Bereichsalarm setting as available to Fob and Pager Device Modes

#### Bereichsalarm aktiv (checkbox)

When enabled, devices in this Mode will raise a Wander alarm if they receive location data from a static device that has been assigned to a network Zone to which they have not been granted access. Forbidden areas are identified under the **Verbotene Zone** setting. To clear a Wander alarm, return the device to an authorised network Zone.

**PLEASE NOTE:** Wander alarms may only be triggered when a device enters a new Zone. If access to the Zone in which a device is currently located is revoked, this will not be detected by the device until the device leaves that Zone and returns at a later time.

#### Alarmtext (text field)

This setting defines the message text that is sent to other devices when an Assist alarm is raised from devices in this Mode. This is set as **Wandern** by default. The **Bereichsalarm aktiv** setting must be enabled for this setting to apply.

To customise this message, enter an alphanumeric string into the text field (maximum 20 characters).

#### Bereichsalarm akustisch (checkbox)

When enabled, the device will emit an audio tone if location data from an unauthorised network Zone is received. The **Bereichsalarm aktiv** setting must be enabled for this setting to apply.

#### Bereichsalarm vibrieren (checkbox)

When enabled, the device will vibrate if location data from an unauthorised network Zone is received. The **Bereichsalarm aktiv** setting must be enabled for this setting to apply.

#### Verbotene Zone (multiple checkboxes)

Select the Zone identifiers that correspond to any network areas to which portable devices in this mode are not permitted access.

**PLEASE NOTE:** Multiple Zones may be selected; however, devices must be permitted access to at least one area of the network. If all network Zones are restricted, no Location alarms will be raised.

### 5.4.11 BEWOHNERRUF SETTINGS

These settings determine whether an EkoCare device in this Mode may be used to raise Patient Call alarms, and how other devices display these alarms when received.

Bewohnerruf	<input checked="" type="checkbox"/>	Alarmtext	Bewohner
-------------	-------------------------------------	-----------	----------

Fig. 38 The Bewohnerruf settings as available to EkoCare Device Modes

**Bewohnerruf (checkbox)**

When enabled, Patient Call alarms can be raised by pressing the **ORANGE** button on an EkoCare device in this Mode. For EkoCare Wall Units, the number of times any button must be pressed in order to raise an alarm is set as **1** and cannot be changed.

**Alarmtext (text field)**

This setting defines the message text that is sent to other devices when a Patient Call alarm is raised from devices in this Mode. This is set as **Bewohner** by default. The **Bewohnerruf** setting must be enabled for this setting to apply.

To customise this message, enter an alphanumeric string into the text field (maximum 20 characters).

**5.4.12 DOWNSTREAM-KANAL (DROP-DOWN LIST)**

This setting defines the 2.4 GHz radio frequency of the Main Beacon utilised by devices in this Mode for sending messages outwardly from the system Hub in the direction of portable devices. This may include manual alarms and other messages sent directly from the system Hub. This setting also defines the channel over which upstream messages from Child devices may be received by devices in this Mode.

Downstream-Kanal	Wie Bezugsgerät ▼
------------------	-------------------

Fig. 39 The Downstream-Kanal setting

If the **Frequenzsprung** setting on the Radio configuration page is disabled, all 16 specific channels listed in the drop-down menu are available for use.

If the **Frequenzsprung** setting is enabled, a channel is created for each broadcast frequency that was made available for use. Each channel is numbered consecutively from **1** up to the total number of frequencies that were enabled. Any channel numbers greater than this value are void.

**EXAMPLE:** If a total of **4** broadcast frequencies were enabled in the **Frequenzsprung** setting, channel numbers **1** to **4** may be used, representing each frequency in numerical order. Channels **5** and above may be selected but cannot be used.

If **Wie Bezugsgerät** is selected as the **Downstream-Kanal** value, the device will inherit the downstream radio channel from the parent device to which it is connected. When enabled, static devices will respond to a change in the radio channel of the parent device by adjusting its own broadcasts accordingly. This can be daisy-chained back to the system Hub.

**PLEASE NOTE:** The **Wie Bezugsgerät** option **MUST NOT** be selected as the Downstream Channel value where more than 60 static devices have been installed within a single system. This prevents static devices from migrating to other channels and exceeding the maximum number of devices.

Selection of a specific radio channel can be used to prevent devices in this Mode from autonomously adjusting their downstream broadcast frequency (in an attempt improve performance) when consistent transmission over a designated frequency is more desirable.


This may be useful in the following circumstances:

- The system contains more than 60 static devices, meaning that the number of devices broadcasting on each channel must be controlled
- To create channel regions within the network to ensure fixed transmission over channels with known low interference levels or to segregate areas of the network
  - Static devices in a radio subnetwork are configured to broadcast messages over the same specific channel, keeping network traffic contained and ensuring that devices do not reconnect elsewhere in the network
- To configure multiple devices that bridge between radio subnetworks by broadcasting messages received on one channel onwards on another channel as appropriate to access a new subnetwork
  - This can prevent peripheral devices from migrating to other channels and reducing the number of devices that bridge between differing radio subnetworks

#### 5.4.13 FREIGABE ZUR ALARMLÖSCHUNG (CHECKBOX)

This setting allows alarms to be cleared by a responder's device when in close physical proximity to the device that raised the alarm. When enabled, the **Quittiert** option is added to the list of alarm message responses on Pagers assigned to this Device Mode. When this response option is actioned, the device broadcasts a temporary short-range signal that clears the active alarm of a device within range, which is indicated by a **Ruf quittiert** message on the LCD display.

This setting is only available for Pager devices.



Freigabe zur Alarmlöschung ☐

Fig. 40 The Freigabe zur Alarmlöschung setting, as available for Pager Device Modes

**PLEASE NOTE:** In DIN VDE V 0825-1 compliant systems, **ONLY** devices for which this setting is enabled can be used to clear alarms raised by portable devices.

#### 5.4.14 FUNK (CHECKBOX)

This setting determines whether the devices in this Mode function as a network repeater.

Each static device is capable of emitting both a Main Beacon (network radio signal) and Location Beacon. The Main Beacon is used to establish wireless connections between devices and transmit system messages to and from the Hub; the Location Beacon delivers location data to nearby devices (see section 5.4.18).

If this setting is disabled, devices in this mode will not extend the system network or form downstream links to other devices. A device with the **Radio** setting disabled cannot act as a parent to other static devices but may use less battery power, and will continue to emit a 2.4 GHz Location Beacon from which portable devices within range are assigned location data that is reported back to the Hub. It is still possible to raise alarms on static devices for which the Radio setting has been disabled.



Fig. 41 The Funk setting

This setting should be enabled for all devices from which a wireless connection to other system devices is required.

**PLEASE NOTE:** It is recommended in most instances that the Funk setting is disabled for EkoCare Wall Units as these devices are typically installed below head height and the movement of people and equipment around the device may cause interference to the network signal.

#### 5.4.15 KANAL (DROP-DOWN LIST)

This setting defines the Main Beacon frequency over which devices in this Mode transmit messages downstream and receive upstream messages from Child devices. 2.4 GHz frequencies can be selected using the Channel identifiers (**1-16**) and 863-870 MHz transmission can be selected on applicable devices using **Long-Range**. This setting is only available for Hub, IP Client Hub, and Ethernet Repeater devices.



Fig. 42 The Funk Kanal setting, available for Hub, IP Slave Hub, and Ethernet Repeater devices

**PLEASE NOTE:** No more than **60** static devices should be assigned to the same channel.

If the **Frequenzsprung** setting on the Radio configuration page is disabled, all 16 specific channels listed in the drop-down menu are available for use.

If the **Frequenzsprung** setting is enabled, a channel is created for each broadcast frequency that was made available for use. Each channel is numbered consecutively from



1 up to the total number of frequencies that were enabled. Any channel numbers greater than this value are void.

**EXAMPLE:** If a total of **4** broadcast frequencies were enabled in the **Frequenzsprung** setting, channel numbers **1** to **4** may be used, representing each frequency in numerical order. Channels **5** and above may be selected but cannot be used.

Other static devices permit the selection of different channels for Upstream and Downstream traffic, which may be used to prevent devices from automatically switching the channel over which it broadcasts and receives messages; see sections 5.4.12 and 5.4.26. This is required when the number of static devices within a system exceeds **60** in order to prevent excessive numbers of devices migrating to the same channel.

**PLEASE NOTE:** It is recommended that Channel **15** is avoided where possible as this may interfere with location reporting within the system.

Hub devices can also be configured with the channel option **Long-Range**. For systems consisting solely of a Hub, Long Range Repeaters, and EkoSecure Pagers, it is recommended that **Long-Range** is selected. This limits message transmission to the 860 MHz band signal, which is managed automatically by the Hub's Adaptive Frequency Agility and Listen Before Talk capabilities.

**PLEASE NOTE:** The **Long-Range** option can only be used in systems containing a single radio subnetwork **ONLY**.

#### 5.4.16 KONTAKTEINGABE SETTINGS

These settings determine the way in which devices in this Mode respond to signals received over their contact inputs. These settings are only applicable to Long Range Repeater and Call Point devices.

Kontakteingabe	<input type="checkbox"/>	Alarmtext	Assistenzalarm
		Betriebsart	Umschaltung ▼

Fig. 43 The Kontakteingabe settings as available for Long Range Repeater and Call Point devices

**PLEASE NOTE:** These settings concern inbound alarm signals from outside the EkoSecure system. For Relay Contact settings relating to outbound alarm signals, see section 5.4.23.

##### Kontakteingabe (checkbox)

If selected, this setting enables the device to receive alarm inputs through its circuit contacts. When enabled, signals received through the contacts will raise an alert within the system.

EkoCare Wall Units can accept alarm inputs through **input port 2** on the base of the



device. If this setting is disabled, input port 2 can be used for an additional Bed Call button. Bed Call buttons should otherwise be connected to Port 1.

#### Alarmtext (text field)

This setting defines the message text that is sent to other system devices when an alert is raised as a result of a contact input. The default value of this setting varies according to the Device Type. The **Kontakteingabe** setting must be enabled for this setting to apply.

To customise this message, enter an alphanumeric string into the text field (maximum 20 characters).

#### Betriebsart (drop-down list)

This setting defines the type of the input signal. The **Kontakteingabe** setting must be enabled for this setting to apply.

Following options are available:

- **Umschaltung** – If no alarm is active, every switch change raises an alarm; if an alarm is active, every switch change raises an alarm clearance
- **Tastend** – A brief closure of the input switch raises an alarm; a second brief closure of the input switch clears the alarm
- **Geschaltet** – Sustained closure of the input switch raises an alarm until the switch opens and the alarm is cleared
- **Eingerastet** – A brief closure of the input switch raises an alarm; the alarm must be cleared by a signal down the **CLEAR** line or by the configured device button before another alarm can be raised

### 5.4.17 LAGEALARM SETTINGS

These settings determine whether Man Down functionality is enabled for devices in this Mode.

Lagealarm aktiv	<input type="checkbox"/>	Alarmtext	Lagealarm	
Trigger			5	(Sekunden)
Quittierungszeit			5	(Sekunden)

Fig. 44 The Lagealarm settings as available to Pager and Fob Device Modes

#### Lagealarm aktiv (checkbox)

If enabled, the Man Down alarm is raised automatically when the device is held out of its configured **Upright** orientation for a designated period. To clear a Man Down alarm, return the device to its configured Upright orientation. The Upright orientation of Pager devices can be set individually on each device using the **Aufrichten** setting in the Pager menu. The Upright position of Fob devices cannot be changed.

#### Alarmtext (text field)

This setting defines the message text that is sent to other devices when a Man Down is

raised. This is set as **Lagealarm** by default. The **Lagealarm aktiv** setting must be enabled for this setting to apply.

To customise this message, enter an alphanumeric string into the text field (maximum 20 characters).

#### **Trigger (text field)**

This setting defines the length of time, in seconds, for which a device in this Mode must be held out of its configured Upright orientation in order to raise a Man Down alarm. The **Lagealarm aktiv** setting must be enabled for this setting to apply.

This value cannot exceed 90 seconds. If a greater value is submitted, the setting will default to 90 seconds.

#### **Quittierungszeit (text field)**

This setting defines the length of time, in seconds, for which an audio tone will sound before a Man Down alarm is raised, to warn the user of the impending alarm. To prevent the alarm from being raised, return the device to its intended orientation.

This value cannot exceed 15 seconds. If a greater value is submitted, the setting will default to 15 seconds.

### **5.4.18 LOKALISIERUNGBEREICH (DROP-DOWN LIST)**

This setting defines the range of the 2.4 GHz Location Beacon signal transmitted by static devices in this Mode.

Each static device is capable of emitting both a Main Beacon (network radio signal) and Location Beacon. The Main Beacon is used to establish wireless connections between devices and transmit system messages to and from the Hub. The 2.4 GHz Location Beacon is a signal with shorter reach that delivers Location data to portable devices within range, but cannot be used to transmit system messages.

EkoSecure Repeaters also broadcast their Location Beacon over 868 MHz frequencies when the radio is enabled. The range of this signal is fixed and matches that of the Main Beacon.

Each portable device stores two types of Location data:

- The identity of the static device to which it current holds a radio (Main Beacon) connection
  - This device is considered the **Parent** of the portable device
- The identity of the static device from which it most recently received Location data
  - This is received by moving into range of the Location Beacon emitted by the device

Every time a portable device moves within range of the Location Beacon emitted by a static device, the portable device receives Location data from that source, identifying its current location. When the portable device leaves this range, it will continue to report the static device as its last known location until it moves within range of the Location Beacon of another device.

A portable device may be connected to the same static device from which it currently holds Location data. As the range of 2.4 GHz Location Beacons is shorter than that of Main Beacons, a portable device may move out of range of the network signal of one static device and establish a connection with another without travelling within range of the Location Beacon of the new device. When this happens, the parent of the portable device is now the new static device to which it is connected, but the Location data held by the portable device continues to identify the original static device as the last known location. This ensures that portable device **ONLY** report locations in which they have been proven to have been located, increasing the accuracy of location reporting.



Fig. 45 The Lokalisierungsbereich setting

The **Lokalisierungsbereich** setting determines the range of the 2.4 GHz Location Beacons of devices in that Mode, and is defined by a scale of 1-10, where **1** signifies a narrow range and **10** is the maximum range of the Location Beacon. The Range is set with a value of **2** by default, giving an approximate signal range of 3 m.

**PLEASE NOTE:** The **Lokalisierungsbereich** setting should not be set to higher values in areas where static devices are located in close proximity, even if separated by walls or floors, or in areas where more accurate location reporting is required. Overlapping Location Beacons may increase the difficulty of identifying the location of an alarm when raised.

#### 5.4.19 MANUELLER ALARM SETTINGS

These settings determine whether alarms can be raised manually by pressing the **RED** button on devices in this Mode, and how other devices display these alarms when received. For Pager and Fob devices, these settings apply to the Emergency alarm button.

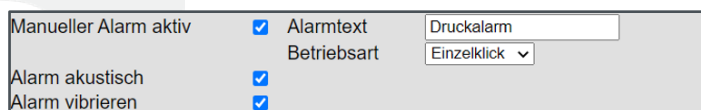


Fig. 46 The Manueller Alarm settings as available to Pager and Fob Device Modes; the Alarm Vibrieren setting is not available for static devices

##### Manueller alarm aktiv (checkbox)

In order to enable alarms to be raised by pressing the appropriate button on the device, ensure that the checkbox is selected. Deselecting the checkbox disables Manual Alarm functionality.

**Alarmtext (text field)**

This setting defines the message text that is sent to Pagers and other devices with display screens when an alarm is raised manually from devices in this Mode. This is set as **Druckalarm** by default. The **Manueller alarm aktiv** setting must be enabled for this setting to apply.

To customise this message, enter an alphanumeric string into the text field (maximum 20 characters).

**Betriebsart (drop-down list)**

This setting determines whether the alarm button on the device must be pressed once or twice in order to raise a manual alarm. The **Manueller alarm aktiv** setting must be enabled for this setting to apply.

**Alarm akustisch (checkbox)**

If enabled, the device will sound an audible alert when an alarm is raised manually using the button on the device. The **Manueller alarm aktiv** setting must be enabled for this setting to apply.

**Alarm vibrieren (checkbox)**

If enabled, the device will vibrate when an alarm is raised manually using the button on the device. The **Manueller alarm aktiv** setting must be enabled for this setting to apply.

The **Alarm vibrieren** setting is only available for Pager and Fob devices.

**5.4.20 NOTRUF SETTINGS [EKOCARE UNITS]**

These settings determine whether EkoCare devices in this Mode may be used to raise Emergency alarms, and how other devices display these alarms when received.

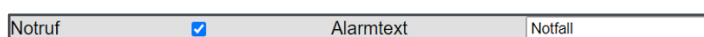


Fig. 47 The Notruf settings as available to EkoCare Wall Unit devices

**Notruf (checkbox)**

When this setting is enabled, Emergency alarms can be raised by pressing the **RED** button on an EkoCare device in this mode. On EkoCare Units, the number of times a button must be pressed to raise an alarm is set as **1** and cannot be changed.

If the **Anwesenheit setting** is enabled in the same Device Mode (see section 5.4.7), the **RED** Emergency button raises a Patient Call alarm unless the **GREEN** Nurse Present button has been pressed to indicate the presence of a responder. While the Nurse is present, the Emergency button can be used to raise Emergency alarms. A second press of the Nurse Present button clears any active alarms raised from the device and returns the Emergency button to Patient Call mode.

If the **Notruf** setting is disabled, the **RED** button raises a Patient Call on every press.

**Alarmtext (text field)**

This setting defines the message text that is sent to other devices when an Emergency alarm is raised from devices in this Mode. This is set as **Notfall** by default. The **Notruf** setting must be enabled for this setting to apply.

To customise this message, enter an alphanumeric string into the text field (maximum 20 characters).

**5.4.21 NUR LONG-RANGE / KONVERTOR (RADIO BUTTONS)**

These settings determine the signal types transmitted by EkoSecure Long Range Repeaters in this Mode and are used in conjunction with the **Funk** setting.

These settings are only applicable to Long Range Repeater devices.

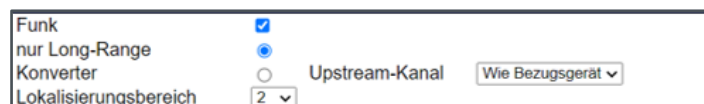


Fig. 48 The Nur Long-Range and Konvertor settings available to Long Range Repeater devices

Long Range Repeaters can be configured to perform one of three functions:

**Location Beacon only**

Long Range Repeaters can be configured so that they do not extend the system messaging network, but continue to emit a 2.4 GHz Location Beacon to deliver Location data to portable devices within range. Messages like alarms and status reports from other devices are not transmitted by devices configured in this way, however the battery life may be elongated.

To configure a Long Range Repeater to emit a Location Beacon only, apply the following settings:

- **Funk** – Disabled
- **Nur Long-Range / Konvertor** – Nur Long-Range
- **Upstream-Kanal** – N/A
- **Lokalisierungsbereich** – As appropriate; see section 5.4.18

**Secure Repeater with Long Range capability**

When configured as a Repeater, Long Range Repeaters transmit messages over 863-870 MHz radio frequencies, allowing the Repeater to extend the system messaging network, as well as broadcasting a Location Beacon over both 2.4 GHz and 860 MHz band frequencies.

To configure a Long Range Repeater with Repeater functionality, apply the following settings:

- **Funk** – Enabled
- **Nur Long-Range / Konvertor** – Nur Long-Range
- **Upstream-Kanal** – As appropriate to the network configuration
- **Lokalisierungsbereich** – As appropriate; see section 5.4.18

### Signal Converter

Where EkoSecure devices are installed as part of a wider EkoTek system, Long Range Repeaters can also be used to convert messages transmitted over 2.4 GHz radio frequencies into an 863-870 MHz signal. This allows messages from the EkoTek regions of the system to be broadcast into the EkoSecure region and vice versa.

To configure a Long Range Repeater with Converter functionality, apply the following settings:

- **Funk** – Enabled
- **Nur Long-Range / Konvertor** – Konvertor
- **Upstream-Kanal** – As appropriate to the network configuration
  - It may be appropriate to fix the Upstream Channel to ensure that messages back to the Hub are directed to the correct device when leaving the broadcast out of the EkoSecure region of the network; see section 5.4.26
- **Lokalisierungsbereich** – As appropriate; see section 5.4.18

### 5.4.22 REIßLEINE SETTINGS

These settings determine whether an alarm is raised by Pager devices when the Snatch Cord is removed (if installed). These settings are only available for Pager devices.

Reißleine aktiv	<input type="checkbox"/> Alarmtext	Reißleine
-----------------	------------------------------------	-----------

Fig. 49 The Reißleine alarm settings available to Pager Device Modes

#### Reißleine aktiv (checkbox)

When this setting is enabled, Pager devices in this Mode raise an alarm when the Snatch Cord is removed from the device. To clear the alarm, re-insert the Snatch Cord.

**PLEASE NOTE:** This setting should only be enabled for Pagers in which the Snatch Cord has been installed.

#### Alarmtext (text field)

This setting defines the message text that is sent to other devices when a Snatch Cord alarm is raised. This is set as **Reißleine** by default. The **Reißleine aktiv** setting must be enabled for this setting to apply.

To customise this message, enter an alphanumeric string into the text field (maximum 20 characters).

### 5.4.23 RELAIS-BETRIEB SETTINGS

These settings define the way in which the device's Relay Contacts respond to alarms and maintenance messages within the system, and are only available for Hub, IP Hub, and Ethernet Repeater devices.

Relais-Betrieb	
Zeitüberschreitung	Trigger
1 -	+
2 -	+
3 -	+

Fig. 50 The Relais-Betrieb settings available to Hub Device Modes

**PLEASE NOTE:** These settings concern alarm signals that are outbound from the EkoSecure system. For contact input settings relating to inbound alarm signals, see section 5.4.16.

The Hub Relay Contacts may be connected to external devices and circuits that react when an output is received from the Hub; this may include lights, sirens, and telephone diallers. These circuits may also have the potential to deliver a signal through the Clear contacts of the Hub Relays to clear the relevant alarms.

For more information on configuring Pager Groups, see section 5.5.

For more information on alert handling and Rules, see sections 5.6 and 5.7.

Relay Contact connections should be installed by the system engineer.

#### Relay 1

All personal alarm messages that are sent to a Pager Group of which the Hub is a member also trigger an output via the Hub's Relay 1 contacts. This Relay 1 output via Relay 1 can be cleared using one of the following methods:

- Pressing any navigation button on the Hub front panel upon receipt of the alarm
- Receipt of a signal through the **Clear** contact of Relay 1
- Expiration of the **Zeitüberschreitung** period configured using the Relay 1 drop-down list
  - If the **Zeitüberschreitung** setting is for Relay 1, the Relay can only be deactivated using the other methods

**PLEASE NOTE:** In DIN VDE V 0825-1 compliant systems, the Hub should be assigned to **ALL** configured Pager Groups to ensure that it is notified of all system alarms.

#### Relays 2 and 3

Relays 2 and 3 can be configured independently to activate in response to alarm messages sent to other Pager Groups. The Hub is not required to be a member of the



Pager Groups to which Relays 2 and 3 respond; however, if the Hub is not a member of the Pager Groups assigned to Relays 2 and 3, the alarm will not be displayed on the Hub LCD display.

The Relays can also be configured to activate in response to system Maintenance Messages according to their designated message **Stufe**, as configured on the **Rangfolge der Nachrichten** page of the **Systeminfo** menu; see section 7.4. To achieve this, select **Maintenance 1** or **Maintenance 2** as appropriate from the relevant **Trigger** drop-down list.

It is also possible to configure the Relays to trigger an output when any Personal Alarms or Maintenance Messages are raised within the EkoSecure system. This can be achieved by selecting **Immer aktiv** in the appropriate **Trigger** drop-down list.

Once activated, Relay 2 and 3 outputs can be cleared using one of the following methods:

- Clearing the alarm on any device from the Pager Group to which the alarm was sent
- Receipt of a signal through the **Clear** contact of the appropriate Relay
- Expiration of the **Zeitüberschreitung** period configured using the appropriate drop-down list
  - If the **Zeitüberschreitung** setting is left blank, the Relay can only be deactivated using the other methods

Signal output via Relays 2 and 3 can be configured independently in response to the following **Trigger** options, available in the drop-down list for each Relay:

- **[1-120]** – Activated when an alarm is sent to the selected Pager Group
  - The Hub does not need to be a member of that Pager Group to activate the Relay
- **Wartung 1** – Activated when a Maintenance Message classified as **Stufe 1** is generated within the system
- **Wartung 2** – Activated when a Maintenance Message classified as **Stufe 2** is generated within the system
- **Immer aktiv** – Every Personal Alarm or Maintenance Message raised within the system activates the Relay
- If the **Trigger** is left blank, the Relay is disabled

For more information on Maintenance Message ranking, see section 7.4.

#### 5.4.24 SCHWESTERNRUF SETTINGS [EKOCARE UNITS]

These settings determine whether EkoCare devices in this mode may be used to raise Nurse Assist alarms, and how other devices display these alarms when received.

Schwesternruf	<input checked="" type="checkbox"/>	Alarmtext	Assistenz
---------------	-------------------------------------	-----------	-----------

Fig. 51 The Schwesternrufbetrieb settings as available to EkoCare Device Modes



**Schwesternruf (checkbox)**

When enabled, Nurse Assist alarms can be raised by pressing the **BLUE** button on an EkoCare device in this Mode. On EkoCare Units, the number of times a button must be pressed to raise an alarm is set as **1** and cannot be changed.

If the **Anwesenheit** setting is enabled in the same device mode (see section 5.4.7), the **BLUE** Nurse Assist alarm button raises a Patient Call alarm unless the **GREEN** Nurse Present button has been pressed to indicate the presence of a responder. While the Nurse is present, the Nurse Assist button raises Emergency alarms when pressed. A second press of the Attendance button clears any active alarms raised from the device and returns the Nurse Assist button to Patient Call mode.

If the Nurse Call setting is disabled, the **BLUE** button raises a Patient Call when pressed.

**Alarmtext (text field)**

This setting defines the message text that is sent to other devices when a Nurse Assist alarm is raised from devices in this Mode. This is set as **Assistenz** by default. The **Schwesternruf** setting must be enabled for this setting to apply.

To customise this message, enter an alphanumeric string into the text field (maximum 20 characters).

### 5.4.25 SCHWESTERNRUFBETRIEB SETTINGS [CALL POINT AND FOB DEVICES]

These settings enable the alarm buttons on Call Point and Fob devices in this Mode to be used to raise Patient Call alarms, and the way in which the device responds when this occurs. If **Schwesternrufbetrieb** is enabled for a Call Point or Fob, all alarm buttons raise a Patient Call alarm when pressed.

<b>Schwesternrufbetrieb</b> <input type="radio"/>	
Bewohnerruf	Alarmtext <input type="text" value="Bewohner"/>
Akustischer Alarm <input type="button" value="Aus"/>	
Priorität	Intervall <input type="text" value="1"/> (Minuten)

Fig. 52 The Schwesternruf settings as available to Call Point and Fob Device Modes

If a Call Point is linked to an EkoCare Unit for which the Attendance setting has been enabled and is currently active (i.e., the **GREEN** button has been pressed to indicate Nurse Presence at an earlier alarm), all alarms raised by the Call Point until the Nurse Presence has been cleared (i.e., the **GREEN** button has been pressed a second time to clear the original alarm) are treated as an Emergency Alarm. Alarms raised by the Call Point during this time inherit the message code configured in the **Notruf – Alarmtext** setting of the linked EkoCare Unit.

**PLEASE NOTE:** Enabling **Schwesternrufbetrieb** for Fob devices causes all alarm buttons on the device to raise a Patient Call alarm when pressed. Automatic alarms,

including Man Down and Dead Man alarms, are raised as normal.

#### Schwesternrufbetrieb (radio button)

Enabling these settings causes Call Point and Fob devices in this mode to raise a Patient Call when any alarm button on the device is pressed. When **Schwesternrufbetrieb** is enabled, the **Alarmbetrieb** settings are ignored. To enable these settings, select the radio button.

#### Bewohnerruf – Alarmtext (text field)

This setting defines the message text that is sent to other devices when a Patient Call is raised from devices in this Mode. This is set as **Bewohner** by default. The **Schwesternrufbetrieb** settings must be enabled for this setting to apply.

To customise this message, enter an alphanumeric string into the text field (maximum 20 characters).

#### Akustischer Alarm (drop-down list)

When set as **Ein**, the Call Point will sound an audible alert when a Patient Call alarm is raised manually using the button on the device. If set to **Tag**, the audible alert will only sound when the system Day Shift is active; see section 6.1.

#### Priorität – Intervall (text field)

This defines the length of time, in minutes, after which Patient Call alarms raised by devices in this Mode are escalated if they have not been cleared. This is set as 1 minute by default. Alarm escalation procedures can be defined on the Alert Rules page; see section 5.6.

When escalated, an alarm is resent with a **Hoch** escalation level. Alert Rules can be configured to handle alarms in specific ways based on their escalation level, allowing different or additional recipients to be contacted upon escalation if required; see sections 5.6 and 5.7.

### 5.4.26 UPSTREAM-KANAL (DROP-DOWN LIST)

This setting defines the 2.4 GHz radio frequency of the Main Beacon utilised by the device for sending messages upwards through the network towards the system Hub. This may include alarms raised by portable devices, Device Status reports and Maintenance Alarms. This setting also defines the channel over which downstream messages from Parent devices may be received by devices in this Mode.

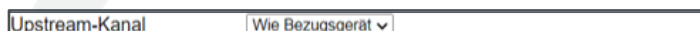


Fig. 53 The Upstream-Kanal setting

If the **Frequenzsprung** setting on the Radio configuration page is disabled, all 16 specific channels listed in the drop-down menu are available for use.

If the **Frequenzsprung** setting is enabled, a channel is created for each broadcast frequency that was made available for use. Each channel is numbered consecutively from 1 up to the total number of frequencies that were enabled. Any channel numbers greater than this value are void.

**EXAMPLE:** If a total of 4 broadcast frequencies were enabled in the **Frequenzsprung** setting, channel numbers 1 to 4 may be used, representing each frequency in numerical order. Channels 5 and above may be selected but cannot be used.

If **Wie bezugsgerät** is selected as the **Upstream-Kanal** value, the device will inherit the upstream radio channel from the parent device to which it is connected. This allows the device to use any available repeating device as a parent in order to expedite delivery of upstream messages. This option should be selected in most instances to allow devices in this Mode to select the best channel over which to broadcast messages upstream, increasing the likelihood that system alarms are transmitted on the clearest channel at the time they are raised.

Selection of a specific radio channel can be used to prevent devices in this Mode from adjusting their upstream broadcast frequency when interference on other channels is likely or to designate devices as a channel changeover point between channel regions.

This may be useful in the following circumstances:

- To create radio subnetworks within the system to ensure fixed transmission over channels with known low interference levels or to segregate areas of the network
  - Static devices in a radio subnetwork are configured to broadcast messages over the same specific channel, keeping network traffic contained and ensuring that devices do not reconnect elsewhere in the network
- To configure multiple devices that bridge between radio subnetworks by broadcasting messages received on one channel onwards on another channel as appropriate to access a new subnetwork
  - This can prevent peripheral devices from migrating to other channels and reducing the number of devices that bridge between differing radio subnetworks
- To force specific devices to connect to the appropriate Synchronised Ethernet Repeater (SER), where several are installed
  - This method can be used to create subnetworks within a system where groups of devices managed by each SER
  - This can also reduce the number of network hops back to the Hub

The Upstream Channel of devices in systems comprising more than 60 static devices do not necessarily need to be fixed as system upstream traffic is more infrequent and fragmented than downstream traffic.

**PLEASE NOTE:** It is recommended to avoid channel **15** where possible as this may interfere with the network Location data transmissions.

#### 5.4.27 ZEITALARM SETTINGS

These settings determine whether Dead Man alarm functionality is enabled for devices in this Mode. This is an automatic alarm that is raised if no input is received from the user when prompted at the configured interval. To respond to a Dead Man prompt when received, press any of the navigation buttons on the device.

Zeitalarm aktiv	<input type="checkbox"/>	Alarmtext	Zeitalarm
Start Zeitalarm nach		30	(Minuten)
Quittierungszeit		5	(Sekunden)

Fig. 54 The Zeitalarm settings

##### Zeitalarm aktiv (checkbox)

If this setting is enabled, devices in this Mode will prompt users for a response the defined interval. Prompts are signalled by an audio tone from the device and will accept any navigation button press as a response; for more information, see section 8.4.

##### Alarmtext (text field)

This setting defines the message that is displayed by Pagers and other devices with a screen upon receipt of a Dead Man alarm raised by devices in this Mode. This is set as **Zeitalarm** by default. The **Zeitalarm aktiv** setting must be enabled for this setting to apply.

To customise this message, enter an alphanumeric string into the text field (maximum 20 characters).

##### Start Zeitalarm nach (text field)

This setting defines the length of time, in minutes, between Dead Man prompts on the device. This value cannot exceed 30 minutes. If a greater value is submitted, the setting will default to 30 minutes.

##### Quittierungszeit (text field)

This defines the length of time, in seconds, in which a user must respond to a Dead Man prompt from the device before an alarm is raised. During this period, devices emit an audible tone until a response is received or the configured time elapses..

This value cannot exceed 15 seconds. If a greater value is submitted, the setting will default to 15 seconds.

## 5.5 Pagergruppen

Devices capable of presenting message and alarm outputs via LCD displays or Relay Contacts can be assigned to Pager Groups. These devices include:

- Hub devices
- IP Slave Hub devices
- Ethernet Repeaters
- Long-Range-Repeater devices
- Pager devices
- Overdoor Lights

External paging devices can also be added to Pager Groups.

The system can be configured to notify only specific Pager Groups when alarms are raised, meaning that only the appropriate personnel are notified of a particular situation.

When **Autoregistrierung Gerät** is enabled (see section 5.2.4), all new devices with a display or Relay output are automatically added to **Pager Group 1** provided that the maximum group capacity of 35 devices has not been exceeded. Devices can be assigned to any number of Pager Groups, including none. Up to 120 different Pager Groups may be configured.

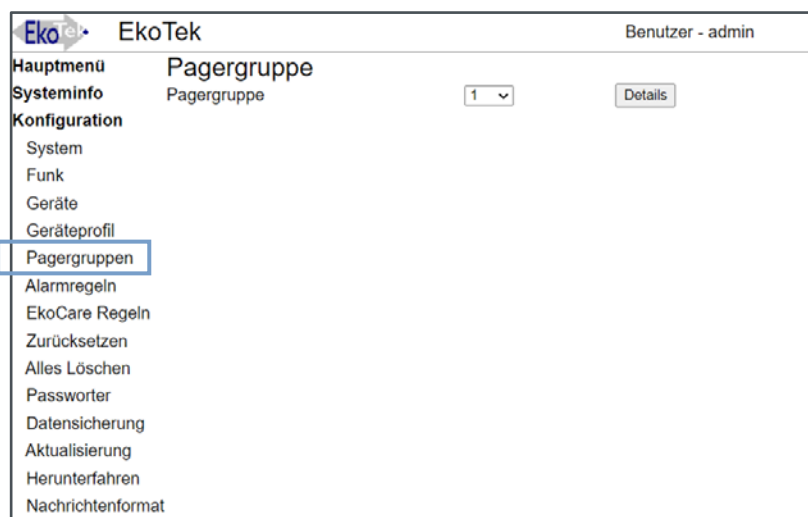


Fig. 55 The Pager Group configuration page

**PLEASE NOTE:** If multiple Pager Groups are configured, **Alert Rules** must be configured to ensure that system alarms are delivered correctly; see section 5.6.

To view and manage Pager Groups, navigate to **Konfiguration > Pagergruppen** using the web interface menu.

### 5.5.1 MANAGING PAGER GROUPS

To view or configure a Pager Group:

- a) Select the appropriate Pager Group from the drop-down list and click **DETAILS**
  - i) The **Details** page lists all registered system devices with Pager

## Group capability

- b) Enter an appropriate Group name into the **Pagergruppe** text field
  - i) It is recommended that the name identifies the purpose of the Group
  - ii) Maximum 10 characters

**PLEASE NOTE:** Renaming a Pager Group changes only the user-friendly identifier assigned to that Group; although the new name is displayed throughout the browser interface, each Pager Group is still managed by the system according to its original number. Regardless of any name changes, drop-down lists will always display Pager Groups in numerical order according to their originally assigned number.

Where multiple Pager Groups are configured, it is recommended to apply names that clearly differentiate between Groups and their purpose.

- c) Select any devices to be included in the Pager Group
  - i) To include a device in the Pager Group, ensure the checkbox corresponding to that device is selected

EkoTek		Benutzer - admin
Hauptmenü	Pagergruppe	
Systeminfo	[001]Pagergruppe Security	
Konfiguration	005-4885731 Hub - Foyer	<input checked="" type="checkbox"/>
System	020-0037286 Pager 37286 – Cardiac 1	<input type="checkbox"/>
Funk	020-0048892 Pager 48892 – Cardiac 2	<input type="checkbox"/>
Geräte	020-0035216 Pager 35216 – Cardiac 3	<input type="checkbox"/>
Geräteprofil	020-0034461 Pager 34461 – Reception 1	<input checked="" type="checkbox"/>
Pagergruppen	020-0037111 Pager 37111 – Reception 2	<input checked="" type="checkbox"/>
Alarmregeln	020-0048814 Pager 48814 – Reception 3	<input checked="" type="checkbox"/>
EkoCare Regeln	020-0049362 Pager 49362 – Security 1	<input checked="" type="checkbox"/>
Zurücksetzen	020-0045726 Pager 45726 – Security 2	<input checked="" type="checkbox"/>
Alles Löschen	020-0039117 Pager 39117 – Security 3	<input checked="" type="checkbox"/>
Passwörter	032-1802501 Repeater – Cardiac WR	<input type="checkbox"/>
Datensicherung	032-1830299 Repeater – Cardiac West Hall	<input type="checkbox"/>
Aktualisierung	032-1802525 Repeater – Cardiac North Hall	<input type="checkbox"/>
Herunterfahren	032-1803352 Repeater – Stairwell	<input type="checkbox"/>
Nachrichtenformat	032-1813006 Repeater – Security Office	<input type="checkbox"/>
	External Pager 000152043006277	<input checked="" type="checkbox"/>

Fig. 56 The Pagergruppe Details page where individual devices are assigned to a Group

- ii) To include an external paging device in the Pager Group:
  1. Enter the Pager identifier as sent by the ESPATAP output interface into the **External Notrufpager** field
  2. Select the checkbox corresponding with the external Pager

**PLEASE NOTE:** Only one external paging device can be included in each Pager Group.

- d) Click **BESTÄTIGEN** to confirm the configuration
  - i) If the new Pager Group configuration now includes more than 35 devices, changes will not be accepted

## 5.6 Alarmregeln

Alert Rules are used to determine which alarms are sent to which devices when raised, allowing specific devices to be targeted when certain conditions are met. This avoids every alarm being sent to every device where this is not desirable. To view and create Alert Rules, navigate to **Konfiguration > Alarmregeln**.

No Alert Rules are initially configured. When no Alert Rules have been configured, all alarms raised through the system delivered to Pager Group 1 by default. Alarms that do not meet the criteria of any of the configured Alert Rules are also sent to Pager Group 1. All new devices with a built-in display (Hub devices, Pagers, etc.) are automatically added to Pager Group 1, provided that the maximum group capacity of 35 devices has not been exceeded.

**PLEASE NOTE:** Alert Rules apply only to alarms raised by EkoTek and EkoSecure devices. Alarms raised by EkoCare Units are handled by the configured EkoCare Rules; see section 5.7.

Benutzergruppe	Zone	Zeit	Prio	Ereignis
1	1	1	1	1
2	2	2	2	2

Fig. 57 An example Alert Rules table as shown on the Alarmregeln page once configured

Alarms are routed to recipients according to the following parameters:

- The **Benutzergruppe** to which the device raising the alarm may be assigned
  - Devices that are capable of indicating an alarm can be assigned to a Benutzergruppe on the **Geräte** page; see section 5.3
- The **Zone** in which the alarm is raised
  - Zones are defined by the devices that are assigned to them
  - Static devices are assigned to a network Zone on the **Devices** page; see section 5.3
- The current system Shift (**Tag or Nacht**)
  - For more information, see section 6.1



- The escalation level of the alarm (**Priorität**)
  - Alarms that have been escalated (**Hoch**) did not receive a response from other system users when first raised and have been resent
  - Alarms that have been escalated can be handled in a different way to initial alarms (**Normal**)
- The alarm type (**Ereignis**) that has been raised
  - **Zeitalarm (Z)** – Triggered when no response is received to a Dead Man prompt (if configured)
  - **Lagealarm / Kontakteingabe (L)** – Triggered when a device is held outside the configured orientation for the designated trigger period or an input is received through the circuit contacts on an EkoTek or EkoSecure device (if configured)
  - **Druckalarm (D)** – Triggered when the red button on an EkoTek or EkoSecure device is pressed
  - **Wandern (W)** – Triggered when a portable device receives location data from a static device assigned to a network Zone to which it is not permitted access (if configured)
  - **Reißlein (R)** – Triggered when the Snatch Cord is removed from a Pager (if configured)
  - **Assistenzalarm (A)** – Triggered when the blue button on an EkoTek or EkoSecure device is pressed (if configured)
- The **Pagergruppe** to which alarms matching the chosen criteria are sent
- Whether or not external paging devices included in the recipient Pager Group should also receive the alert

Alarms must meet at least one condition within each parameter for the Alert Rule to be applied.

**EXAMPLE:** The following parameters are defined for an Alert Rule:

- **Benutzergruppe** – 1, 3, 4
- **Zone** – 1
- **Tagszeit** – Tag
- **Priorität** – Hoch, Normal
- **Ereignis** – Druckalarm, Reißleine, Assistenzalarm
- **Pagergruppe** – 2
- **Nur für EkoTek**
- **Notrufpager** – Enabled

**Tabelle Alarmregeln**

Regeln bearbeiten

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Benutzergruppe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Zone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Tageszeit	Tag		Nacht													
Priorität	Hoch		Normal													
Ereignis	Zeitalarm		<input type="checkbox"/> Z													
	Lagealarm / Kontakteingabe		<input type="checkbox"/> L													
	Druckalarm		<input checked="" type="checkbox"/> D													
	Wandern		<input type="checkbox"/> W													
	Reißleine		<input checked="" type="checkbox"/> R													
	Assistenzalarm		<input checked="" type="checkbox"/> A													
Pagergruppe	2															
Nur für EkoTek Pager	<input checked="" type="checkbox"/>															

Bestätigen

For this Alert Rule to apply, the alarm raised must have been raised by a device assigned to User Group 1 **OR** 3 **OR** 4, **AND** have been raised in network Zone 1, **AND** be raised during the Tag Shift, **AND** the alarm must be an Emergency alarm **OR** Snatch Cord alarm



**OR Assist Alarm.** If all of these statements apply to the alarm, it will be sent to all devices in Pager Group 2, excluding any external paging devices included in the Group.

Configured Alert Rules are displayed as rows on the Alert Rules table, with required conditions for each parameter marked with a ✓. The Pager Group to which alarms meeting the criteria for each Alert Rule is sent is indicated on the right of row. The Alert Rules table may contain up to 32 rules; if more than 16 rules are configured, the column headers are also shown at the bottom of the Alert Rules table.

Benutzergruppe																Zone																Zeit	Pri	Ereignis								
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	T	N	H	N	Z	L	D	W	R	A	
✓		✓	✓	✓												✓																✓	✓	✓			✓	✓	✓		2	

Fig. 58 Alert Rules are shown in the Alert Rules table according to the conditions selected; this rule presents the conditions selected in the Example

### 5.6.1 ADDING A NEW ALERT RULE

To configure a new Alert Rule:

- a) Click **NEU** beneath the Alert Rules table
- b) Use the checkboxes to select the acceptable conditions within each parameter to define which alarms will be processed by the rule:
  - i) **Benutzergruppe** – The User Group of the device raising the alarm
  - ii) **Zone** – The areas of the network or building from which the alarm is raised
  - iii) **Tagezeit** – The Shift during which the alarm is raised
  - iv) **Priorität** – Whether the alarm is being sent for the first time (**Normal**) or has been escalated (**Hoch**) due to lack of response from other devices
  - v) **Ereignis** – The type of alarm raised

Fig. 59 Adding a new Alert Rule

**PLEASE NOTE:** For each of the above parameters, at least one condition must be selected. Each of these parameters permits multiple selections; alarms must meet at least one selected condition for each parameter to be handled by the rule.

- c) Select the **Pager group** that will receive the alarm if handled by this rule
  - i) Only one Pager Group can be selected
  - ii) To send alarms meeting the same conditions to multiple Pager Groups, either:
    1. Duplicate the Alert Rule for each additional Pager Group to which the alarm should be sent
    2. Create a new Pager Group that contains all devices to which the alarm should be sent
- d) Use the checkbox to determine whether external paging devices will be excluded from the alarm notification (**EkoTek pagers only**)
  - i) If **EkoTek pagers only** is selected, the rule row will appear with a grey background in the Alert Map

**PLEASE NOTE:** In EkoSecure systems, only one Alert Rule may send a paging message to an external system when alarms are raised. If a second rule is created that potentially includes external devices, the rule cannot be saved until the conflict is resolved.

- e) Click **BESTÄTIGEN** above the Alert Map to apply

**PLEASE NOTE:** If **NEU** is clicked while editing an Alert Rule, any unsaved changes made will be lost.

New Alert Rules are added to the Alert Rules table once submitted.

## 5.6.2 EDITING AN EXISTING ALERT RULE

To edit an existing Alert Rule:

- a) Click the Pager Group recipient identifier on the right of the corresponding Alert Rule row of the table
- b) Edit the parameters as required
- c) Click **BESTÄTIGEN** above the Alert Rules table to apply

**PLEASE NOTE:** If **NEU** is clicked while editing an Alert Rule before any changes have been saved by clicking **BESTÄTIGEN**, changes made will be lost.

To remove an existing Alert Rule, click the Pager Group recipient identifier on the right of the corresponding row in the Alert Rules table and click **ENTFERNEN** when the **Regeln Bearbeiten** screen is shown.

## 5.7 EkoCare Regeln

EkoCare Rules are used to determine which alarms are sent to which devices when raised, allowing specific devices to be targeted when certain conditions are met. This avoids every alarm being sent to every device where this is not desirable. Alarms raised by EkoCare Units are handled exclusively by the EkoCare Rules settings.

To view and manage EkoCare Rules, navigate to **Konfiguration > EkoCare Regeln**.

Fig. 60 Adding a new EkoCare Rule and the EkoCare Rule Map

The alarm types handled by EkoCare Rules differ from standard system Alert Rules and include the following **Ereignisse**:

- **KontaktFehler (F)** – Triggered when a Bed Call button is removed from an EkoCare Wall Unit
- **Externer Kontakt (K)** – Triggered when an input is received through the circuit contacts of an EkoCare device (if configured)
- **Bewohner (B)** – Triggered when the Patient Call button is pressed on EkoCare Units, or the alarm button is pressed on an EkoTek Call Point or EkoTek Fob configured for Patient Call Operation (see section 5.4.25)
- **Notfall (N)** - Triggered when the **RED** button is pressed on an EkoCare Wall Unit under the correct conditions (see section 5.4.20)
- **Assistenz (A)** – Triggered when the **BLUE** button is pressed on an EkoCare Wall Unit if Anwesenheit mode is not active (see section 5.4.24)

EkoCare Rules are configured in the same way as Alert Rules; see section 5.6 or more information.

## 5.8 Zurücksetzen

In the event that the Hub must be restored to its default factory settings, this can be

achieved on the Zurücksetzen page. To access the page, navigate to **Konfiguration > Zurücksetzen**.

Performing a Factory Reset returns the Hub and the system network configuration to their default settings. This includes the following changes:

- All devices are removed from the system
- All Device Modes are reset to default settings
- All Alert Rules and EkoCare Rules are removed
- All custom IP addresses are reconfigured with default values
- User passwords are reset to default values

To perform a Factory Reset, click **ZURÜCKSETZEN** on the Zurücksetzen page.



Fig. 61 The Zurücksetzen page

**PLEASE NOTE:** Always take a system back-up before performing a Factory Reset. If a reset is performed in error, a back-up can be restored; see section 5.11 for more information.

## 5.9 Alles Löschen

In the event that all system devices, including external connections, must be removed from the system but the network configuration must remain intact, this can be achieved on the **Alles Löschen** page. To access the page, navigate to **Konfiguration > Alles Löschen**.

To delete all registered devices from the system, click **DATENBANK LÖSCHEN**. Network configurations including Device Modes, Alert Rules, custom IP addresses, and user passwords are not affected.

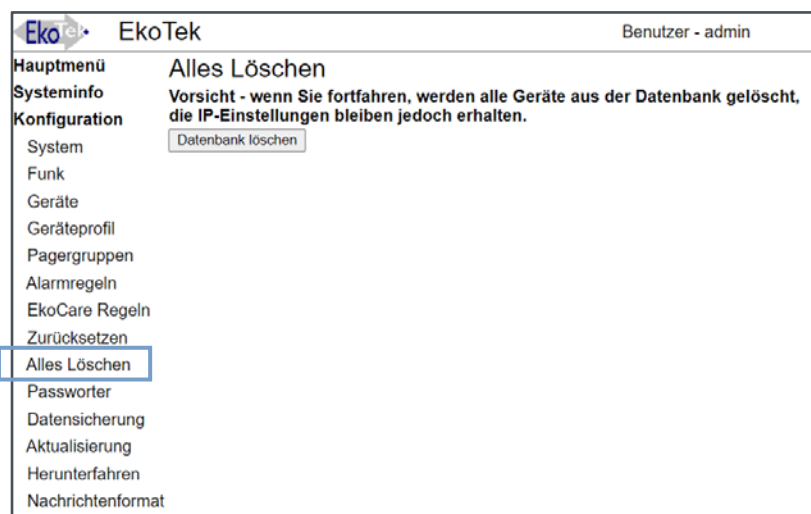


Fig. 62 The Alles Löschen devices page

**PLEASE NOTE:** Always take a system back-up before removing all system devices. If devices are removed in error, a back-up can be restored; see section 5.11.2 for more information.

## 5.10 Passwörter

The EkoSecure Hub permits access to the web interface via two user accounts. The default credentials for these accounts are as follows:

- Administrator access:
  - **Benutzer** – admin
  - **Passwort** – [Leave blank]
- Operator access:
  - **Benutzer** – benutzer
  - **Passwort** – [Leave blank]

**PLEASE NOTE:** Both the Benutzer and Passwort fields are case-sensitive.

Accounts cannot be added or removed from the system.

To prevent unauthorised access to the system configuration, it is highly recommended that secure passwords be configured to each account once the system is installed. To manage the account passwords, navigate to **Konfiguration > Passwörter**.

This page is also accessible by users logged in to the web interface with the username **benutzer**; however, in this instance, the **admin** account password cannot be changed.

The screenshot shows the EkoTek web interface. On the left, a sidebar menu lists various system functions. The 'Passwörter' (Passwords) option is highlighted with a blue box. The main content area is titled 'Passwort-Verwaltung'. It features a 'Benutzer' (User) dropdown menu currently set to 'admin'. Below this is a 'Neues Passwort' (New Password) input field, which is masked with dots. A 'Bestätigen' (Confirm) button is located below the password field.

Fig. 63 The Passwörter management page

### 5.10.1 EDITING THE ACCOUNT PASSWORDS

To edit the password of one of the system web interface accounts:

- a) Select the required account from the **Benutzer** drop-down menu
- b) Enter a new password into the **Neues password** field
  - i) Passwords must be 4 and 8 characters in length
- c) Click **BESTÄTIGEN** to apply
  - i) **[Benutzer / Admin] password changed** is shown on-screen when the change has been successfully applied

### 5.10.2 ACCESS BASED ON USER ACCOUNT

The account with which the user is logged in determines the system functionality available through the interface.

The Administrator account (**admin**) has full access to the system functions and configuration available through the web interface menu.

The Operator account (**benutzer**) may only access the following functions:

- Under **Hauptmenu**:
  - All menu items
- Under the **Systeminfo** menu:
  - **Gerätestatus**
  - **Netzwerk-Baum**
- Under the **Konfiguration** menu:
  - **System**
  - **Passwort** (only the **benutzer** account can be edited)

Functions and pages to which access is not permitted will fail to load in the browser.

## 5.11 Datensicherung

Back-ups of the system configuration and device registry can be taken through the **Datensicherung** page. Existing back-ups can also be restored through this page. To access the Datensicherung page, navigate to **Konfiguration > Datensicherung**.

The device registry available for download from this page is intended for use as an import into a new or restored EkoFamily system. For a more digestible breakdown of devices registered to the system, type the **IP address** of the Hub into the URL field of a web browser, followed by **/devices.php**.

**EXAMPLE:** To do this for a Hub that is configured with the default IP address, navigate to **192.168.1.2/devices.php** in a web browser.

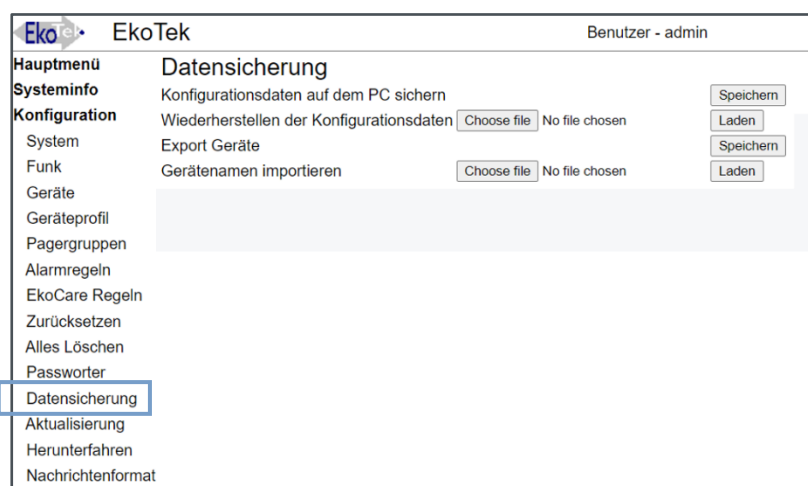


Fig. 64 The Datensicherung configuration page

This triggers a download of a Text Delimited register of the devices registered to the Hub, which may be imported into a spreadsheet for convenient viewing. This file cannot be imported back into an EkoFamily system.

**PLEASE NOTE:** It is recommended to create an archive of the current configuration before any significant change to the system is made. **ALWAYS** create an archive before upgrading or replacing the system Hub.

### 5.11.1 CREATING AN ARCHIVE

To download the current system configuration or device registry:

- Click **DOWNLOAD** in the appropriate row
- If prompted, in the new window, locate and select a suitable location to store the download and click **DOWNLOAD**

**PLEASE NOTE:** The system configuration also includes the device registry. To download

the device registry without the full system configuration, click **DOWNLOAD** beside the **Export devices** option.

### 5.11.2 RESTORING AN ARCHIVE INTO THE SYSTEM

To upload an existing archive of the system configuration or device registry:

- a) Click **CHOOSE FILE** in the appropriate row
- b) In the new window, locate and open the required archive to upload
  - i) Ensure that the contents of the file correspond to the upload option selected (i.e., full archive or device names)
- c) The selected file is listed beside the **CHOOSE FILE** button
- d) Click **UPLOAD** to begin restoring the archive
  - i) This may take several minutes
- e) If the archive is uploaded successfully, a **RESET** button is added to the page
- f) Click **RESET** to apply the archive data
  - i) The archive will not be applied until a Hub reset has taken place
  - ii) The reset process may take a few minutes and is indicated on the system Hub LCD display by a flashing ! in the timestamp
    1. When the timestamp returns to its normal format with a : separator, the process has completed

**CAUTION: DO NOT** navigate away from the **Archive** page in the web browser as this may interrupt the reset process irreversibly. During the reset process, carefully monitor the Hub LCD display until the timestamp returns to its normal format with a : separator, indicating that the process has completed.

Once the reset process has completed, the Hub can be reached at its new IP address, if changed as part of the archive data, or, if it was not changed, by refreshing the page.

**PLEASE NOTE:** When replacing an older Hub model with this device, create an archive of the system configuration and device registry using the original Hub and import the data into the new Hub once installed.

## 5.12 Aktualisierung

Where required, software upgrades for system devices that can receive upgrades *over-the-air* can be applied via the Hub's **Upgrade** page.

**PLEASE NOTE:** The Hub itself cannot be upgraded through this page. For guidance on upgrading the Hub, see section 9.

To access the Upgrade page, navigate to **Configuration > Upgrade**.



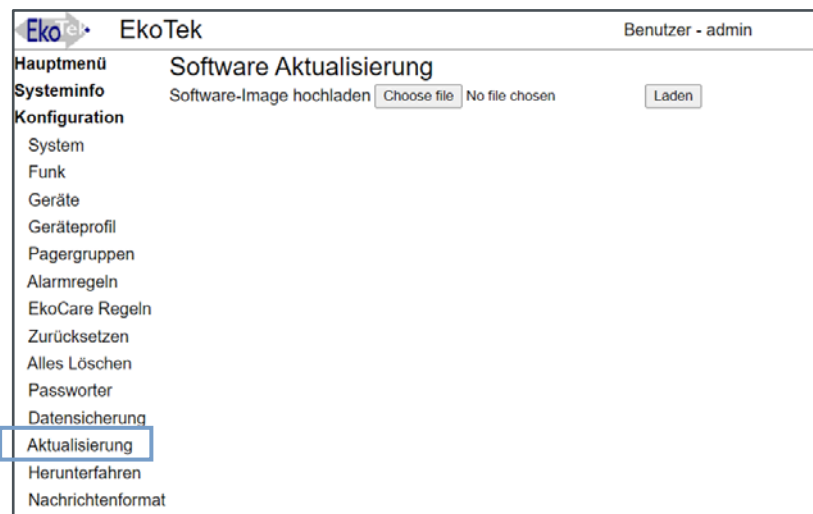


Fig. 65 The Aktualisierung configuration page

**PLEASE NOTE:** Upgrades should be performed only when instructed by Multitone or when new system devices have been purchased. Upgrade files are provided by Multitone upon request.

To upload a device software upgrade package to the Hub for distribution across the system:

- a) Create an archive of the current system configuration and device registry
  - i) See section 5.11
- b) Return to the **Aktualisierung** page of the interface
- c) Click **CHOOSE FILE**
- d) In the new window, locate and open the required software upgrade file
- e) The file is listed beside the **CHOOSE FILE** button
  - i) Only one file can be selected at a time
- f) Click **LADEN** to upload the upgrade file
- g) If the file is uploaded successfully, the device variant to which it applies and the firmware version number are shown
  - i) Up to 10 upgrade files can be processed simultaneously
  - ii) To clear the list of loaded upgrade files, click **LÖSCHEN**
- h) To apply the firmware upgrade to applicable connected devices in the system, click **LOS**
  - i) An **Upgrade Läuft** message is displayed to indicate that the upgrade is in process

**CAUTION: DO NOT** navigate away from the **Aktualisierung** page in the web browser as this may interrupt the upgrade process.

## 5.13 Herunterfahren

In the event that power must be manually removed from the system Hub, the system must be switched off safely using a controlled power-down procedure managed by the Hub. This is performed automatically when the on-board batteries approach the end of their charge capacity, but can also be manually triggered remotely from within the web interface.

This process can be initiated from the Power Down page, which can be accessed by navigating to **Konfiguration > Herunterfahren**.

From this page, the Hub can be switched off until power is manually restored (**Herunterfahren**), or temporarily powered down for 60 seconds and automatically rebooted (**Zurücksetzen**) in the event that a forced restart is required.

**PLEASE NOTE:** Performing a reset from this page reboots the device with the current settings. To perform a factory reset or remove registered devices from the system, see sections 5.8 and 5.9.

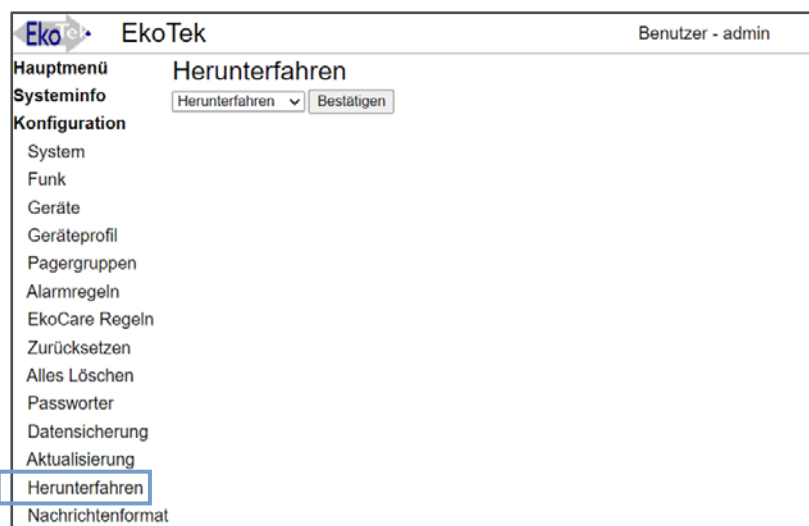



Fig. 66 The Herunterfahren page

To power down or reset the device, select the appropriate option from the drop-down menu and click **BESTÄTIGEN**.

**CAUTION: DO NOT** disconnect the power supply or batteries in the device while the power down or reset process is taking place as this may interrupt the controlled power down procedure. Once the Hub LCD display is no longer illuminated, it is safe to remove any power supplies if required. The EkoTek logo  will remain illuminated to indicate an active external power supply. Removing and restoring the external power will restart the device.

## 5.14 Nachrichtenformat

The order in which alarm information is presented on the system Hub and Pager LCD screens can be customised. This may be used to allow the most appropriate information to be visible in the message preview and to prioritise message content in the message details screen.

**PLEASE NOTE:** Changes made to the message format are universal and cannot be defined for specific devices or conditions. Customisation of message formatting **DOES NOT** affect the content recorded in the Event and Pager Logs, nor does it affect the message content as stored in the database.

Customisation can be achieved on the **Konfiguration > Nachrichtenformat** page.

By default, messages are presented in the following order:

- **Ereignis** – The type of alarm raised
- **Auslösendes Gerät** – The device from which the alarm was raised
- **Lokalisierung** – The source of the Location Beacon from which the raising device most recently received Location data
  - This applies only to portable devices

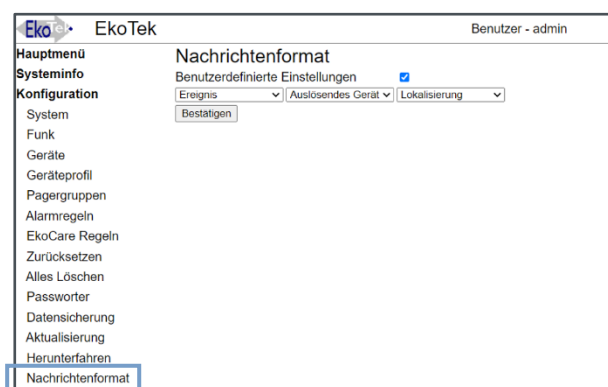


Fig. 67 The Nachrichtenformat page

To customise the message ordering:

- a) Ensure that the **Benutzerdefinierte Einstellungen** setting is enabled by checking the box
- b) Use the three drop-down lists to select the order in which message data will appear
  - i) A value must be configured for each drop-down list
- c) Each drop-down list must be configured with a unique value
- d) Click **BESTÄTIGEN** to apply any changes

To remove any customisation and return to the default message format, uncheck the **Benutzerdefinierte Einstellungen** option and click **BESTÄTIGEN** to apply.

## 6 Hauptmenu

The following operational and management tasks can be performed from the Hub web interface via the **Hauptmenu** options on the left of the web interface screen. These functions are available to both **benutzer** and **admin** system accounts.

### 6.1 Tag / Nacht – Setting the current Shift

The EkoSecure Hub can accommodate differing alarm handling procedures for daytime and night-time hours. The periods for which these two configurations are assigned are labelled **Shifts**. The time at which the system switches between Shifts, and the way that this is achieved, is managed from the **Shift** page. By default, the system Shift is set to **Tag** until manually changed.

Tag	
Montag	06 : 00 - 20 : 59
Dienstag	06 : 00 - 20 : 59
Mittwoch	06 : 00 - 20 : 59
Donnerstag	06 : 00 - 20 : 59
Freitag	06 : 00 - 20 : 59
Samstag	08 : 00 - 21 : 59
Sonntag	08 : 00 - 21 : 59

Fig. 68 The system Shift management page with a Shift schedule applied

To access the Shift page, navigate to **Hauptmenu > Tag / Nacht**.

For more information on Rules for alarm handling, see sections 5.6 and 5.7.

#### 6.1.1 MANUELLE AUSWAHL

To manage the current shift manually:

- Enable **Manuelle Auswahl** by clicking the appropriate radio button
- Select the required Shift from the drop-down list
- Click **BESTÄTIGEN** to apply

When in **Manuelle Auswahl** mode, the system Shift can be changed using the following methods:

- Selecting the current Shift from the **Manuelle Auswahl** region of the **Tag/Nacht** page and clicking **BESTÄTIGEN**
- Altering the current Shift through the Hub display interface using the buttons on the front panel of the device; see section 6.1

**PLEASE NOTE:** When in **Manuelle Auswahl** mode, the Hub will continue to apply any Rules associated with the current Shift until the Shift is manually changed.

### 6.1.2 AUTOMATICSH

The Hub can be configured to automatically switch Shifts at specified times of the day according to a schedule. Each day of the week is configured separately.

To create a Shift schedule:

- a) Enable **Automaticsh** by clicking the appropriate radio button
- b) Use the drop-down menus to configure the time included in the 'Tag Shift' for each day of the week
  - i) Any time outside of the configured periods is automatically defined as the 'Nacht Shift'
- c) Click **BESTÄTIGEN** to apply

### 6.1.3 EXTERN

The current shift can be determined via the contact terminals on the Hub's Relay Board interface if the schedule is managed by devices outside the EkoSecure system. The current Shift is assigned as follows:

- **Closed contacts** – The current Shift is set to **Nacht**
- **Open contacts** – The current Shift is set to **Tag**

When configured in this way, the current Shift cannot be overridden using the buttons on the front panel of the Hub.

To configure Shift assignment via the external contacts once the connected:

- a) Enable **Extern** by clicking the appropriate radio button
- b) Use the drop-down list to select the device through which the Shift change input is received
  - i) Only Hub, IP Client Hub, and Ethernet Repeater devices can assign the current Shift to the EkoSecure system
- c) Click **BESTÄTIGEN** to apply

Connections via the Relay Board contact terminals should be made by the system engineer.

## 6.2 Ereignisprotokoll

The Event Log records all alarm and message activity that occurs within the system. To view the Event Log, navigate to **Hauptmenu > Ereignisprotokoll**.

Datum	Ereignis	Primär	Primärer Name	Secundäre	Secundärer Name	Benutzer	Zone
2021-02-07 10:42	MT Repeater - Stairwell maintenance required	032-1803352	Repeater - Stairwell			1	1
2021-02-07 10:47	PS Pager 49362 - Security I Emergency	020-0049362	Pager 49362 - Security I	032-1813006	Repeater - Security Office	4	4
2021-02-07 10:49	LO Repeater - Cardiac WR	032-1802501	Repeater - Cardiac WR			2	2

Fig. 69 The Ereignisprotokoll page

Each record contains a combination of the following information, subject to the event type. Some fields can be hidden if preferred.

- **Datum** – The system timestamp at which the event occurred
- **Ereignis Code** – An event class identifier
- **Ereignis Detail** – The event type and text content of the event message
- **Primär (Gerät)** – The serial number of the device that created the message
- **Name (Primärer)** – The assigned name of the device that created the message
- **Secundäre** – Variable according to the context of the message:
  - When an alarm or message is created by a portable device, this field contains the serial number of the static device associated with the Location data currently held by the Primärer Device
    - This is the source of the Location Beacon that was most recently detected by the Primärer Device
  - When an alarm is accepted by another device, this field contains the serial number of the device that accepted the alarm
  - When an alarm or message is created by a static device, there is initially no Secundäre Device information as the Primärer Device information already identifies the Location
    - When an alarm raised by a static device is accepted, the serial number of the device that accepted the alarm is listed
- **Secundäre Name** – The assigned name associated with the serial number identified in the **Secundäre** field
- **Benutzer (Benutzergruppe)** – The User Group to which the Primärer Device was assigned
  - Devices can be grouped according to characteristics of the personnel that will carry them (e.g., role, shift pattern, etc.); see section 5.3

- **Zone (Benutzer Zone)** – The Zone number assigned to the static device associated with the Location data held by the Primärer Device when the alarm or message was raised
- If the message is raised by a static device, the Zone of that device is shown

The following event types may be recorded within each event class:

- **Personal Security (PS)**
  - Alarm raised
  - Alarm accepted
  - Alarm cleared
- **Maintenance (MT)**
  - Device status not reported
  - Low battery warning
  - These messages are also sent to Pager Group 1
- **Paging (PG)**
  - Pager message sent
  - Delivery report (if requested when sent)
  - User response (if requested when sent)
- **Schwesternruf (NC)**
  - Alarm raised
  - Alarm accepted
  - Alarm cleared
- **Log (LO)**
  - Manual entries entered through the Hub web interface; see section 6.2.2

Up to 10,000 records can be stored in the Event Log. When the maximum storage is reached, the oldest records are overwritten by new events and removed.

### 6.2.1 THE EVENT LOG TABLE

Entries in the Event Log can be viewed in the table at the bottom of the page by running a data query using the **To** and **From** parameters at the top of the screen. When the **Ereignisprotokoll** page is loaded, the table lists all event records since midnight on the current day.

To populate the table with event records from a different time period:

- a) Click in the **Von** field and use the calendar to select the first date from which data is required
- b) Click in the **an** field and use the calendar to select the last date from which data is required
- c) Click **AKTUALISIEREN** to run the query and repopulate the table
  - i) The **AKTUALISIEREN** button is only available when the **Von** and **an** parameters have been changed

Records listed in the table can be searched and filtered using the **Filter** text field. Any record with a matching string in any field will be displayed. The table can also be sorted by clicking the header of the appropriate field. The direction of the sort is indicated by an arrow icon beside the column header.

The visibility of optional table columns can be toggled using the checkboxes above the table. The **Datum** and **Ereignis** fields cannot be hidden.

### 6.2.2 ADDING RECORDS

Records can be manually added to the Event Log. This may be used to leave prompts for engineers when investigating the system or to note any actions taken that may affect the configuration or operation of the wider system.

To create a new record, click **LOG HINZUFÜGEN** and enter the required message into the text field when shown. Click **BESTÄTIGEN** to record the new entry.

Records that have been created manually are logged as **LO** in the Event Log table.

### 6.2.3 EXPORTING THE EVENT LOG DATA

If required, data from the Event Log can be exported as a Text Delimited .txt file for review. Only the records listed in the table are exported; however, all fields are included in the export, regardless of their visibility in the browser interface.

To export records from the Event Log:

- a) Use the **Von** and **an** parameters to set the period for which the data history will be exported
- b) Click **AKTUALISIEREN** to update the Event Log table
- c) Click **SPEICHERN** to prompt a download of the file
  - i) The **SPEICHERN** button is only available once changes to the **Von** and **an** parameters have been applied

## 6.3 Nachricht senden

The Hub's browser interface can be used to create and send paging messages to Paging Devices within the system. Messages can be sent to individual devices, Pager Groups, or to all pagers registered on the system as required.

To send a paging message directly from the Hub:

- a) Navigate to **Hauptmenu > Nachricht senden**
- b) Enter the message into the text field
- c) Select the required recipients:



- i) To message all Paging Device within the systems, select **An alle Notrufpager**
- ii) To message all Paging Devices within a Pager Group:
  1. Select **Gruppe Notrufpager**
  2. Select the required Pager Group from the drop-down list
    - A. For guidance in configuring Paging Groups, see section 5.5
  3. If a response from the recipient is required, enable **Rufquittierung anfordern** in the **Gruppe Notrufpager** region
- iii) To message a specific Paging Device:
  1. Select **Notrufpager**
  2. Select the required Pager from the drop-down list
    - A. For guidance on registering and managing Paging Devices, see section 5.3
  3. If a response from the recipient is required, enable **Rufquittierung anfordern** in the **Notrufpager** region
  4. To record the successful delivery of the message in the Pager Log, enable **Protokoll Nachrichtenübermittlung**
- d) Click **BESTÄTIGEN** to send

Messages sent from the Hub are displayed and managed on Paging Devices in the same way as alarms and other system messages.

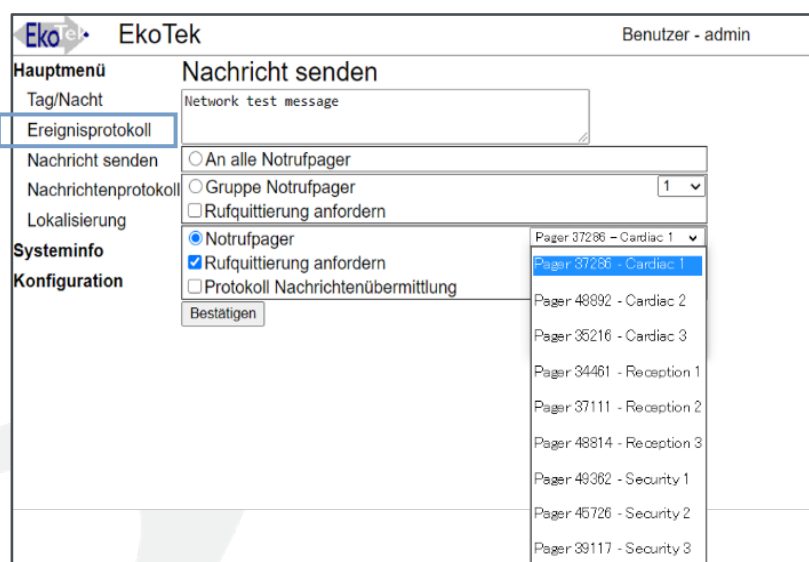


Fig. 70 Locating the Nachricht senden function within the browser interface, with an individual Pager selected

## 6.4 Nachrichtenprotokoll

Messages sent to Paging devices from the Hub are stored in the Pager Log. To view the Pager Log, navigate to **Hauptmenu > Nachrichtenprotokoll**.

Hauptmenü		Nachrichtenprotokoll		
Tag/Nacht	Nachricht	Übermittlung	Antwort	
Ereignisprotokoll	Vorläufiger Netzwerktest	Offen		<a href="#">Details</a>
Nachricht senden	Testen der Pagergruppe 1	Vollständig	Offen	<a href="#">Details</a>

Systeminfo  
Konfiguration

Fig. 71 Locating the Nachrichtenprotokoll within the browser interface

The Pager Log stores the 15 most recent Pager messages sent by the Hub where the **Rufquittierung anfordern** or **Protokoll Nachrichtenübermittlung** options were enabled. When the storage limit is reached, new stored messages overwrite the oldest message in the Log.

All Pager messages, including those stored in the Pager Log, are recorded in the Event Log.

#### 6.4.1 THE NACHRICHTENPROTOKOLL TABLE

The following information is displayed in the Pager Log:

- **Nachricht** – The text content of the message
- **Übermittlung** – Indicates whether the message has been successfully delivered to all recipients:
  - **Offen** – The message has not been delivered to any intended recipients
  - **Teilweise** – The message has been delivered to some of the intended recipients
  - **Vollständig** – The message has been successfully delivered to all intended recipients
    - If the **Rufquittierung anfordern** option was not checked when the message was sent (see section 6.3), this will automatically be listed as **Vollständig**
- **Antwort** – The status of the response from the recipient device (if requested when sent)
  - **Offen** – No response has been received from the recipient device
  - **Empfangen** – The recipient device has sent a response to the message

To view a message in more detail, click **DETAILS** in the appropriate row. The Details page indicates which devices have received and responded to the message if requested when sent. No data can be changed on this page.

Both the Pager Log table and the Details page are updated upon page load. To update either page, click **AKTUALISIEREN**.

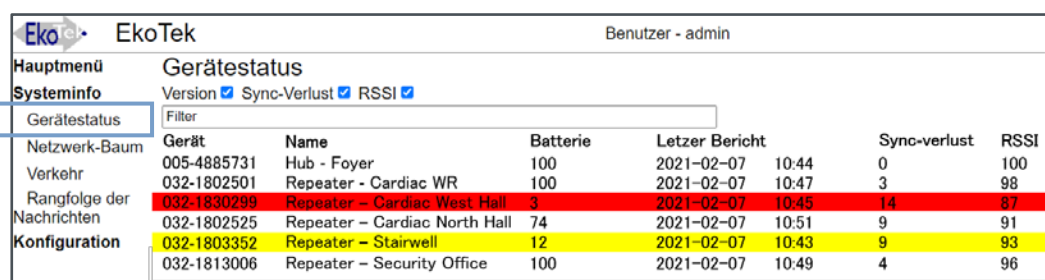
## 7 Systeminfo menu

Management of the EkoSecure network mesh and system devices can be achieved through the browser interface using the **Systeminfo** menu on the left of the screen. Maintenance Message prioritisation can also be managed on these pages.

The following pages are available through the Systeminfo menu and are only accessible by users logged in to the web portal with the username **admin**, unless otherwise stated.

### 7.1 Gerätestatus

All system devices deliver a Device Status Report to the Hub approximately every 10 minutes. To view the latest Device Status Reports, navigate to **Systeminfo > Gerätestatus**. This page can also be viewed by users logged in with the username **benutzer**.



Gerät	Name	Batterie	Letzter Bericht	Sync-verlust	RSSI
005-4885731	Hub - Foyer	100	2021-02-07 10:44	0	100
032-1802501	Repeater - Cardiac WR	100	2021-02-07 10:47	3	98
032-1830299	Repeater - Cardiac West Hall	3	2021-02-07 10:45	14	87
032-1802525	Repeater - Cardiac North Hall	74	2021-02-07 10:51	9	91
032-1803352	Repeater - Stairwell	12	2021-02-07 10:43	9	93
032-1813006	Repeater - Security Office	100	2021-02-07 10:49	4	96

Fig. 72 The Gerätestatus page

Device Status Reports contain the following information:

- **Gerät** – The serial number of the listed device
- **Name** – The user-friendly name assigned to the listed device
- **Batterie** – The current percentage charge of the listed device's on-board batteries, if present
  - Mains-powered devices with a battery failover will display a value of **100** unless the mains supply has been disconnected
- **Letzter Bericht** – The timestamp of the latest report received from the listed device
  - Data updates can be requested for each device from the Device **Details** page
- **Version** – The software version currently installed on that device
- **Sync-verlust** – The number of times the device has lost connection with its Parent device
- **RSSI [Optional]** – A numerical indicator of the strength of the received radio signal from the Parent device
  - A value of **100** indicates maximal signal strength
  - A value of **1** indicates minimal signal strength

Warnings are displayed in the table as highlighted rows:

- **Yellow** – Indicates a battery charge of **5-20%**, or that the latest Device Status Report was not received from the listed device when requested
- **Red** – Indicates a battery charge of **>5%**, or that 4 consecutive requested Device Status Reports have not been received from the listed device

Devices in the Status Report table can be searched and filtered using the **Filter** text field. Any record with a matching string in the **Gerät** or **Name** fields will be displayed. The table can also be sorted by clicking the header of the appropriate field. The direction of the sort is indicated by an arrow icon beside the column header.

The visibility of optional columns of the table can be toggled as required using the checkboxes above the table itself.

Further detail relating to each specific device is available on the Device Details page.

### 7.1.1 DEVICE DETAILS PAGE

Additional information relating to each device can be accessed by selecting the appropriate row and clicking the **DETAILS** button that appears on the right of the screen.


 EkoTek		Benutzer - admin	
Hauptmenü	Gerätestatus		
Systeminfo	005-4885731		
Gerätestatus	Name	Hub - Foyer	
Netzwerk-Baum	Hardware/Software	005-140	
Verkehr	Letzter Bericht	2021-02-07	10:44
Rangfolge der Nachrichten	Batteriestand	100%	
Konfiguration	Beacon-Verlustzähler	0	
	Synchronisationsverluste mit Bezugsgerät	0	
	<input type="button" value="Aktualisieren"/>	<input type="button" value="Löschen"/>	

Fig. 73 The Gerätestatus Details page relating to a Hub device

The following information is available on the Device Details page, subject to the type of device selected:

- **[Device Type]** – The Device Type and serial number of the device
- **Name** – The user-friendly device name assigned to the device
- **Hardware / software** – The revision number of the hardware device and its installed software
  - If no report has been received, this is shown as **\*\*\*-\*\*\***
- **Letzter Bericht** – The timestamp of the latest Device Status Report received from the device
  - If no report has been received, this is shown as **Statusbericht**
- **Batteriestand** – The current percentage charge of the device's on-board batteries, if present
  - Mains-powered devices with a battery failover will display a value

- of **100** unless the mains supply has been disconnected
  - Devices to which mains power has been restored after a period of reliance on battery power will display **Wird geladen**
  - If no report has been received, **Unbekannt** is displayed
- **Upstream-Anbindung** – The serial number and user-friendly name of the device's parent connection
  - Where a cabled connection has been established between the device and the system Hub, **Direktverbindung** is shown
  - This is only available for static devices
- **Beacon-Verlustzähler** – The number of times that the device has lost connection with its Parent device
  - This may occur due to a problem with the Parent device, or the degradation of the signal between the device and its Parent
  - In the event that connection is lost, the device will automatically search for a new viable Parent device until a new connection can be established
  - The Device Details page of the Hub displays the total Beacon Loss Count across the whole mesh since start-up or the count was reset
- **Synchronisationsverluste mit Bezugsgerät** – The number of times that the broadcast synchronisation between the device and its Parent has been lost
  - This is automatically rectified by the system
  - The Device Details page of the Hub displays the total Parent Sync Loss count across the whole mesh since start-up or the count was reset
- **Funksignalqualität** – A numerical indicator of the overall signal quality from the device through the mesh back to the Hub
  - A value of **100** indicates optimal signal quality
  - A value of **1** indicates poor signal quality
- **Funksignalstärke** - A numerical indicator of the overall signal strength from the device through the mesh back to the Hub
  - A value of **100** indicates maximal signal strength
  - A value of **1** indicates minimal signal strength
- **Funkverkehr** – The number of data packages sent from the device to its Parent

**PLEASE NOTE:** Some information may not be applicable for all Device Types.

Click **AKTUALISIEREN** to retrieve the current Device Status Report from the current device.

Click **LÖSCHEN** to reset the **Beacon-Verlustzähler**, **Synchronisationsverluste mit Bezugsgerät** counter, and **Funverkehr** values to 0.

To close the Device Details page and return to the list of devices without making changes, click **GERÄTESTATUS** in the menu on the left of the screen.

## 7.2 Netzwerk-Baum

The **Netzwerk-Baum** displays a schematic map of the network mesh and the connections between static devices as they route back to the Hub.

The top row of the Network Tree consists of two timestamps: the time at which the tree was last mapped (listed first), and the time at which the configuration request count values were last reset (enclosed in **< >** brackets).

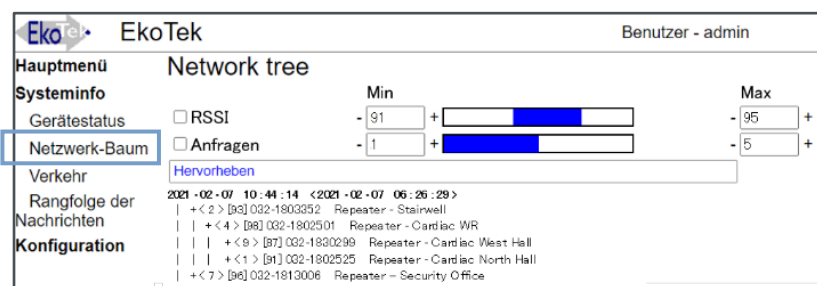


Fig. 74 The Netzwerk-Baum

The Hub itself is listed first, followed by the subsidiary devices that define each branch of the network. The following information is listed for each device:

- **< n >** - The number of times the device has requested its configuration from the Hub
- **[ n ]** – A numerical indicator of the strength of the received radio signal from the Parent device
- The device serial number
- The user-friendly name assigned to the device

The Upstream and Downstream connections of each device are also listed, with **+** symbols identifying the point at which a device intersects a branch of the network.

To identify the Parent (Upstream connection) of a specific device, locate the **+** symbol beside the device information and follow the network branch ( **|** symbols ) directly upwards until the configuration request count ( **< n >** ) of another device is reached. All messages sent Upstream from the original device in question are currently carried via this device.

To identify the Child devices (Downstream connections) of a specific device, follow the network branch ( **|** symbols ) directly downwards from the device configuration request count ( **< n >** ). Any devices for which the **+** symbol intersects this line are the immediate Child devices of the device at the starting point.

The number of network 'hops' (transmissions between devices) between a static device and the Hub can be quickly identified by counting the number of | symbols that precede the device information in the Network Tree.

When initially connected, new devices should automatically determine the most appropriate connection path back to the Hub. However, it may be appropriate to force connection between specific devices by locking the Upstream and Downstream broadcasts of those devices to specific radio channels; see sections 5.4.12 and 5.4.26.

### 7.2.1 SEARCHING THE NETWORK TREE

To ease the location and assessment of performance of devices within the system network, the devices in the Network Tree can be highlighted based on their listed RSSI and configuration request count values. A free text search can also be run on serial numbers and device names.

To search the Network Tree based on performance values:

- a) Use the checkboxes to select which parameters are required for the search
  - i) **RSSI** corresponds to the [ *n* ] value listed beside each network device
  - ii) **Anfragen** corresponds to the < *n* > value listed beside each network device
  - iii) Both parameters may be selected if required
    1. If both search parameters are enabled, only one condition must be met for inclusion in the results
- b) Use the **Min** and **Max** fields to set the minimum and maximum value of the appropriate parameter to be included in the search
  - i) Values can be typed manually into the fields or the - / + symbols used to reach the correct figure
  - ii) The coloured bar represents the position of the selected values against the total range of values available in the current Network Tree data
- c) Click outside of the text fields to implement the most recent change
- d) Where a device matches any of the stipulated conditions, the relevant information in the Network Tree entry is highlighted in blue

**Network tree**

☒ RSSI      Min: 91      Max: 95

☒ Anfragen      Min: 1      Max: 7

Hervorheben

2021 - 02 - 07 10:44:14 < 2021 - 02 - 07 06:26:29 >

- | + < 2 > [93] 032-1803352 Repeater - Stairwell
- | | + < 4 > [98] 032-1802501 Repeater - Cardiac WR
- | | | + < 9 > [87] 032-1830299 Repeater - Cardiac West Hall
- | | | + < 1 > [91] 032-1802525 Repeater - Cardiac North Hall
- | + < 7 > [96] 032-1813006 Repeater - Security Office

**Fig. 75** Using the checkboxes and Min/Max values to identify devices based on their network communication – only one condition must be met to be highlighted



To search the device list by name or serial number, enter the required string into the **Highlight** text field. Matching devices are shown with blue text.

Both types of search may be active at the same time.

To reset the configuration request count for each device in the Network Tree, click **IN-ZÄHLER ZURÜCKSETZEN**.

The screenshot shows the 'Network tree' interface. At the top, there are two checkboxes: 'RSSI' and 'Anfragen'. Below each checkbox are 'Min' and 'Max' value fields. For 'RSSI', the 'Min' field contains '91' and the 'Max' field contains '95'. For 'Anfragen', the 'Min' field contains '1' and the 'Max' field contains '5'. Below these fields is a search bar containing the text 'cardiac'. Under the search bar, a list of devices is displayed, each preceded by a plus sign and a number in brackets. The devices are: '032-1803352 Repeater - Stairwell', '032-1802501 Repeater - Cardiac WR', '032-1830299 Repeater - Cardiac West Hall', '032-1802525 Repeater - Cardiac North Hall', and '032-1813006 Repeater - Security Office'. The device names are highlighted in blue.

Fig. 76 Using the Hervorheben field to identify devices in the Netzwerk-Baum

## 7.3 Verkehr

The Funkverkehr Graph displays the changing volume of radio data packages sent within the EkoSecure System over time and may be used to identify periods of high traffic during which reduced performance may be experienced. Typically, high volumes of traffic are caused by the mesh reconfiguring itself to accommodate signal interference from external devices.

In instances of cyclical periods of increased traffic, the graph may be used to assist in both identifying the cause of interference and predicting the length of time until normal service is restored.

The graph can also be used in conjunction with the Network Tree to identify any potential maintenance issues with devices installed as part of the EkoSecure network. Increased traffic may be indicative of a device struggling to retain connection to a Parent; see section 7.2 for more information.

The default data on the graph displays the combined volume of radio traffic to and from the Hub, but can be broken down using the checkboxes at the top of the page:

- **RX** – The quantity of data packages sent upstream across the EkoSecure network
- **TX** – The quantity of data packages sent downstream across the EkoSecure network

To view the Traffic graph, navigate to **Systeminfo > Funkverkehr**.



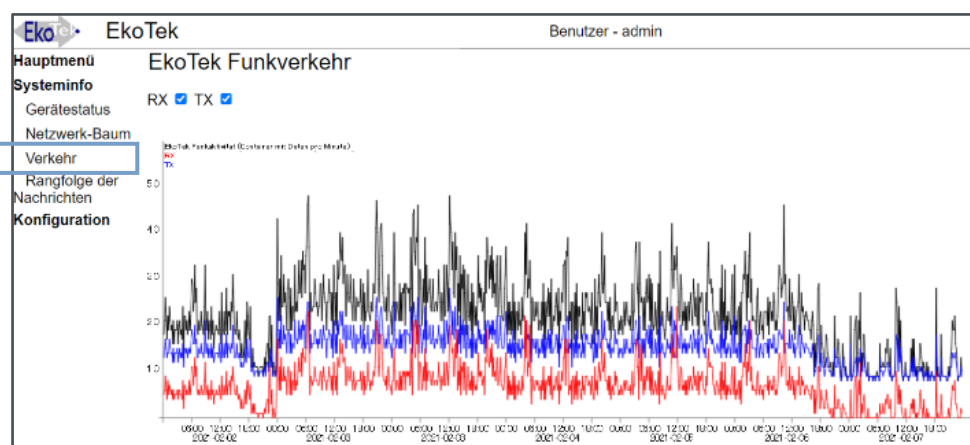


Fig. 77 The network Funverkehr chart, showing both RX and TX values, and the combined total

## 7.4 Rangfolge der Nachrichten

Maintenance Messages generated by devices within the EkoSecure system can be classified as either **Stufe 1** or **Stufe 2**. This allows specific groups of Maintenance Messages to be configured to trigger signal outputs via Relays 2 and 3 of the Hub's interface according to their assigned Stufe. Maintenance Messages that are not assigned to a Stufe cannot be used in conjunction with the Relay Contacts.

To view and manage the Message Rank Map, navigate to **Systeminfo > Rangfolge der Nachrichten**.

The screenshot shows the 'Maintenance message rank' table. The table has columns for 'Ereignis', 'Gerät' (with checkboxes for various device IDs), and 'Stufe'. The 'Rangfolge der Nachrichten' menu item is highlighted in the left sidebar.

Ereignis	005	002	004	010	020	030	031	032	033	040	041	Stufe	
Batterie NIEDRIG	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2	Details
Wartung erforderlich	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	Details
Batterie NIEDRIG	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	Details
Synchronisation verloren	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	Details
Wartung erforderlich	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2	Details

Below the table is a 'Neu' button.

Fig. 78 The Rangfolge der Nachrichten page

To classify a Maintenance Message type with a Level:

- Click **NEU** beneath the Message Rank Map
- Select the appropriate Maintenance Message **Ereignis** type from the drop-down list
- Use the checkboxes to select any devices for which Maintenance Messages of this type will be classified to the assigned Level
  - Multiple devices can be selected
- Select the required **Stufe** from the drop-down list
- Click **BESTÄTIGEN** to save
  - The new classification is displayed as a new row in the Message Rank Map

All existing Maintenance Message classifications are displayed in the Message Rank Map and can be edited by clicking **DETAILS** in the appropriate row. The Device Types to which each message classification applies are indicated by their hardware prefix code; see Appendix A.3.

Fig. 79 Adding a new Maintenance Message rule

**PLEASE NOTE:** Only one rule can exist for each event type at each level. If a second rule is configured using the same combination of **Ereignis** and **Stufe** selections, the first rule configured with these parameters will be overwritten.

To remove a Maintenance Message classification, click **DETAILS** in the appropriate row of the Message Rank Map and click **ENTFERNEN** to delete.

For guidance on the configuration of the Hub's Relay Contacts in response to Maintenance Message Levels, see section 5.4.23.

## 8 Operating the hardware interface

The front panel of the EkoSecure Hub can be used to raise and respond to system alarms and messages. Maintenance Messages and system alarms are shown on the LCD display.

**PLEASE NOTE:** The Emergency alarm button on the front of the device may be disabled as part of the Hub's Device Mode settings; see section 5.4.19.

### 8.1 Default display

During standard operation when no system alarms are active and all messages have been cleared, the following information is shown on the LCD display:

- System date and time
- The device name
- The power supply source
- The current system Shift

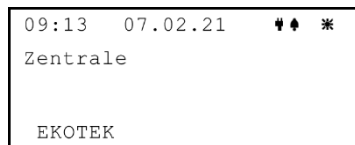


Fig. 80 The LCD display default screen

## 8.2 Raising and clearing alarms

System alarms are shown on the Hub LCD display and responses can be issued using the navigation buttons. Alarms can also be manually raised and cleared from the front panel interface, if enabled in the Hub's Device Mode settings; see section 5.4.19.

### 8.2.1 RAISING AN ALARM FROM THE HUB


Alarms can be raised manually from the Hub by pressing the **RED** Emergency button  on the front panel either once or twice, depending on the value of the **Betriebsart** parameter in the **Manueller alarm aktiv** setting of the Hub's configured Device Mode settings; see section 5.4.19.



Fig. 81 The LCD display as an alarm is raised from the Hub

When raised, alarms are sent to the devices included in the Pager Group specified by any configured Alert Rules that apply. If no Alert Rules have been configured that include manual alarms raised by the Hub, alarms are sent to devices assigned to Pager Group 1.

The alarm message text sent to devices included in the configured Pager group contains the following information:


- The identity of the device raising the alarm
- The type of alarm that has been raised

**PLEASE NOTE:** Only Emergency alarms can be raised from the Hub front panel; however, alarms raised by other devices will indicate the type of alarm that has been raised.

Alarms raised by portable devices also include the location in which the alarm was raised, based on the identity of the static system device from which the alarm device most recently detected Location Beacon data. If an alarm is raised by a static device, including the Hub, location data is not included in the alarm message as the device identifier already contains this information.

When an alarm is received by portable devices in the system, an audio alert sounds, if enabled, and the display illuminates to show the alarm message.

### 8.2.2 CLEARING AN ALARM RAISED BY THE HUB

To clear an alarm raised by the Hub, press and hold the  button on the front panel of the device. The Hub display will indicate that the alarm has been cleared and an audio tone will sound, if configured.

Upon clearance of an alarm, a message containing the identity of the device is sent to other system devices to indicate that the alarm has been cleared.



Fig. 82 The LCD display indicates that the alarm has been cleared

### 8.2.3 ALARM ESCALATION

If an alarm raised manually from the Hub is not cleared within 60 seconds of the alert, the alarm message is resent to all system devices. The message is resent each time the configured period elapses.

## 8.3 Receiving messages

When a message is received by the Hub, an audio tone will sound and the full message is shown on the display.

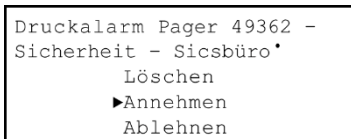



Fig. 83 The message detail screen with available response options when accessed

### 8.3.1 RESPONDING TO A MESSAGE

To respond to a message:

- a) Press  to view and scroll through the available actions for the current message
  - i) Available responses may include:
    1. **Annehmen** – A message is sent to the sender device to notify that assistance is coming
    2. **Ablehnen** – The alarm notification is cleared from the Hub display but message remains in the message list

### 3. **Löschen** – The message is removed from the Hub display

- b) Press  to perform the selected action

If no action is taken, the message display will time out after a few seconds and the Hub will revert to the default display screen, where a preview of the message is listed.

### 8.3.2 MESSAGES LISTED ON THE DEFAULT DISPLAY

The first part of each received message that has not been cleared by the sender or deleted from the Hub is listed on the default display screen. The list may contain up to 4 messages at one time.

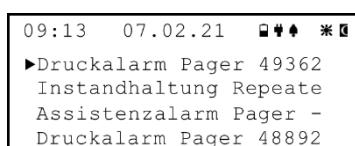






Fig. 84 The default LCD display when messages have been received

To respond to a message from the default display screen:

- a) Press  to scroll through the available messages
- b) Press  to display the selected message in full
- c) Press  to view and scroll through the available actions for the current message
- d) Press  to perform the selected action

### 8.3.3 RECEIVABLE MESSAGE TYPES

The following message types may be received by the Hub and shown on the LCD display:

- In response to a Personal Security alarm:
  - **Alarm angenommen** – Received when another device has accepted an alarm raised by the Hub and the user is en route
- When the Hub interface is used to respond to an incoming alarm:
  - **Ruf angenommen** – Confirmation that the user has accepted the alarm
  - **Ruf abgelehnt** – Confirmation that the alarm was rejected by the Hub operator
- Generated when system maintenance is required:
  - **Batterie NIEDRIG** – Shown on the bottom of the LCD display screen when the Hub's on-board battery charge level drops to 20%
  - **Batterie austauschen** – Shown on the bottom of the LCD display screen when the Hub's on-board battery charge level drops to 5%
  - **Wartung erforderlich** – Delivered in the same format as a system message
    - Generated when a static system device fails to report on

its status for a fourth time

- This message is repeated on every sixth consecutive occasion that a device fails to deliver a status report
- This message includes the name of the device requiring attention

## 8.4 Zeitalarm prompts

Like other system devices, in order to verify the safety of its operator, the Hub is configured to request a user response every 30 minutes. These prompts appear as a **Drücke ◀ ▼ oder ▶** message on the LCD display and are accompanied by an audible alert.



Fig. 85 The Hub requests a user response every 30 minutes

To acknowledge the prompt, press any of the navigation buttons on the Hub front panel. If a response is not received within 15 seconds of the prompt, a Zeitalarm is raised by the Hub and a message is sent to system Pagers according to any configured Alert Rules; see section 5.6.

A Zeitalarm raised by the Hub can be cleared by holding the ◀ button.

## 8.5 Hub operation menu

The Hub operation menu can be accessed by holding the ▼ button while the default screen is shown.

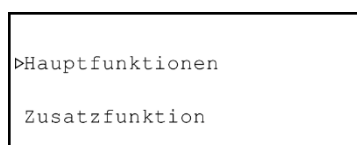


Fig. 86 The Hub operation menu

### 8.5.1 HAUPTFUNKTIONEN

To access the **Hauptfunktionen** sub-menu, use ▼ to scroll to the appropriate option and press ▶ to enter.

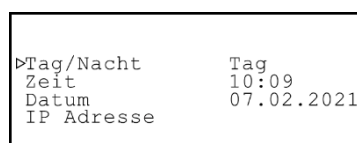






Fig. 87 The settings available in the Hauptfunktionen sub-menu

The Hauptfunktionen sub-menu contains the following options:

### Tag/Nacht

This setting defines the current system Shift. The devices to which alarms are sent may differ depending which Shift is currently active.

To manually set the current system Shift:







- a) Use  to scroll to the **Tag/Nacht** setting and press  to enter
- b) Use  to select the required option and press  to confirm

**PLEASE NOTE:** Changes made to the **Tag/Nacht** setting using the LCD display are only permanent if the system Shift mode is set to **Manuelle Auswahl**; see section 6.1.1. If **Automatisch** mode is enabled, the **Tag/Nacht** setting can be temporarily changed through the LCD display, but will revert to the configured settings at the next scheduled Shift change. If **Extern** Shift mode is enabled, the **Tag/Nacht** setting cannot be changed through the LCD display.

### Zeit

This setting configures the EkoSecure system time as shown on the Hub LCD display.

To manually set the system time:






- a) Use  to scroll to the **Zeit** setting and press  to enter
- b) Use  to set the clock hour value
- c) Press  to enable the minutes selector
- d) Use  to set the clock minutes value
- e) Press  to confirm the configured time
- f) The Hub display updates with the new time after a short delay

**PLEASE NOTE:** If the Hub is configured to receive its time settings from an NTP server, permanent changes to the Time and Date cannot be made using the LCD display.

### Datum

This setting configures the EkoSecure system date as shown on the Hub LCD display.

To manually set the system date:

- a) Use  to scroll to the **Datum** setting and press  to enter
- b) Use  to set the first value
  - i) This may represent the day or month depending on the date format configured in the system settings
- c) Press  to enable selection of the second value
- d) Use  to set the second value
  - i) This may represent the day or month depending on the date format

- configured in the system settings
- e) Press > to enable selection of the year value
- f) Use ▼ to set the year value
- g) Press > to confirm the configured date
- h) The Hub display updates with the new time after a short delay

**PLEASE NOTE:** If the Hub is configured to receive its time settings from an NTP server, permanent changes to the Time and Date cannot be made using the LCD display.

### IP adresse

This option shows the IP address of the Hub on the LCD display.

To view the IP address of the Hub:

- a) Use ▼ to scroll to the **IP adresse** setting
- b) Press > to select the setting
- c) Press > to confirm the selection
- d) The display returns to the default screen
- e) The IP address of the Hub is displayed as a message after a short delay
  - i) Delivery of the message is indicated by an audible tone
  - ii) The message containing the Hub's IP address is added to the list of received messages and can be deleted in the same way as other messages

### 8.5.2 ZUSATZFUNKTION

To access the **Zusatzfunktion** settings sub-menu, use ▼ to scroll to the appropriate option and press > to enter.

```

>Display
  Nutzerprofil
  Zeige Löschinfo  Ein
  
```

Fig. 88 The Zusatzfunktion sub-menu of the LCD display

The Zusatzfunktion sub-menu contains the following options:

- **Display** – Sub-menu
- **Nutzerprofil** – Sub-menu
- **Zeige Löschinfo** - Setting

To edit any option in the sub-menus available with the Zusatzfunktion settings:

- a) Use ▼ to scroll to the required setting
- b) Press > to access the selected setting
- c) Use ▼ to scroll through the available options for the selected setting



- d) Press **>** to confirm the selected option
- e) Press **<** to return to the Display sub-menu
- f) Press **<** again to return the Hub operator menu if required

### Display

The **Display** option of the Zusatzfunktion menu contains a further sub-menu. To access the Display sub-menu, use **<** to scroll to the appropriate option and press **>** to enter.

```

>Stunden Modus      24H
Display Timer       16s
Schriftart          10x5
Kontrast            2

```

Fig. 89 The settings available in the Display sub-menu of the LCD display

The following settings can be edited from within the Display sub-menu:

- **Stunden Modus** – Defines whether the system clock is displayed in 12-hour or 24-hour format
- **Display Timer** – Defines the period of inactivity, in seconds, after which the LCD display will return to the default display screen
- **Schriftart** – Defines the font size of the message display screen
  - Other display text is not affected
- **Kontrast** – Sets the LCD display contrast between the text and backlight

### Nutzerprofil

The **Nutzerprofil** option contains a further sub-menu. To access the Nutzerprofil sub-menu, use **<** to scroll to the appropriate option and press **>** to enter.

```

>Beleuchtung        Ein
Ruftone              Ein

```

Fig. 90 The settings available in the Nutzerprofil sub-menu of the LCD display

The following settings can be edited from within the Nutzerprofil sub-menu:





- **Beleuchtung** – Determines whether the LCD display backlight is on or off during normal operation
  - Even if set as **Aus**, the backlight will continue to illuminate when alarms and other messages are received by the Hub
- **Ruftone** – Determines whether an audible tone is emitted from the Hub when alarms and messages are received

### Zeige Löschinfo

This setting toggles the visibility of the **Halte ◀ zum löschen** message shown at the

bottom of the screen when an alarm is raised manually from the Hub.

To edit this setting:

- a) Use  to scroll to the **Zeige Löschinfo** setting
- b) Press  to edit the setting
- c) Use  to select the required option
- d) Press  to confirm the selection

**PLEASE NOTE:** Hiding the **Halte zum löschen** message does not disable the ability to clear the alarm from the Hub.

## 9 Upgrading the Hub software

Upgrades to the Hub software can be performed by entering **http://[Hub IP address]/upgrade** into the URL field of the web browser.

**EXAMPLE:** The upgrade URL for a Hub device using the default IP address would be **http://192.168.1.2/upgrade**.

To perform a device software upgrade for the Hub:

- a) Create an archive of the current system configuration and device registry
  - i) See section 5.11
- b) Navigate to the appropriate address of the Hub's Upgrade page
- c) Click **CHOOSE FILE**
- d) In the new window, locate and open the required software upgrade file
  - i) Upgrade files are available from Multitone upon request
- e) The file is listed beside the **CHOOSE FILE** button
- f) Click **LADEN** to upload the upgrade file
- g) If the archive is uploaded successfully, a **ZURÜCKSETZEN** button is added to the page
- h) Click **ZURÜCKSETZEN** to begin the upgrade
  - i) The upgrade process may take a few minutes and is indicated on the system Hub LCD display by a flashing ! in the timestamp
  - ii) When the timestamp returns to its normal format with a : separator, the process has completed

**CAUTION: DO NOT** navigate away from the upgrade page or attempt to load any configuration pages in the web browser as this may interrupt the upgrade process. During the upgrade process, carefully monitor the Hub LCD display until the timestamp returns to its normal format with a : separator, indicating that the process has completed. **ALWAYS** contact Multitone for assistance when planning to upgrade a system Hub.

## 10 Servicing

Only the 4 x on-board batteries should be replaced by the user. The EkoSecure Hub contains no other serviceable parts. All 4 batteries should be replaced at the same time, every 24 months.

**WARNING:** Batteries installed in the device **MUST** be rechargeable AA Nickel-Metal-Hydride (NiMH) batteries with a minimum capacity of 2.4 Ah. Replace all 4 batteries at the same time.

As far as possible, the Hub should not be exposed to rain, moisture, or other liquids, but may be wiped clean using a damp cloth.

Any additional device maintenance or repair should be carried out by Multitone. Contact your Multitone Agent at *info@multitone.de* or *supportdesk@multitone.com* for assistance.

## 11 Additional support

For additional support and further details about this product, please contact Multitone directly using the appropriate contact details:

### Deutschland:

Multitone Elektronik International GmbH  
Roßstraße 11  
40476 Düsseldorf  
**www.multitone.de**

*info@multitone.de*  
+49 211 46902-0

### UK:

Multitone Electronics plc  
Multitone House  
Shortwood Copse Lane  
Kempshott  
Basingstoke  
Hampshire  
RG23 7NL  
United Kingdom  
**www.multitone.com**

*info@multitone.com*  
+44 (0)1256 32029

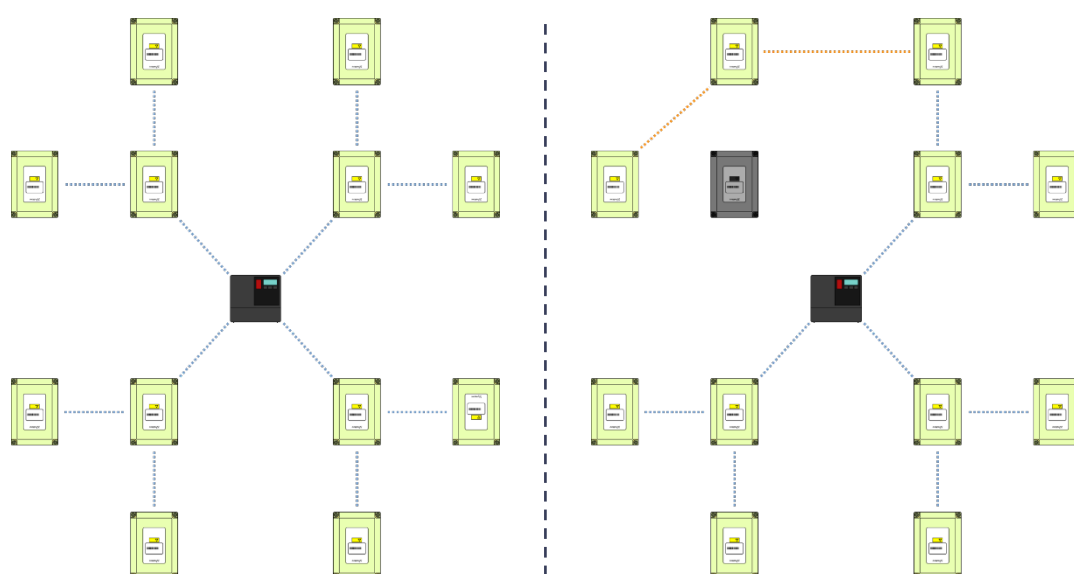
# Appendices

## A EkoSecure principles

EkoSecure is a long-range personal security system comprising static and portable devices that communicate via a radio network mesh to deliver alarm and maintenance messages to device operators. A combination of alarm location data and audible alert tones assist responders in locating the site of a raised alarm.

### A.1 THE RADIO NETWORK MESH

An EkoSecure personal security system comprises a radio messaging network mesh formed by nodes (static devices, including Long Range Repeaters). The system nodes form a network mesh that relays data between a central Hub and portable or static EkoSecure messaging devices on which personal security and maintenance messages are displayed, along with the location of the source. The wireless connection between two static devices is considered a 'network hop'.



**Fig. 91-92** The EkoSecure network mesh automatically establishes new connections when a system node becomes unreachable

The network mesh created by the system nodes has multi-hop capability, allowing the network to exist in three dimensions. This enables the network to cover areas on multiple floors of the same, or different, buildings. The mesh is also self-healing and self-organising, allowing the system to select the most effective connection between nodes and remap its connections should a device become unreachable. The connections available to specific devices can be restricted to designated groups to provide greater control over the

remapping process where required. In most instances, the system Hub should be located at the centre of the network, and the number of hops between nodes within an EkoSecure system should be kept as minimal as possible.

All static EkoSecure devices utilise an external power supply with a battery back-up to ensure robust and continued operation.

## A.2 BEACONS

EkoSecure network nodes broadcast two beacons as standard:

- Main (radio) Beacon
- Location Beacon

The purpose of the Main Beacon is to create the network mesh and transmit system messages between devices; the Location Beacon delivers location data to nearby portable devices, which is included in the system messages when alarms are raised.

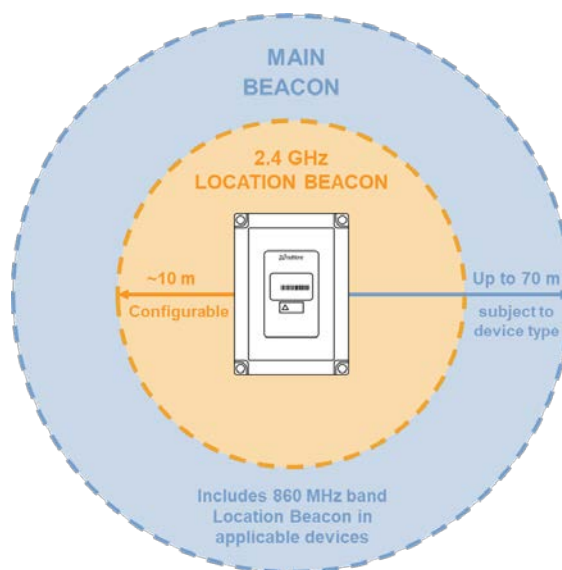


Fig. 93 Each network node can broadcast two Beacons

### A.2.1 MAIN BEACON

The Main Beacons broadcast by network nodes establish connections with other devices within the system and carry radio messages either downstream (in the direction of portable devices, which form the end points of each network branch) or upstream (in the direction of the Hub, which forms the centre of the mesh).

Within EkoSecure systems, the Main Beacon must be broadcast over 863-870 MHz frequencies. Where EkoSecure is installed as part of a wider EkoTek system, nodes in the EkoTek regions of the system may broadcast Main Beacons over 2.4 GHz frequencies. Where this occurs, an EkoSecure Repeater

functioning as a signal convertor must be installed at the boundary of the two regions.

Transmissions over 860 MHz band frequencies are managed by the new EkoSecure Hub's Adaptive Frequency Agility (AFA) capability, which enables system nodes broadcasting in this band to automatically select the specific frequency that is most appropriate at the time of each message. The new EkoSecure Hub also has Listen Before Talk (LBT) capability, which enables the device to assess the traffic on its current frequency before transmitting a message across the mesh.

Where the Main Beacon is broadcast over 2.4 GHz, the specific signal frequencies are defined as Channels and can be fixed for each individual node if required. This can be used to create segregated areas of the network mesh and limit the number of devices to which a node may automatically connect when a network remap occurs. This may help to avoid frequencies over which radio interference is anticipated in specific areas of the network, or to limit the number of network hops between specific devices and the Hub. A network channel must be selected for the Hub itself.

Alternatively, static devices can be configured to inherit their upstream and downstream broadcast frequencies from their Parent device. This allows nodes to select the most appropriate device with which to connect when remapping is required, but there are no restrictions as to which node the device will form a connection. Configuring the upstream channel of a node to inherit the frequency of its parent allows that device to transmit upstream messages (typically alarms or Maintenance Messages) to any viable device, which may expedite delivery of the message to the Hub.

The new EkoSecure Hub can be configured to enable frequency hopping within the system, through which transmission over an alternating sequence of frequencies is achieved. This may be useful in the avoidance of intermittent interference across the radio spectrum; however, in most circumstances this is not required.

The number of nodes per channel is limited to 60 devices. In systems where more than 60 static devices are installed, some or all system devices must be configured with fixed downstream channels to prevent overcrowding of a single frequency. In such cases, it may be possible to retain upstream channel inheritance from Parent devices, as the upstream radio traffic is significantly less frequent.

The Main Beacon can be disabled for some node types. This enables devices at the peripheries of a network to function as a Location Beacon where extension of the mesh coverage is not necessary, but Location data is still required for nearby

portable devices. Devices configured as a Location Beacon still transmit alarms upstream when raised.

Main Beacons broadcast over 860 MHz band frequencies can cover a radius of up to 70 m between repeating devices, or up to 50 m to a pager, subject to environmental factors. Main Beacons broadcast over 2.4 GHz frequencies can cover a radius of up to 10-15 m. When using either frequency range, the Hub should be positioned within close range of multiple repeaters in order to overcome potential signal interference caused by the presence of personnel.

## A.2.2 LOCATION BEACON

Portable EkoSecure system devices carry two pieces of Location data:

- The identity of the Parent device with which the portable device has established a radio connection
- The identity of the Location Beacon of which the portable device was most recently within range

These items of data may refer to either the same or different devices.

The Location Beacon broadcast by EkoSecure system nodes is transmitted as a short-range signal over 2.4 GHz frequencies and as a long-range signal over 860 MHz band frequencies. The range of the 2.4GHz signal can be customised using the Lokalisierungsbereich Device Mode setting (see section 5.4.18), but the 860 MHz band signal is fixed at the same range as the Main Beacon.

These signals deliver the name of the node device as Location data to nearby portable devices. When a portable device moves within range of a new Location Beacon, the device's Location data is updated. The device stores this data and transmits it as part of the alert message when it is used to raise an alarm.

**PLEASE NOTE:** EkoSecure Repeaters configured to function as a Location Beacon only do not broadcast any signal over the 863-870 MHz frequencies.

Unlike EkoTek devices, EkoSecure devices use 860 MHz band Location Beacons to identify potential parents.

Location Beacons are also utilised in the configuration of Wander alarms, which are triggered by portable devices when they receive Location Beacon data from a node assigned to a network Zone to which the portable device is not permitted access.

The Location Beacon cannot be disabled for any Device Types.

## A.3 DEVICES

EkoSecure systems consist of three categories of device:

- Static devices (nodes)
- Portable devices
- External devices

Additionally, the Hub functions as a unique static device from which the entire system is managed.

The following Device Types can be configured through the EkoSecure Hub as part of an EkoSecure system. The hardware prefix for each Device Type is also shown

- **Hub** – 001
- **IP Slave Hub** – 002
- **Ethernet Repeater** – 004
- **Fob** – 010
- **Pager** – 020
- **Repeater** – 030
- **Solar Repeater** – 031
- **Long Range Repeater** – 032
- **Overdoor Light** – 033
- **Call Point** – 040
- **EkoCare Unit** – 041

**PLEASE NOTE: ONLY** EkoSecure variants of the Hub, Pager, and Long Range Repeater devices may be used within self-contained EkoSecure systems.

The system does not distinguish between mains-powered and battery-powered variants of the same Device Type.

Communication between devices is achieved via radio broadcasts according to the configuration of the network mesh. Most devices can be used to raise alarms raised within the system.

The EKSHUB model operates in compliance with DIN VDE V 0825-1 (formerly BGR139). To support the timing requirements of this standard, the maximum number of devices supported by a single Hub system is 50.

### A.3.1 THE HUB

The system Hub is a network node that functions as the central control for the EkoSecure system. Most of the system configuration can be managed through the Hub's browser interface, accessible via one of the 10/100Base-T Ethernet ports located beneath the removable lower front panel. This includes device



management, alarm handling, and device software updates. Data assessing network performance is collected by each EkoSecure device and periodically reported to the Hub, and can also be viewed through these web pages.

The Hub may be used to integrate with external devices and systems, and for sharing of system data with remote logging devices. Alarms may also be raised and responded to via the Hub's front panel interface.

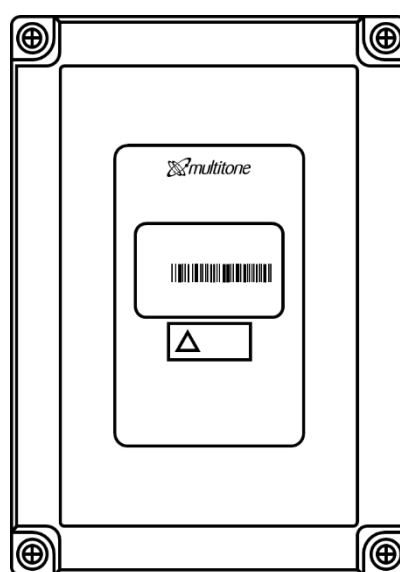
The Hub may be supported by subordinate (Slave) devices that temporarily assume management of the system in the event of device failure.

### A.3.2 STATIC DEVICES

Network nodes are static system devices that are installed in a fixed position and form part of the network mesh through the broadcast of Main (Radio) Beacons. Self-organising wireless connections are established between nodes that remap when a device experiences an issue or becomes inoperable. Network nodes also broadcast Location Beacons, which are used to identify the site at which an alarm was raised.

All portable devices must accept a static device as a Parent in order to transmit and receive messages through the network mesh. Static devices may be assigned to network Zones, which can be used to designate areas of the environment to which portable device carriers are not permitted access.

Some static devices include an interface that may be used to raise and respond to alarms. Some devices may also connect to external devices via on-board Relay Contacts.



**Fig. 94** The EkoSecure Repeater is the only static device permitted within EkoSecure regions of a network

Every static device reports its device status, including battery level and radio performance, to the Hub approximately every 10 minutes.

Where EkoSecure is used in isolation, only EkoSecure Repeater devices may be used as static devices within the system, in addition to the EkoSecure Hub.

### A.3.3 PORTABLE DEVICES

Portable devices within an EkoSecure system can be carried around the environment covered by the network mesh and are the principle means by which operators can raise alarms. Portable devices automatically connect to the most appropriate static device as their position within the environment changes, and receive Location data that is included in alarm messages when passing within range of a network node's Location Beacon.

The network areas to which each portable device is permitted access can be managed through the use of network Zones. A Wander alarm is raised when the presence of a portable device within the range of a Location Beacon in an unauthorised Zone is detected.

In DIN VDE V 0825-1 compliant systems, alarms raised by a portable device must be cleared by the portable device carried by the responder. Portable devices in compliant systems emit an 85 dBA tone when raising an alarm, as a means of pinpointing the exact location of the sender.

Only EkoSecure Pagers may be used as portable devices within EkoSecure regions of a network mesh.



**Fig. 95** The EkoSecure Pager is the only portable device permitted within EkoSecure regions of a network

### A.3.4 EXTERNAL DEVICES AND SYSTEMS

External systems can be integrated into an EkoSecure network through a one-way paging interface comprising two RS232 ports available beneath the Hub's removable front panel. The interface can be configured as TAP or ESPA 4.4.4,

and messages can be either sent to or received from the connected system, but not both.

Inclusion of external pagers in alarm messages when raised within an EkoSecure network can be configured using the system Alert Rules; only one of the configured rules may include external pagers. Messages delivered from external paging systems are one-way downstream messages from the Hub to portable devices.

EkoSecure can also integrate other alarm-based devices via the contacts available within static system devices:

- The Hub features three individually configurable Relay Contacts that can be used to output alarm signals
- Other static system devices include Contact Inputs that accept signal inputs from external devices

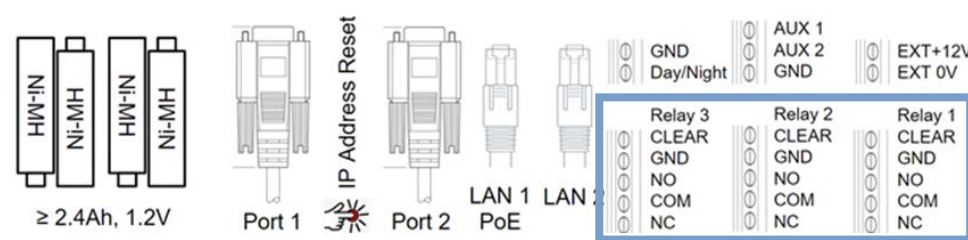


Fig. 96 Locating the Relay Contacts beneath the removable front panel of the Hub

Handling of Contact Inputs and Outputs can be configured in the appropriate Device Mode for each Device Type via the Hub browser interface.

## A.4 DEVICE MODES OVERVIEW

The manner in which EkoSecure system devices operate can be configured using Device Modes. This includes the radio configuration of the device, alarm types that may be raised by the device, and the messages that are sent when those alarms are raised.

Where devices are grouped by the differing ways in which they are used, Device Modes may be configured to define the specific functionality of each group. This may be useful for enabling specific alarms on designated devices, restricting or simplifying device functionality, and managing the network areas into which they are permitted access.

Devices Modes are configured within each Device Type, as each Device Type contains a specific selection of available settings. Up to 120 Device Modes may be configured per Device Type. Each device may only be assigned to one Device Mode at any given time, but the selected Mode and its configured settings may be changed as required.

## A.5 NETWORK ZONES OVERVIEW

Static system devices can be assigned a network Zone number. This Zone number is included in the location data transmitted by the device's Location Beacon and can be used by portable devices to determine whether access to that particular location is permitted.

The Zones to which a portable device is permitted access are configured as part of the Device Mode assigned to the portable device. Each Device Mode may permit access to different Zones, allowing different devices to be used in specific areas of the network. If a portable device is carried within range of a Location Beacon that has been assigned to Zone number that the portable device is not permitted to access, the device will raise a Wander alarm. This can be cleared by returning to a network area to which access has been granted. Unauthorised Zones are identified in the Device Mode settings for each portable Device Type.

Device location data is only updated when a new Location Beacon is detected. Where permission changes are made to a Zone in which a portable device is already located, the portable device must move to a new location before the changes are applied.

Portable devices must always be permitted to access at least one Zone within the network.

## A.6 ALARMS

The primary function of the EkoSecure system is to enable operators to manually raise alarms when in difficulty, or to raise alarms automatically when the operator is unable. System alarms exist in several forms to reflect a number of situations that may befall system operators, each of which requires a specific method in order to be raised and cleared. The recipients of each alarm can also be defined according to several conditions relating to the way in which it was raised.

### A.6.1 ALARM TYPES

The following alarms may be raised as part of an EkoSecure system, if enabled in the Device Mode configuration. Alarms generated by users within the system are two-way messages, with notifications of responses to alarms returned to the original sender.

Alarm category	Alarm type	Raised by	Cleared by
Personal Security	Manual (Emergency)	Pressing the <b>RED</b> button on the device	Holding the designated button on the device
	Assist	Pressing the <b>BLUE</b> button on the device	Cannot be cleared
	Man Down	Holding the device out of the configured orientation for a prolonged period	Returning the device to the correct orientation and holding the designated <b>GREY</b> button
	Dead Man	No response received to a user prompt	Holding the designated <b>GREY</b> button

	Snatch	Removal of the Snatch Cord from the device	Returning the Snatch Cord to the device
	Wander	Carrying the device into an unauthorised area	Returning the device to an authorised area
	External Contact	Receipt of an alarm input via the on-board contacts	Holding the designated button on the device; changes in the contact input signal as configured
Nurse Call	Emergency	Pressing the <b>RED</b> button on the device	Pressing the designated button on the device according to the configured settings
	Nurse Assist	Pressing the <b>BLUE</b> button on the device	Cannot be cleared
	Patient Call	Pressing the <b>ORANGE</b> button on the device	Pressing the designated button on the device according to the configured settings
	Attendance	Pressing the <b>GREEN</b> button on the device	Pressing the <b>GREEN</b> button on the device a second time
	External Contact	Receipt of an alarm input via the on-board contacts	Holding the designated button on the device; changes in the contact input signal as configured
	Tamper	Removal of a Patient Call Button accessory	Return the Patient Call Button and press the <b>GREEN</b> button

Nurse Call alarms are not compatible with self-contained EkoSecure systems.

Each Alarm Type can be configured to be handled differently by the system. The way in which each alarm type is handled can be defined using the system Alert Rules. Several other parameters, including the time of day, the device User Group, and the network Zone in which it was raised, can also be considered as part of the alarm handling conditions.

Most alarm types require action to be taken once raised. Clearing an alarm indicates that the situation has been resolved. Pager devices can be configured to clear alarms raised by devices that are within close physical proximity.

## A.6.2 ALARM ESCALATION

If an alarm is not cleared within the configured time period, it is resent with raised priority. The device will continue to resend the alarm until it has been cleared either by the alarm device or a nearby portable device that has been granted clearance capability.

The handling of escalated alarms can be configured differently to that of alarms with normal priority and may contact additional, or different, devices as a result. This is defined within the system Alert Rules.

## A.6.3 INFORMATION INCLUDED IN ALARM MESSAGES

All system alarm messages contain the following information:

- The alarm type
- The name and serial number of the device that raised the alarm
- The name and serial number of the current or last known location device of the device that raised the alarm
- The name and serial number of the device that accepted the alarm (when actioned)
- The timestamp from when the alarm was raised

Only the alarm type, device name, and location device name are shown on device LCD displays.

The Location data supplied when an alarm is raised relates to the source of the Location Beacon that the alarm device has detected most recently, providing the identity of the current or last known physical location of the device. This avoids misdirection when the alarm device is physically located on another floor or in another building to the static device to which it is connected via the Main Beacon.

Where an alarm is raised by a static device, there is no Location data supplied as the alarm device identifier already defines the alarm location.

#### A.6.4 ALERT RULES OVERVIEW

Alert Rules can be configured to define the devices to which alarms meeting various conditions are sent. This can be used to ensure that each alarm is directed to the appropriate recipients and that other device operators are not disturbed by notifications that are not relevant.

The most appropriate recipients for alarm notifications may differ according to specific parameters, including the alarm type, the time raised, and the level of escalation of the alarm. The handling of alarms that meet specific criteria can be defined using the system Alert Rules. Where applicable, Nurse Call alarm handling is managed using EkoCare rules.

Up to 32 Alert Rules may be configured.

#### A.7 MAINTENANCE MESSAGES

System messages relating to device status and performance can be examined in more detail through the Hub's browser interface. Maintenance Messages typically require intervention from system administrators or engineers.

In DIN VDE V 0825-1 compliant systems, all EkoSecure devices automatically report their status, including mains failure events, battery level, and network performance, to the Hub approximately every 10 minutes. When delivery of this report coincides with a device exhibiting low battery charge, a Maintenance Message is generated. Maintenance Messages are also generated when a device fails to deliver a Device Status Report on 4 consecutive occasions, and for every 6 consecutive missed Reports thereafter.

System Maintenance Messages can be categorised into two Levels according to the devices to which they relate and the type of message generated. Each Level can then be assigned to a Relay Contact on the Hub's interface to trigger an output signal to connected devices and systems.

## B Compliance with DIN VDE V 0825-1

This model of the EkoSecure Hub is preconfigured to function in accordance with DIN VDE V 0825-1 requirements. This affects the following settings and features, which cannot be edited by the user:

### B.1 RESPONSE TIMES

The following requirements relating to the speed of system response in the event of an alarm being raised are stipulated in clause 4.1.2:

- The signal from any personal alarm raised from any portable device within the system must be made evident by the system Hub through audible and visual notification within 2 seconds
- The period for which a user is informed of an impending automatic alarm resulting from inaction must not exceed 15 s
- The period between prompts for user response must not be greater than 30 minutes
- The period for which a portable device may be held at an incorrect orientation before an alarm is raised must not exceed 90 seconds
- Any device or network failure must be made evident by the Hub and other devices through audible and visual notification within 10 minutes of the occurrence

The EkoSecure system employs the following features to meet these specifications:

- The system employs message timeslot optimisation to detect alarm messages early and ensure that personal alarms raised by system devices are delivered to the Hub within 2 seconds
- The maximum period for which a system device will alert the user if a response is not given when prompted is 15 seconds; this can be decreased but not increased
- The maximum interval between prompts for a user to indicate activity is 30 minutes; this can be decreased but not increased
- The maximum trigger period for an alarm caused by an incorrect orientation of a portable device is 90 seconds; this can be decreased but not increased
- All system devices automatically emit a signal every 10 minutes to indicate their continued functionality as part of the network
  - If a device fails to deliver this signal, **Wartung erforderlich** and the relevant device name are clearly shown on the Hub's LCD display



## B.2 PAGER IDENTIFICATION IN ALARMS

The following requirements relating to the inclusion of portable device identification information when alarms are raised are stipulated in clause 4.1.2:

- In the event of a personal or technical alarm being raised by a portable device, the system Hub must indicate the identity of the device from which the alarm is raised

The EkoSecure system employs the following features to meet these specifications:

- The unique identifier of the sender device is included in every alarm package raised within the system; for more information relating to the Hub display in response to system alarms, see section 8.3
  - This information is also included in data packages, in numeric and text format as configured, sent to remote logging devices; see Appendix C

## B.3 MONITORING AND TECHNICAL ALARMS

The following requirements relating to the automatic self-assessment of the network and connected devices are stipulated in clause 4.1.3:

- The system Hub must automatically and frequently monitor and assess the status and performance of the network and portable devices
- Any device or network failure must be made evident by the Hub and other devices through audible and visual notification within 10 minutes of the occurrence

The EkoSecure system employs the following features to meet these specifications:

- The strength of the signal connection between individual static devices and from each static device back to the Hub can be viewed on the Gerätestatus and Netzwerk-Baum pages, respectively
- All system devices automatically emit a signal every 10 minutes to indicate their continued functionality as part of the network
  - If a device fails to deliver this signal, **Wartung erforderlich** and the relevant device name are clearly shown on the Hub's LCD display

## B.4 PAGER OPERATION

The following requirements relating to the recording of portable device operation are stipulated in clause 4.1.3:

- The Hub must record the activation of portable devices within the system

The EkoSecure system employs the following features to meet these specifications:



- Upon removal of a portable device from a charging rack, a test cycle of all configured alarms is performed by the device
  - The result of this test is entered as a record in the system Event Log, visible through the **Hauptmenu** options of the Hub's web interface

## B.5 ALARM TYPE TEST ON PAGER ACTIVATION

The following requirements relating to the test operation of all alarm types by portable devices are stipulated in clause 4.1.4:

- All portable system devices must test the functionality of each alarm type activated for that system when removed from a charging rack
  - This test must be re-run automatically no later than 24 hours after the most recent test on that device
- If this alarm test fails, the device must not be available for use

The EkoSecure system employs the following features to meet these specifications:

- Upon removal of a portable device from a charging rack, a test cycle of all configured alarms is performed by the device
  - This test cycle is also performed automatically if it has not been returned to a charging rack within 24 hours of the most recent test on that device
- The test cycle presents visual prompts on the Pager display that guides the user through the triggers of all configured alarms
- More information on the alarm test cycle is available on request

## B.6 NOTIFICATION OF PERSONAL ALARMS BY THE HUB

The following requirements relating to the presentation of personal alarms are stipulated in clause 4.4.1:

- Alarms relating to user safety (personal alarms) must be made evident by the Hub and other devices through audible and visual notification
  - The presentation of personal alarms must be clearly differentiable from technical alarms

The EkoSecure system employs the following features to meet these specifications:

- All system alarms are displayed on the Hub LCD display and are accompanied by an audible alert
  - The settings permitting alteration of these features are disabled for this model
- Personal alarms and technical alarms are differentiated by variations in:
  - The text shown on the LCD display when received
  - The audible alert pattern heard when received

## B.7 MANUAL CLEARANCE OF AUDIBLE AND VISIBLE ALERTS

The following requirements relating to the ability to clear audible and visual alarm notifications are stipulated in clause 4.4.2 and 4.4.3, respectively:

- It must be possible to end and reset the audible alert manually
- It must be possible to clear and reset the visual alert manually on each system device individually

The EkoSecure system employs the following features to meet these specifications:

- All alarm messages can be cleared from the Hub using the front panel interface; see section 8.3
  - Clearing an alarm resets both the audible and visual alarm alerts
- All system personal alarms can be cleared either by the Hub or by a Pager operating in a Device Mode for which the **Freigabe zur Alarmlöschung** setting has been enabled, that is in close proximity to the device that raised the alarm
- All system maintenance alarms are reset once the maintenance issue has been resolved and the regular signal from the originating device is emit as normal

## B.8 INTERNAL AND EXTERNAL LOGGING OF ALARMS

The following requirements relating to the recording of system alarms are stipulated in clause 4.4.4:

- A record of all personal and technical alarms communicated through the system must be stored by the Hub
- Records of system alarms must contain a minimum of the following information entries:
  - The date and time of the alarm
  - The identification of the device initiating the alarm
  - The type of alarm raised
  - The date and time at which the alarm was cleared
- The system Hub must include at least one interface through which connection to an external logging device or printer can be achieved

The EkoSecure system employs the following features to meet these specifications:

- A full internal log of all system events, including alarms, is available on the Event log page of the Main menu, accessible through the web interface
- The system event log can also be shared with and stored on a remote device
  - This connection can be configured on the **System** settings page of the **Konfiguration** menu
  - For more information, see section 5.1.4 and Appendix C

## B.9 INDEPENDENT POWER SUPPLIES

The following requirements relating to the supply of power to the system Hub are stipulated in clause 4.4.5.1:

- It must be possible to power the system Hub through two independent supplies:
  - One power supply may be available on a public network
  - One power supply must be independent of public supply

The EkoSecure system employs the following features to meet these specifications:

- The EkoSecure Hub is delivered with 4 x on-board rechargeable batteries that ensure continued functionality of the device in the event that the external power supply is removed
  - The device will not function if the on-board batteries are not installed and at an appropriate level of charge to support a controlled power-down procedure
- For more information, see section 3

## B.10 FAIL-OVER POWER CAPABILITY

The following requirements relating to the capability of the network-independent power supply are stipulated in clause 4.4.5.2:

- The network-independent power facility of the system Hub must guarantee the continued function of the device for at least 30 minutes after network power has been removed

The EkoSecure system employs the following features to meet these specifications:

- The EkoSecure Hub is delivered with 4 x on-board rechargeable batteries to provide fail-over power in the event that the external power supply is removed
  - The battery type required for use in the EkoSecure Hub device is expressly stated in this document in several locations and will ensure continued system functionality for at least 30 minutes after failure of the external power supply
- For more information, see section 3

## B.11 INDICATION OF EXTERNAL POWER FAILURE

The following requirements relating to the indication of external power failure are stipulated in clause 4.4.5.3:

- A removal of the external power supply must be made evident by the Hub immediately and automatically in a way that can be easily observed

The EkoSecure system employs the following features to meet these specifications:

- **Stromausfall** is clearly displayed as a message on the Hub front panel display
  - This message is accompanied by an audio tone until a user response is submitted through the Hub front panel
- A Mains Failure message is also sent to all Devices in Pager Group 1
- For more information, see section 3.3

## B.12 PRODUCT LABELLING

The following requirements relating to the information displayed on the product are stipulated in clause 4.4.6:

- The system Hub must feature a clear and permanent label indicating the following information:
  - The name and address of the manufacturer
  - The type of device
  - The device serial number
  - Marking according to Article 19 of the Directive 2014/53/EU (RED)
  - Marking according to the Directive 2012/19/EU (WEEE)

The EkoSecure system employs the following features to meet these specifications:

- Each EkoSecure Hub is supplied with a label that displays the required information located behind the removable front panel of the device casing

## B.13 ENCLOSED USER INFORMATION

The following requirements relating to the delivery of user information are stipulated in clause 5:

- Every system Hub must be supplied with user information sufficient in content and language for the anticipated knowledge of recipient
- All information provided on the device or in accompanying documents must be clearly legible and comprehensible in the local language
- Where possible, information should be delivered using universal symbols
  - Any non-standard symbols used shall be clearly explained
- User information provided by the manufacturer must include:
  - The name and address of the manufacturer
  - The type of device enclosed
  - A clear list of technical data
  - Complete user instruction and handling information relating to the designated use of the device, including:
    - Any and all warnings

- Any and all precautionary measures to be observed during use
- Description of the operating controls
- Explanation of device displays and signals
- The order of operation
- Assembly and disassembly of detachable or replaceable parts
- Guidance on product maintenance
- Explanation of any non-universal symbols, images, abbreviations and warnings included in the documentation
- All Compliance certification and declarations

The EkoSecure system employs the following features to meet these specifications:

- Each EkoSecure Hub is supplied with the following documentation:
  - A Quick Guide covering use of the front panel and LCD display
- The following documents containing supplementary information are also available for download upon request:
  - An Operator Guide covering only the use of the front panel and LCD display
  - An Administrator Guide covering the full extent of operation, management, and configuration of the Hub
  - An Installation & Setup Guide for the EkoSecure system covering the processes and components involved with the installation of a new paging system
- Product documentation is provided in the language required by the customer

## B.14 ELECTRICAL SAFETY

The Hub conforms to the Electrical Safety Requirements outlined in EN 62368-1.

# C Remote logging output

The data output for remote logging is delivered as SysLog messages to UDP Port 514 of the configured IP address.

Messages can contain either numeric or text data only, or a combination of both, in tab-delimited fields. Every message contains all fields, even if empty, up to the last field that contains data, when the message line is terminated and a new line begins.

The data output contains the following information.

**PLEASE NOTE:** Cells in **GREY** are for reference only and are not included in the data package. The format and content of the remote logging output may be subject to change.

Field	1	2	3	4	5	6	7	8	9	10			
Format	Numeric												
Name	Log type	Message type		Primary hardware		Secondary hardware		Primary serial no	Secondary serial no	Text			
		Value	Reference	Value	Reference	Value	Reference			Primary name	Secondary name	Message	
C O N T E N T	1	Personal Security	1	Raised	1	Dead Man	3-digit hardware prefix for device sending message	7-digit serial number of device sending message	3-digit hardware prefix of Current Location Beacon source	7-digit serial number of Current Location Beacon source	Device raising / clearing alarm  OR  Device accepting / rejecting alarm	Location of device raising alarm  OR  Device accepting / rejecting alarm	Personal Security alert text
	2		Accepted	2	Man Down / External Contact	OR			Device responding to an alarm	OR	Device responding to an alarm		
	3		Rejected	3	Manual	OR			Device responding to an alarm	OR	Device responding to an alarm		
	4		Cleared	4	Location	OR			Device responding to an alarm	OR	Device responding to an alarm		
	2	Location	N/A	N/A	N/A	3-digit hardware prefix of current Location Beacon source	7-digit serial number of current Location Beacon source	Device reporting its location	Location	N/A	N/A		
3	Maintenance	1	Low battery	N/A	3-digit hardware prefix of current Location Beacon source	7-digit serial number of current Location Beacon source	Device requiring maintenance	N/A	N/A	Maintenance message			
4	Paging Message	1	Message	1	0 (if no response requested or sent to Pager Group)  OR  Hardware prefix of individually addressed location or responding pager	0 (if no response requested or sent to Pager Group)  OR  Hardware prefix of individually addressed location or responding pager	Blank (if no response requested)  OR  Individual pager name  OR  Pager Group name	N/A	Message text / delivery report / user response				
5	Nurse Call	1	Raised	1	0 (if no response requested or sent to Pager Group)  OR  Hardware prefix of individually addressed location or responding pager	0 (if no response requested or sent to Pager Group)  OR  Pager Group number	3-digit hardware prefix of Current Location Beacon source	7-digit serial number of Current Location Beacon source	Device raising / clearing alarm  OR  Device accepting / rejecting alarm	Location of device raising alarm  OR  Device accepting / rejecting alarm	Nurse Call alert text		

**Fig. 97** The content of data sent to remote logging devices from the EkoSecure Hub; items shown in grey are for reference only and do not appear in the log

# Index

<b><u>A</u></b>		
Alarms		
Clearing alarms	92	
Raising alarms	91	
Responding	92	
Zeitalarm prompts at the Zentrale	94	
<b><u>B</u></b>		
Buttons		
IP Reset Button	<i>See Removable front panel</i>	
Use 90		
<b><u>D</u></b>		
Device Types	104	
DIN VDE V 0825-1 compliance	111	
<b><u>L</u></b>		
LCD display		
Icons	12	
Message types	93	
Responding to messages	92	
LED indicators		
Configuration Installed	13	
EkoTek logo	13	
Radio beacon	13	
Timing Synchronisation	12	
<b><u>M</u></b>		
Menu		
Hauptmenu	76	
Konfiguration	21	
Systeminfo	83	
<b><u>P</u></b>		
Power		
Changing batteries	17	
Power failure	18	
Power supplies	15	
Powering down	16	
Powering up	16	
<b><u>R</u></b>		
Removable front panel		
12 V DC contacts	15	
IP Reset Button	14	
LAN ports	15, 23, 27	
Removal	13	
<b><u>S</u></b>		
Servicing	99	
Settings and pages		
Abstellruf	37	
Aktualisierung	72	
Alarm löschen	37	
Alarm Wiederholung	38	
Alarmbetrieb	38, 40	
Alarmregeln	63	
Alle löschen	68	
Anwesenheit	41	
Assistenzalarm	42	
Auf netzwerk fixieren	42	
Automatic Shift selection	77	
Autoregistrierung gerät	31	
Bereichsalarm	43	
Bewohnerruf	44	
Datensicherung	71	
Downstream-Kanal	45	
EkoCare Rules	67	
Ereignisprotokoll	78	
External Shift selection	77	
External systems	24	
Freigabe zur alarmlöschung	46	
Frequenzsprung	29	
Funk (page)	28	
Funk (setting)	47	

Funkverkehr	88	Relay operation	55
Geräte	32	Remote logging	25
Geräteprofil	35	Schwesternruf	56
Herunterfahren	74	Schwesternrufbetrieb	57
IP settings	23, 27	System	22
Kanal	47	System clock	22
Kontakt eingabe	48	Tag / Nacht	76
Lagealarm	49	Upstream-Kanal	58
Lokalisierungsbereich	50	Zeitalarm	60
Manual Shift selection	76	Zurücksetzen	67
Manueller alarm	51	Synchronisation PTP domain	29
Nachricht senden	80		
Nachrichtenformat	75	<b><u>W</u></b>	
Nachrichtenprotokoll	81	Web browser	
Netzwerk-baum	86	Connection	19
Netzkennung	28	Log in	20
Notruf	52	Log out	20
Pagergruppen	60		
Passwort	69	<b><u>Z</u></b>	
Rangfolge der Wartungsnachrichten	89	Zentrale upgrades	98
Reißleine	54		





FM 20122

Document Part Number: 9262-0119  
Issue Number: I

**Multitone Elektronik International GmbH,**  
Roßstr. 11,  
40476 Düsseldorf,  
Germany

[www.multitone.de](http://www.multitone.de)

Multitone Electronics plc is part of Kantone Holdings Ltd.

**Registered in England & Wales No. 256314**  
**Registered VAT No.: GB232150709 ©**

[www.multitone.com](http://www.multitone.com)

Registered office:  
© **Multitone Electronics plc**, Multitone House  
Shortwood Copse Lane, Basingstoke  
Hampshire, England  
RG23 7NL