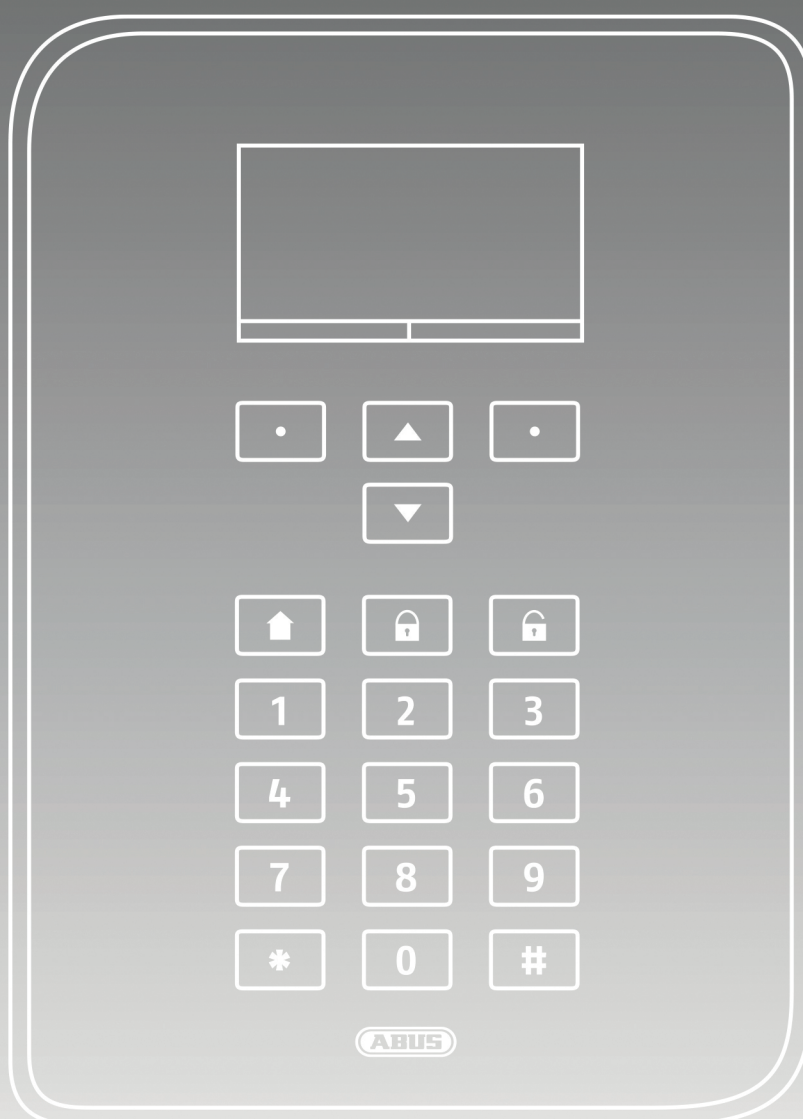


SECVEST

Installer manual



Deutsch

Diese Bedienungsanleitung enthält wichtige Hinweise zur Inbetriebnahme und Handhabung.

Achten Sie hierauf, auch wenn Sie dieses Produkt an Dritte weitergeben.

Eine Auflistung der Inhalte finden Sie im Inhaltsverzeichnis mit Angabe der entsprechenden Seitenzahlen.

English

These user manual contains important information for installation and operation.

This should be also noted when this product is passed on to a third party.

A list of contents with the corresponding page number can be found in the index.

Français

Ce mode d'emploi appartient à de produit.

Il contient des recommandations en ce qui concerne sa mise en service et sa manutention.

Vous trouverez le récapitulatif des indications du contenu à la table des matières avec mention de la page correspondante.

Nederlands

Deze gebruiksaanwijzing hoort bij dit product.

Er staan belangrijke aanwijzingen in betreffende de ingebruikname en gebruik, ook als u dit product doorgeeft aan derden.

U vindt een opsomming van de inhoud in de inhoudsopgave met aanduiding van de paginanummers.

Dansk

Denne manual hører sammen med dette produkt.

Den indeholder vigtig information som skal bruges under opsætning og efterfølgende ved service.

Indholdet kan ses med sideanvisninger kan findes i indekset.

Contents

Quick start guide	7
Target audience	7
Installing Secvest	7
Configuring Secvest	7
Secvest function test	7
Safety information	8
Explanation of symbols	8
Intended use	8
General	8
Power supply	9
Wireless operation	10
Mounting location of the alarm panel	10
Device overview	11
Device front	11
International key assignment	12
Device rear (mounting plate)	13
Introduction	15
Terms and definitions	15
Mounting/Installation	21
Connection overview, terminal block	21
Fixing the mounting plate to the wall	23
Positioning the wireless alarm system (alarm panel)	23
Fixing the mounting plate	23
Connecting the components	24
Installing the optional GSM (FUMO50000)	24
Installing the micro SD card	24
Final steps	24
Commissioning	25
Initial commissioning/factory reset	25
For a system that is already installed	25
Logging into the wireless alarm system	26
Configuration	27
Notes	27
Menu structure	27
Menu control elements	29
Login screen	30
Main menu	31
INFO	33
Panel	33
Communications	34
Status	37
Devices	38
Detectors	38
Control Devices	50
Adding control devices (alarm panel only)	50
Outdoor (external) sirens	52
Info module/indoor siren	54
WAM (Wireless Accessory Module)	55
Door Locks	57
Outputs	58
Radio Outputs	58

Wired Outputs.....	59
Partitions.....	69
Configuring partitions.....	70
Full Set.....	70
Configuring partitions.....	77
Part Set.....	77
Configuring partitions.....	85
HUA response	85
System	87
General	87
Installer details.....	91
User access.....	92
User reset	95
Confirmation	97
Hardware	99
Security settings	101
Backup/restore	108
Panel upgrade	109
Communications	110
Network.....	110
Email setup	111
VoIP dialler setup	112
ARC reporting.....	113
ARC Reporting, Phone Book.....	114
ARC Reporting, Account Numbers.....	115
ARC Reporting, Fast Fmt Channels (for "Fast Format" protocol only).....	116
ARC Reporting, CID/SIA Events (for all protocols EXCEPT "Fast Format").....	117
ARC Reporting, More	118
Social Care	121
Social Care, Phone Book	123
Social Care, Account Numbers	124
Speech Dialler	125
Speech Dialler, Triggers	126
Speech Dialler, Destinations	127
SMS	128
SMS, Triggers.....	129
SMS, Destinations	130
SMS, Destinations, Message	131
SMS, Destinations, Message, Telephone Recipients	132
SMS, Messages	133
SMS, PSTN SMS	134
Email.....	136
Email, Triggers	137
Email, Destinations.....	138
Email, Messages	139
Communication options.....	140
Contacts.....	143
Social Care	144
Test (only available on alarm panel)	145
View Log	152
Virtual keypad.....	153
Appendix.....	154
Technical data	154
Email error messages.....	157
TCP/IP error messages	158
Overview of the SSL-relevant messages	158

Contents

VoIP error messages160

Time zones161

Landline notification centre161

GSM network notification centre162

 SMS notification162

Email notification/email setup163

Index.....167

Quick start guide

Target audience

The instructions for installers aim to help navigate the individual menus of the program interface.

These instructions are aimed at trained technicians that have taken an ABUS Security-Center GmbH & Co. KG seminar and acquired the necessary fundamental knowledge about the following:

- Installing the wireless alarm system.
- Installing peripheral devices for the wireless alarm system (e.g. detectors, sirens, GSM/GPRS module, surveillance cameras).
- Configuring peripheral devices for the wireless alarm system.

These instructions for installers provide an overview of the setting options in the individual menus.

Installing Secvest

The installation of the Secvest wireless alarm system is described in chapter Mounting/Installation from page 21.

Additional information can be found in the document supplied in the scope of delivery, "Quick Guide FUAA50000".

The installation/user manual can also be downloaded as a PDF document.

Link to download the document:

www.abus.com/ger/products/FUAA50000

Configuring Secvest

The configuration of the wireless alarm system is described in chapter Configuration from page 27.

Secvest function test

After installation and configuration, perform a complete function test for all systems and components.

Train the user in the basic operation of the system:

- Logging in/out.
- Arming/disarming the system.
- Operating the Secvest and remote control.
- Create a handover log.







Note

Follow the instructions in user training in the appendix.

Safety information

Explanation of symbols

The following symbols are used in this manual and on the device:

Symbol	Signal word	Meaning
	Caution	Indicates a risk of injury or health hazards.
	Caution	Indicates a risk of injury or health hazards caused by electrical voltage.
	Important	Indicates possible damage to the device/accessories.
	Note	Indicates important information.

The following conventions are used in the text:

	Meaning
1. ...	Required action to be carried out in a set order
2. ...	
• ...	List without a set order, given either in the text or warning notice
• ...	

Intended use

Only use the device for the purpose it was designed and built for. Any other use is not considered to be the intended use.

This device may only be used for the following purpose(s):

- intruder alarm system, alarm system.

General

Before using this device for the first time, please read the following instructions carefully and observe all warning information, even if you are familiar with the use of electronic devices.



Caution

All guarantee claims are invalid in the event of damage caused by non-compliance with these instructions.

We cannot be held liable for resulting damage.



Caution

In the event of personal or material damage caused by improper operation or non-compliance with the safety information, we cannot be held liable.

All guarantee claims are void in such cases.

Retain the accompanying quick start guide for future reference.

If you sell or pass on the device on to third parties, you must include this quick start guide with the device.

This device has been manufactured in accordance with international safety standards.

Power supply

- To prevent a fire risk or risk of electric shock, do not expose the alarm panel or the components to rain or other sources of moisture.
- Do not commission the device near bathtubs, swimming pools or areas where water is splashed around.
- Do not alter the device.
- Discontinue use of damaged devices or accessories.
- Using the device for purposes other than those described may damage this product and may also lead to hazards such as short circuits, fire or electric shock.



Note

Connection to the public electrical grid is subject to your country's specific regulations.
Please seek information on these regulations before connecting the product to the public grid.

- If the device is brought into a warm environment from a cold environment, condensation may form on the inside of the device. In this case, wait about an hour before commissioning the device.
- Disconnect the device from the power supply before carrying out maintenance or installation work.



Caution

Alterations or modifications to the device invalidate the guarantee.



Caution

The alarm panel is supplied power via an integrated power supply unit.

The power supply unit is connected to the building's 230 V AC grid via a separately secured line.

Connection to the building's grid is subject to the country's specific regulations.

The backup power supply is ensured through an internal battery.

Always replace fuses with fuses of the same type, never higher.



Caution

Mount the device safely to a dry point in the building.

Ensure there is sufficient ventilation for the alarm panel.

Do not expose the alarm panel to temperatures below 0 °C or higher than 50 °C.

The alarm panel is designed for indoor use only.

The maximum humidity must not exceed 90% (non-condensing).

Ensure that no metal objects can be inserted into the alarm panel from the outside.

Disconnect the alarm panel from the power supply before any work is carried out on the device.



On alarm panels in general

Incorrect or unclean installation work may lead to erroneous interpretation of signals and therefore false alarms.

The operator is liable for any costs incurred for involving rescue services such as the fire brigade or police.

For this reason, read these instructions carefully and ensure that lines and components used are labelled precisely when the system is installed.

Wireless operation



Note

No wireless licence is required for Secvest and its components.

The send/receive properties could be affected by other signals (e.g. DECT telephones, WLAN).

The wireless devices in this system have been tested by an independently accredited laboratory for R&TTE certification.

Mounting location of the alarm panel



Note

The alarm panel should be positioned in a safe place out of sight of possible intruders and easily accessible to the operator.

The alarm panel should be mounted on a flat surface in order to ensure that the back of the device cannot be tampered with when the alarm panel is mounted.

The alarm panel should be mounted at a comfortable height (between 1.5 and 2 m).



Note

If small children are present, the alarm panel should be mounted out of their reach.



Note

Position the alarm panel so that signal tones can be heard even outside of the area being monitored.

The alarm panel should be positioned within a monitored zone so that an unauthorised person would have to enter a monitored area first before gaining access to the panel when it is armed.

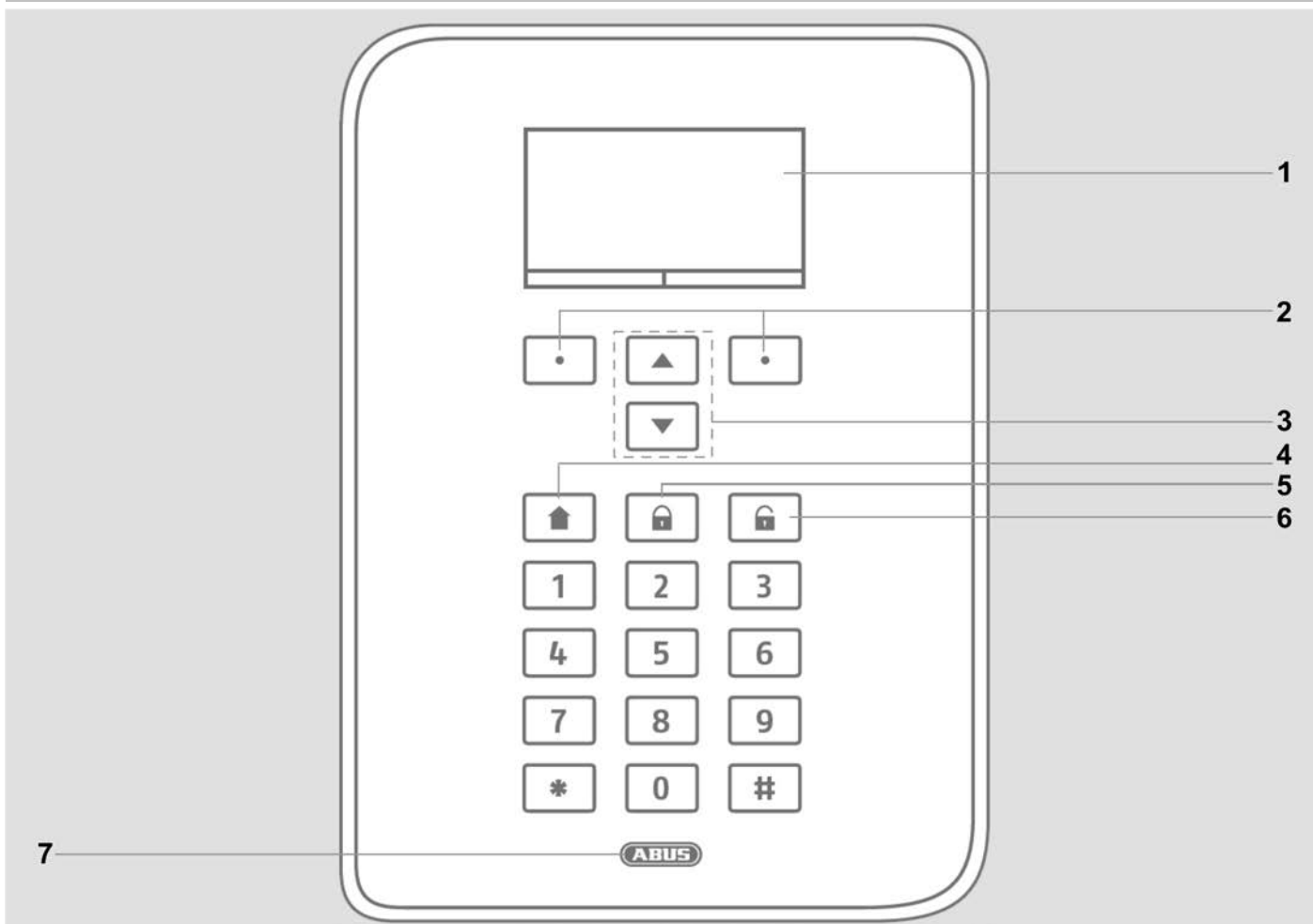
The alarm panel should be mounted near a socket or power supply.

If a telephone dialler is used, the alarm panel must be connected to a telephone connection.

The alarm panel should be mounted at least 1 metre away from metal objects (e.g. mirrors or radiators).

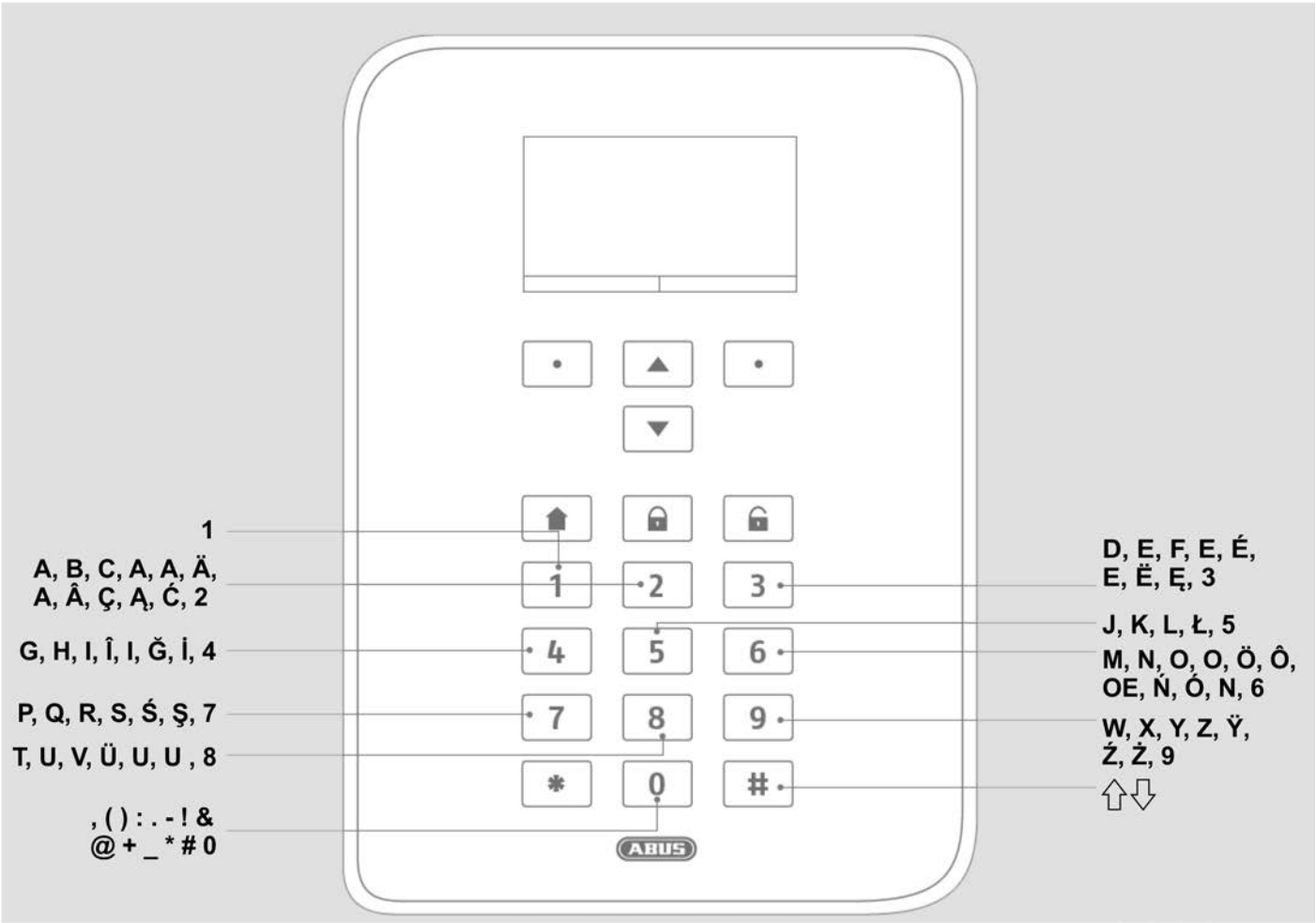
Device overview

Device front

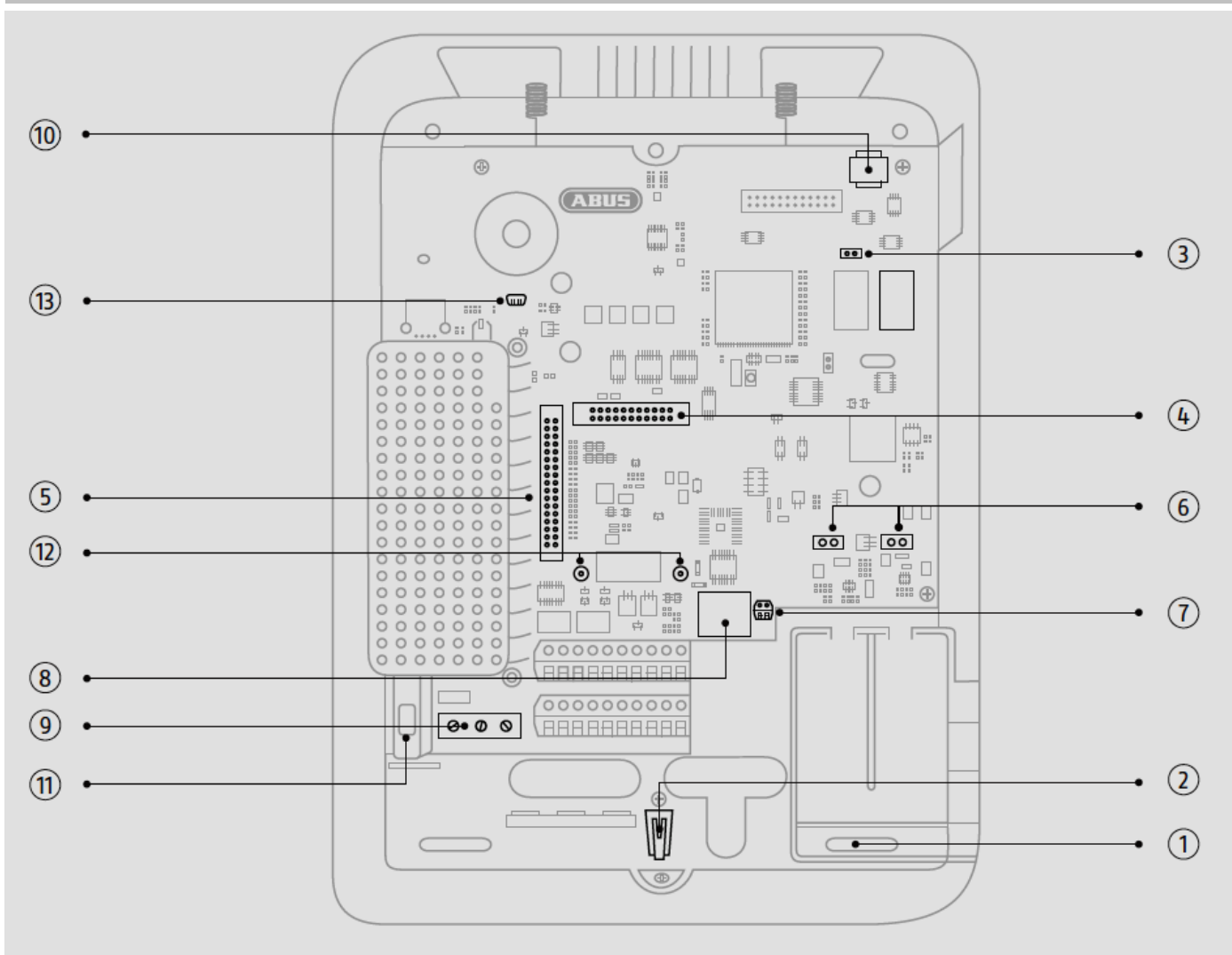


No	Name/function	No	Name/function
1	Status display Display of status and menus	5	Arm button Monitoring of all available areas is activated (device armed).
2	Confirmation buttons Used to navigate to a higher/lower menu level or to select options or to exit a menu	6	Disarm button Monitoring is deactivated (device disarmed).
3	Navigation buttons Used to navigate up/down	7	Proximity reader Reader for the proximity keyfob. Hold the keyfob in front of the ABUS logo.
4	Internal arm button Perimeter monitoring is activated (device armed internally).		

International key assignment



Device rear (mounting plate)



No	Name/function	No	Name/function
1	Mounting opening for screws	8	Connection for LAN cable
2	Housing tamper switch	9	Connection for mains voltage 110 V/230 V AC 50/60 Hz
3	Code reset PINs	10	Micro SD card holder
4	Connection for optional GSM module (FUMO50000)	11	Fuse holder for mains fuse
5	Connection for ribbon cable	12	Holes for plastic holder for optional GSM module
6	Connections for battery pack	13	USB mini-B
7	Analogue telephone connection		

Introduction

Terms and definitions

Alarm system

Common term for a burglar alarm system or danger alarm system.

Alarm type

Alarm systems may have the following alarm types: internal, local, external or silent.

Danger detector

Device that sends a message to the alarm panel when a certain event occurs (e.g. movement, glass breakage, vibrations).

Sounder

Device that sends an alarm message acoustically (siren) or visually (strobe). Even diallers are sounders.

Alarm zone

A detector (wireless) or detector group (wired) is monitored via each zone and can be programmed separately.

Alarm panel

The switching panel of the entire alarm system, which processes all information, forwards it and responds as necessary.

Arming, disarming

"Activation" of the alarm panel – the panel triggers an alarm if an intrusion is detected (e.g. a door is opened); "deactivation" of the alarm panel – the panel does not trigger an alarm if an intrusion occurs. Danger detectors are programmed differently: if smoke is detected, for example, an alarm is triggered even if the alarm panel is disarmed.

Active intrusion protection

Even an attempt to break in is reported. This can be done using alarm components that not only combine state-of-the-art wireless technology with effective mechanical intrusion protection (mechatronic detectors), but also monitor attempts to open a door or window using a lever via innovative magnetic field sensors.

Perimeter protection

All points of access to the premises are monitored, including house doors, terrace doors, cellar doors, skylights and all windows. Usually magnetic contacts, glass breakage detectors and wireless window/door locks are used. The building's occupants can still move around freely within the building when the alarm system is armed internally.

External siren

Sounder for outdoor use, usually designed as a combination sounder (siren + strobe).

End of line (EOL)

End point of the line system, end point of access to telephone network.

The line end point or "building distribution for telephone lines" is the end of the distribution cable for the consumer connection line within the telephone network.

User

Different users of the alarm system (e.g. owners, tenants) can be assigned separate rights and user codes.

User guidance

Electronically guided help for operating the alarm panel.

Motion detector

Detector used to identify people by thermal movement (PIR), ultrasound (US) or microwave/radar (MW).

Bidirectional 2-way wireless (2WAY)

Unidirectional: components (e.g. remote control) and control modules only transmit commands to the alarm panel. Bidirectional: components can both receive the feedback from the alarm panel and evaluate it (e.g. via LED displays).

BS8243

British standard BS8243 describes a set of methods for reducing false alarms generated by intruder and hold up alarm systems.

Chip key/proximity keyfob/Prox Tag

Electronic "key" for quick access to the building without code entry.

CLIP

Calling Line Identification Presentation

Coding of wireless signals

Ensures secure transmission of signals without manipulation or tampering between the alarm panel and its components.

Contact ID, CID

Protocol for transmitting data to an ARC (alarm receiving centre).

DD243

British requirement for sequential alarm confirmation.

DHCP

The Dynamic Host Configuration Protocol (DHCP) is a communications protocol in computer technology. It facilitates the assignment of the network configuration to clients through a server.

DHCP makes it possible to automatically integrate a computer into an existing network without having to configure it manually. The client usually only has to be set to obtain the IP address automatically. When the computer starts on the network, it is automatically assigned an IP address, subnet mask, gateway and DNS server by the DHCP server. Without DHCP some additional settings are required depending on the network to which the computer is connecting.

Display

Display field on the alarm panel for operating and configuring the panel.

DNS

The Domain Name System (DNS) is one of the most important services in many IP-based networks. Its main task is to respond to name conversion requests.

The DNS works like a telephone directory enquiries centre. The user knows the domain (the "friendly" computer name on the IP network), such as "example.org". The user sends this domain as the query. The URL is then converted by the DNS into the associated IP address (the "connection number" on the IP network), e.g. an IPv4 address in form 192.168.2.21 and directs it to the correct computer.

Double end of line (DEOL)

Wiring version for wired alarm systems; wired zones also take on this configuration.

Wired detector

Alarm and danger detectors that are connected via wire to the alarm panel.

Wired zone, wired alarm zone

Alarm zone monitored via one or more wired detectors (usually switched in series).

DTMF

Dual Tone Multi-Frequency

The multi-frequency dialling method is commonly used by analogue telephone systems.

Intruder alarm system, burglar alarm system

Alarm system that detects an intrusion and triggers an alarm.

Individual identification of detectors

Makes it possible to determine exactly which detector has triggered (see also wireless alarm zone).

EN 50131

European standard for alarm systems, "Intrusion and hold up systems"

External alarm

(Alarm type)

Alarm to which all sounders (internal and external) respond when triggered. An alarm receiving centre is also notified of the event.

Shock detector

This detector identifies vibrations that occur when an attempt to break in is made.

Fast Format, FF

Protocol for transmitting data to an ARC (alarm receiving centre).

Remote access/remote configuration

Servicing/configuration of the alarm panel from outside of the monitored premises (e.g. via the internet).

Wireless alarm system

Alarm system with detectors that are connected to the alarm panel wirelessly (quick and easy installation, high flexibility).

Wireless alarm zone, wireless zone

Zone of the wireless alarm panel that is used to identify and monitor every individual wireless detector.

Wireless control device

For convenient arming/disarming of the alarm panel, e.g. in another room (in entrance area etc.) The status can be queried if a bidirectional wireless control device is used.

Wireless window lock/wireless door lock

Combination of mechanical lock and electronic detector. Pry-attempt monitoring is also possible. i.e. even attempts to break in are detected.

Wireless remote control

For convenient arming/disarming of the alarm panel, status query, emergency alarm, etc. regardless of the user's location.

Wireless detector

Alarm and danger detectors that are connected wirelessly to the alarm panel.

Wireless key switch

For convenient arming/disarming of the alarm panel without code entry (by key).

Wireless range

The max. distance between the alarm panel and wireless detector varies depending on the properties of the building.

Glass breakage detector

These detectors respond to breaking glass. There are passive, active and acoustic glass breakage detectors.

Danger alarm system

Alarm system that triggers an alarm for additional dangers/emergencies as well as intrusion.

Protected outdoor area

Area outside of the buildings that is protected from heavy rain (e.g. a covered entrance area or terrace).

GSM

Global System for Mobile Communications (previously Groupe Spéciale Mobile), a standard for fully digital wireless mobile networks, mainly used for telephony but also for line and packet-based data transmission and short text messages (SMS).

HTTPS

HyperText Transfer Protocol Secure, a communications protocol on the web, used to transfer data securely.

HTTPS is used online to establish confidentiality and integrity in communications between web server and web browsers (clients). This is achieved through encryption and authentication.

Without encryption, data transmitted over the internet can be read as plain text by anyone who has access to the corresponding network.

IMEI

International Mobile Station Equipment Identity, a unique 15-digit serial number which can be used to uniquely identify each GSM or UMTS end device.

IMSI

International Mobile Subscriber Identity, used in GSM and UMTS wireless mobile networks to uniquely identify network subscribers (internal subscriber identification). In addition to other data, the IMSI is saved on a special chip card known as a SIM (Subscriber Identity Module). The IMSI number is uniquely assigned worldwide to each customer by the wireless mobile network operators. The IMSI has nothing to do with the telephone number assigned to the SIM card.

Indoor siren

Sounder for indoor use, usually a purely acoustic sounder (in addition to outdoor sirens).

Interior protection

The indoor area of the premises is protected here, especially areas that an intruder most likely has to enter; motion detectors and light barriers are usually used here.

Installation

Mounting of the alarm panel and components, including commissioning.

Internal alarm

Alarm sounds only within the building. The outdoor sirens do not sound.

Intuitive operation

Easy operation of a device using a menu that is logical from the point of view of the user.

IP

Internet Protocol, a network protocol widely used in computer networks.

Jamming

Interference that makes normal reception of wireless emissions of electromagnetic waves difficult or impossible. The source of interference sends out energy in the form of electromagnetic waves, just like the instruments affected by the interference, which overlap the original waves either partially or completely.

Combination signalling device

Combined sounder, e.g. siren (acoustic signal) + strobe (visual signal).

Communication options

Used to transmit alarm notifications using additional routes, e.g. wirelessly (GSM module) for voice/text messages or digital protocols.

Devices

See system components

Receiving centre

See ARC

Line

Another term for zone, mainly used in wired areas.

Local alarm

(Alarm type)

If this alarm is triggered the sounders indoors and outdoors sound (outdoors the acoustic alarm (siren) must stop after 3 minutes if in Germany, but the visual alarm (strobe) can remain on).

MAC

The MAC address (Media Access Control, Ethernet ID) is the hardware address of every single network adaptor, used to uniquely identify the device in the network.

Medical emergency

Personal medical emergency, for which help can be arranged using an alarm.

NC

Normally Closed; contact or switch that opens when actuated.

NO

Normally Open; contact or switch that closes when actuated.

Alarm and relay command centre

See ARC.

ARC

Receiving centre; in an alarm receiving centre, messages collected in connected subscriber zones, e.g. from danger alarm systems or building technical equipment, are transmitted, received, documented and processed, and intervention is provided, via the power supply of the network operator (leased lines), the public telephone network, Datex-P/X.25/X.31, IP, GSM, ISDN, or in Switzerland, via TUS (Alarmnet). Receiving centre from private security service providers also control call for intervention services (police/fire brigade).

Magnetic contact

A detector that identifies when a window, door, shutter, garage door, etc. is opened.

Perimeter surveillance

Continuous monitoring of large areas of open land around the periphery or the areas used for approaching the property, e.g. using light barriers and motion detectors on the premises and/or surveillance cameras with intelligent motion detection.

Port

Part of a network address.

Configuration

Detailed settings for the alarm panel according to the user's requirements (e.g. zones/sub-areas can be defined).

PSTN

Public Switched Telephone Network, analogue, a/b

Smoke alarm device

Optical smoke alarm devices save lives, as they respond to smoke particles in the air (usually poisonous gases). Heat detectors/heat difference detectors respond to a maximum temperature (e.g. 65°C) or a rapid increase in temperature.

Relay outputs

Switching outputs for external devices (lighting control, electric shutters, other sounders, etc.)

Sabotage, tamper protection, tampering

So that the alarm panel and its components cannot be tampered with, each component is monitored for tampering. Opening a detector and disconnecting cables ALWAYS triggers an alarm. The components are usually protected by a cover contact (alarm when detector is opened) and an anti-removal wall contact.

Scancom

A social care alarm protocol.

Scancom is the same as Scanfast, except for channel 8. Channel 8 in this case is used to establish a 2-way voice connection between the alarm panel and the alarm receiving centre.

Scanfast

A social care alarm protocol.

Scanfast is the same as Fast Format, except that in this case only channel 2 (social care alarm) and channel 3 (inactivity) are used. Channels 1, 4, 5, 6, 7, 8 are always "5" (unused).

Arm, disarm

Activating/deactivating the alarm panel.

Arm components

Devices that can be used to arm/disarm the alarm panel (e.g. remote control, key switch, control device).

Security frequency band

(868 MHz)

This frequency range is approved by the authorities for the security field. Signals from wireless earphones, mobile phones, garage door openers, etc. cannot interfere with devices operating in these ranges.

Europe: frequency use specification of the European Conference of Postal and Telecommunications Administrations (CEPT)

Germany: Bundesnetzagentur (BNetzA) – Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway

Austria: the frequency use plan is published by the Federal Ministry for Traffic, Innovation and Technology

Switzerland: the frequency use plan is set out in the Swiss National Frequency Assignment Plan (NaFZ) and published by the Federal Office of Communications

Seismic sensor

See shock detector.

Server

A program that waits for contact from a client in order to perform a certain service.

SIA

Protocol for transmitting data to an ARC (alarm receiving centre).

SIA-IP (DC-09)

An IP-based protocol for transmitting data (e.g. FF, SIA or CID) to an ARC.

Sounder

Sounder that triggers an alarm when it receives a corresponding command from the alarm panel (siren, strobe, etc.)

SIM

Subscriber Identity Module, a chip card for mobile telephones

SMS

Short Message Service, text message; a telecommunications service for transmitting text messages, first developed for GSM wireless mobile networks and now available on landlines as well.

SMSC

Short Message Service Centre

F-SMSC = SMSC for landlines

SMTP, SMTP server

Simple Mail Transfer Protocol

An internet protocol used to exchange email in computer networks.

It is mainly used to send and forward email.

Other specialised protocols such as POP3 or IMAP are used to retrieve messages.

SMTP servers use conventional connections to port 25 ("smtp"). Newer servers also use port 587 in order to receive mail for authenticated users that must be sent to other mail servers ("submission").

Speech dialler

Component in the alarm panel for transmitting voice messages. The alarm information is transmitted in plain text. The text to be transmitted is recorded using a microphone on the alarm panel.

SSL

Secure Sockets Layer, a network protocol for the secure transmission of data.

Transport Layer Security (TLS), widely known under its previous designation, Secure Sockets Layer (SSL), is a hybrid encryption protocol for secure data transmission on the internet. Since version 3.0, the SSL protocol has been further developed and standardised under the new name TLS, where version 1.0 of TLS corresponds to version 3.1 of SSL.

TLS encryption is mainly used today with HTTPS. Most web servers support TLS 1.0, and many also support SSLv2 and SSLv3 with a number of encryption methods.

Status

Alarm panel status: armed, internally armed or disarmed.

Status feedback

Feedback from the alarm panel to a module (arm component, info module, etc.) about its current status.

Status query

Query sent to the alarm panel about the system status (e.g. by pressing the button on the wireless remote control).

Silent alarm

(Alarm type)

This alarm does not trigger any sounders (indoors and outdoors remains quiet and calm), but an alarm receiving centre is discreetly notified (intruder is not scared off, rather caught in the act, aggressive intruders are not provoked, etc.)

Supervision

The alarm panel monitors whether detectors are present and active. The components report approx. every 4 min. The alarm panel responds if it fails to receive status messages over a longer period of time.

TAE

The Telekommunikations-Anschluss-Einheit (telecommunications connection unit) is a type of connector used in Germany for telephone connections.

It is used as a connection to the public telephone network or as an a/b interface for analogue telephone connections to additional devices.

Tampering

See sabotage.

TAP

Telocator Alphanumeric Protocol, a transmission protocol for SMS messages

Technical damage

For example, water damage or escaped gas (protection against these things is only provided by special danger detectors).

Partitions

An alarm system can be divided into sub-areas (partitions), each of which functions separately as an individual alarm system.

Each partition (e.g. apartment, workshop) can be operated and configured separately and can contain any number of zones/detectors.

Telephone dialler

Device used to send alarm messages from a alarm panel by telephone line. Telephone diallers can be integrated in alarm panels or added as additional components.

Tunstall

A social care alarm protocol.

Overlapping signal

See jamming.

UCP

Universal Computer Protocol

VdS

Verband der Schadensversicherer (German Association of Insurers against Loss or Damage); defines guidelines for different safety and security levels.

VDS-A for the non-commercial sector

VDS-Home for home risk management systems

VDS-B for the commercial sector

VDS-C for banks and jewellers (high-risk commercial entities)

Flood detector

For detecting water damage and flooding, consisting of a basic device and water sensor. The sensor is always mounted at a point where flooding would first start to incur water damage.

Certifications

Inspection seal from an independent body that ensures the high quality and safety of alarm systems (in Germany the following are relevant: certification as per POS in accordance with accident prevention regulations and VdS loss prevention)

Zone

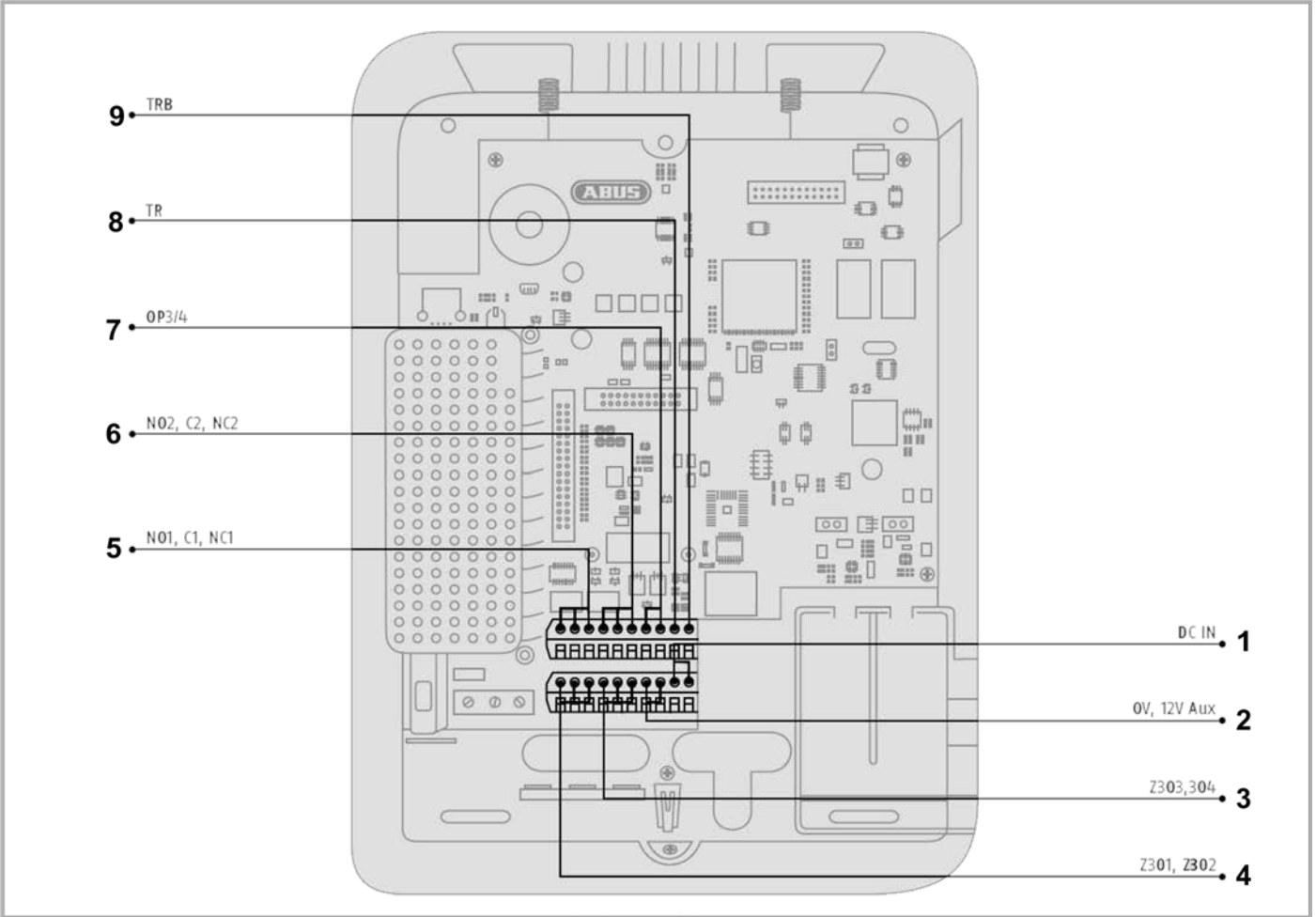
Another term for a line. Describes a closed circuit to which alarm or tamper contacts are connected, which are then connected to the alarm panel. With wireless zones usually one zone is used per detector.

Force Set

Zones with this attribute, if opened, are automatically omitted when the alarm system or a partition is armed.

Mounting/Installation

Connection overview, terminal block



No	Name/function	No	Name/function
1	DC IN 13.8 V +: connection for voltage supply 13.8 V	6	NO2, C2, NC2 – relay output 2: potential-free relay contact, 30 V DC, 24 V AC rms, 500 mA

Mounting/Installation

2	0 V, 12 V aux: voltage output 13.8 V	7	OP3/4 – transistor outputs: for a wired sounder, strobe and audio alarm signalling device Open drain transistor output 500 mA 13.8 V DC
3	Z303, Z304: wired zones 303 and 304	8	TR – tamper return: tamper input from a wired sounder
4	Z301, Z302: wired zones 301 and 302	9	TRB – trouble: malfunction indication input from a wired sounder
5	NO1, C1, NC1 – relay output 1: potential-free relay contact, 24 V AC rms/500 mA		

Fixing the mounting plate to the wall

Positioning the wireless alarm system (alarm panel)



Note

The alarm panel should be positioned in a safe place out of sight of possible intruders and easily accessible to the operator.

The alarm panel should be mounted on a flat surface in order to ensure that the back of the device cannot be tampered with when the alarm panel is mounted.

The alarm panel should be mounted at a comfortable height (between 1.5 and 2 m).



Note

If small children are present, the alarm panel should be mounted out of their reach.



Note

Position the alarm panel so that signal tones can be heard even outside of the area being monitored.

The alarm panel should be positioned within a monitored zone so that an unauthorised person would have to enter a monitored area first before gaining access to the panel when it is armed.

The alarm panel should be mounted near a socket or power supply.

If a telephone dialler is used, the alarm panel must be connected to a telephone connection.

The alarm panel should be mounted at least 1 metre away from metal objects (e.g. mirrors or radiators).

Fixing the mounting plate



Caution

The alarm panel is supplied power via an integrated power supply unit.

The power supply unit is connected to the building's 230 V AC grid via a separately secured line.

Connection to the building's grid is subject to the country's specific regulations.

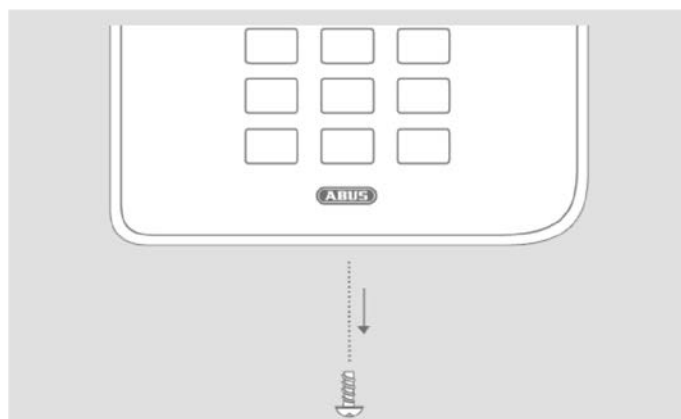
Ensure that the supply line is disconnected from the power and secured against being reconnected.



Caution

Ensure that there are no lines in the wall of the selected mounting location.

1. Drill the mounting holes into the wall using the drilling template in the quick start guide.
2. Unscrew the screw on the bottom of the housing.



3. Carefully open the housing.
4. Carefully pull the ribbon cable connector out of the terminal block on the PCB.
5. Separate the top part of the housing from the bottom part.



Note

During mounting ensure that the housing tamper switch (1) definitely has contact with the wall. Ensure that the bottom part and the integrated components are not damaged when the screws are tightened and that all screws are screwed in completely.

6. Mount the bottom part of the housing to the wall.
7. Connect the mains connection properly while it is disconnected from the power supply.
8. Install the strain relief clamp.
9. Connect the network cable to the socket on the PCB.
10. Place the battery (or batteries) in the battery compartment.

Connecting the components



On alarm panels in general

Incorrect or unclean installation work may lead to erroneous interpretation of signals and therefore false alarms.

The operator is liable for any costs incurred for involving rescue services such as the fire brigade or police. For this reason, read these instructions carefully and ensure that lines and components used are labelled precisely when the system is installed.

11. Connect all components to the terminal blocks.
12. Ensure that all connections are securely fitted.

Installing the optional GSM (FUMO50000)

If available:

Plug the GSM module (FUMO50000) into the terminal block (CON 7 GSM/GPRS) on the PCB. Ensure that no electronic components are damaged or touched if possible.

(See also the installation instructions for the FUMO50000.)

Installing the micro SD card

1. Insert the SD card into the SD card holder on the PCB if it is not already inserted.
2. Ensure that the SD card is correctly inserted into the card holder.

Final steps

1. Check all connections to ensure they are correct and fitted properly, in order to prevent false alarms.
2. Connect the ribbon cable connector on the top of the device to the terminal block (CON 2) on the PCB.
3. Connect the connecting cable connector of the battery (or batteries) into the connector (BATT1 CON 8, BATT2 CON 9) on the PCB.
4. Carefully close the housing by first hooking the clip at the top and then pressing the housing into the snap points, working downwards.
5. Close the housing with the screw on the bottom of the device.

Commissioning

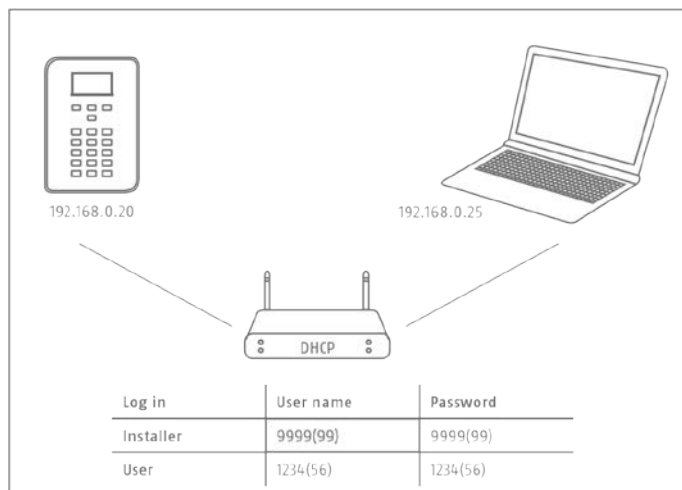
Initial commissioning/factory reset



Note

The wireless alarm system **cannot** be accessed via the web server without running the installation/start wizard.

1. Connect your PC to your customer's network.



2. Switch on the power supply.
3. Follow the installation/start wizard on the alarm panel.
4. Select:
 - the language
 - the country-specific settings
 - a 4 or 6-digit user code
 - the type of wired zone (e.g. 2-wire FSL 2K2/4K7).
5. The overview then displays:
 - the IP address of the wireless alarm system
 - DHCP ON/OFF
 - the current software version
 - the serial number of the wireless alarm system
 - the part number of the wireless alarm system
 - the temporary login data for the installer and administrator.
6. Make a note of the IP address.
7. Open the web browser on your PC and enter the IP address indicated by the alarm panel. Alternatively you can also use the ABUS IP Installer to display the alarm panel and automatically access it. You can download the IP Installer from www.abus.com.

8. Connect to the wireless alarm system via the web browser.



Note

When the alarm panel is first set up, it may take up to three minutes for the web browser to access the wireless alarm system as the SSL certificate is automatically generated during this time.

9. Log into the wireless alarm system as an installer.



Note

It is sometimes beneficial to use a fixed IP address instead of a dynamically assigned IP address (DHCP).
Some routers assign other IP addresses to their clients after a certain time, for example. Other devices do not recognise this new IP address yet.

For a system that is already installed

1. Log into the wireless alarm system as an installer.
2. Navigate to the following submenu:
Info>Communications>Ethernet.
3. Make a note of the IP address.
4. Log out of the alarm panel.
5. Open the web browser on your PC and enter the IP address indicated by the alarm panel.
6. Open the web browser on your PC and enter the IP address indicated by the alarm panel.
7. Enter your user name and password to log onto the web server.

Logging into the wireless alarm system

1. Open the web browser.
2. Enter the IP address in the following form:
xxx.xxx.xxx.xxx.

The browser then switches to https automatically.



Note

If a user (operator, installer) is logged in directly to the wireless alarm system, it cannot be accessed via web browser for security reasons.

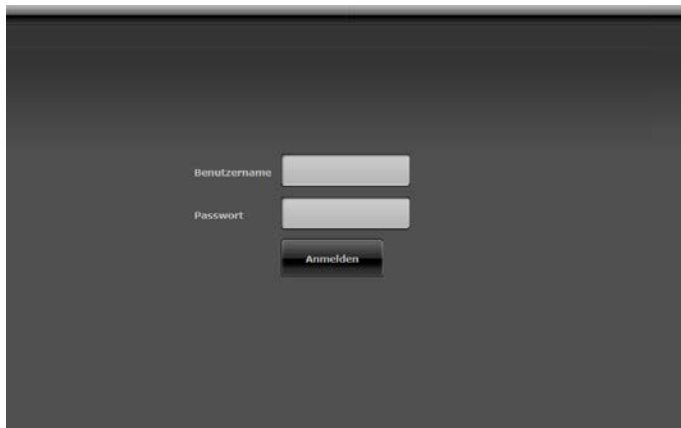


Note

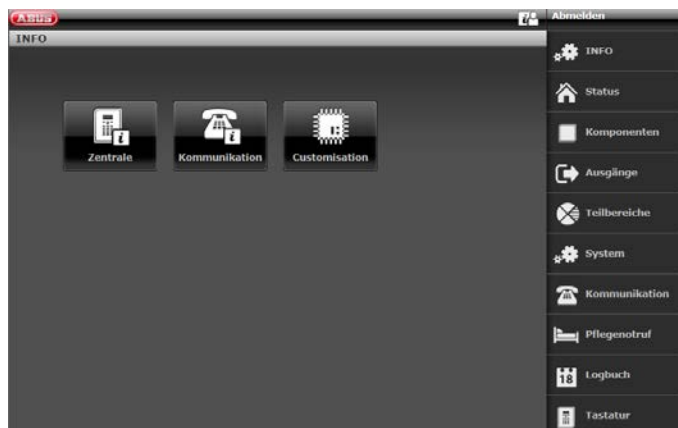
Depending on the browser, a message may appear, indicating that the connection/certificate is unsafe.

Confirm the security exception rule and save it.

3. Load the page. The login screen appears.



4. Log in as an **Installer** with the user name **9999(99)** and password **9999(99)**.
5. Click on the **Login** button or press the **enter key** on the keyboard.
6. The main menu appears:



Configuration

Notes

The wireless alarm panel is configured in installer mode.

There are two ways to configure the wireless alarm panel:

- Directly on the wireless alarm panel using the keypad
- Via a web browser on the integrated web server.

The following mainly describes how to configure the wireless alarm panel via the integrated web server.

The integrated web server can be used to define settings for the wireless alarm system easily using an internet browser.

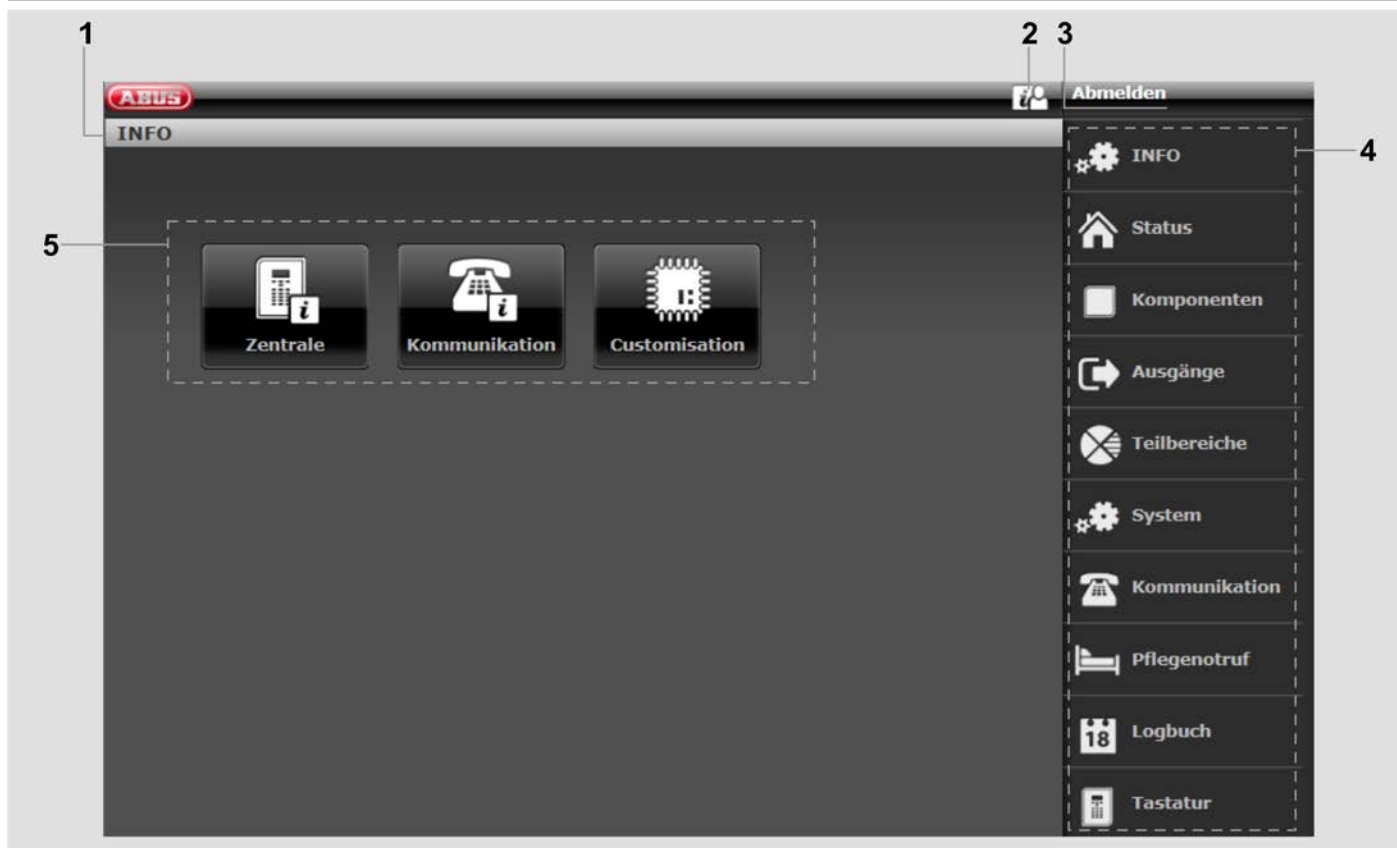
(Wireless) components are set up/taught in directly on the wireless alarm panel (see next chapter, "Setting up components").

Menu structure

Menu structure	27
Menu control elements	28
Login screen	29
Main menu	30
INFO	32
Panel.....	32
Communications.....	33
Status.....	36
Devices	37
Detectors	37
Control Devices	49
Add control devices (panel only)	49
External Sirens	51
Info module/indoor siren	53
WAM (Wireless Accessory Module)	54
Door Locks	56
Outputs	57
Radio Outputs.....	57
Wired Outputs.....	58
Partitions.....	68
Configure partitions	
Full Set.....	69
Configure partitions	
Part Set.....	76
Configure partitions	
HUA response	84
System	86
General	86
Installer Details	90
User Access	91
User Reset.....	94
Confirmation	96
Hardware	98
Security Settings.....	100
Backup/Restore	107
Panel Upgrade.....	108

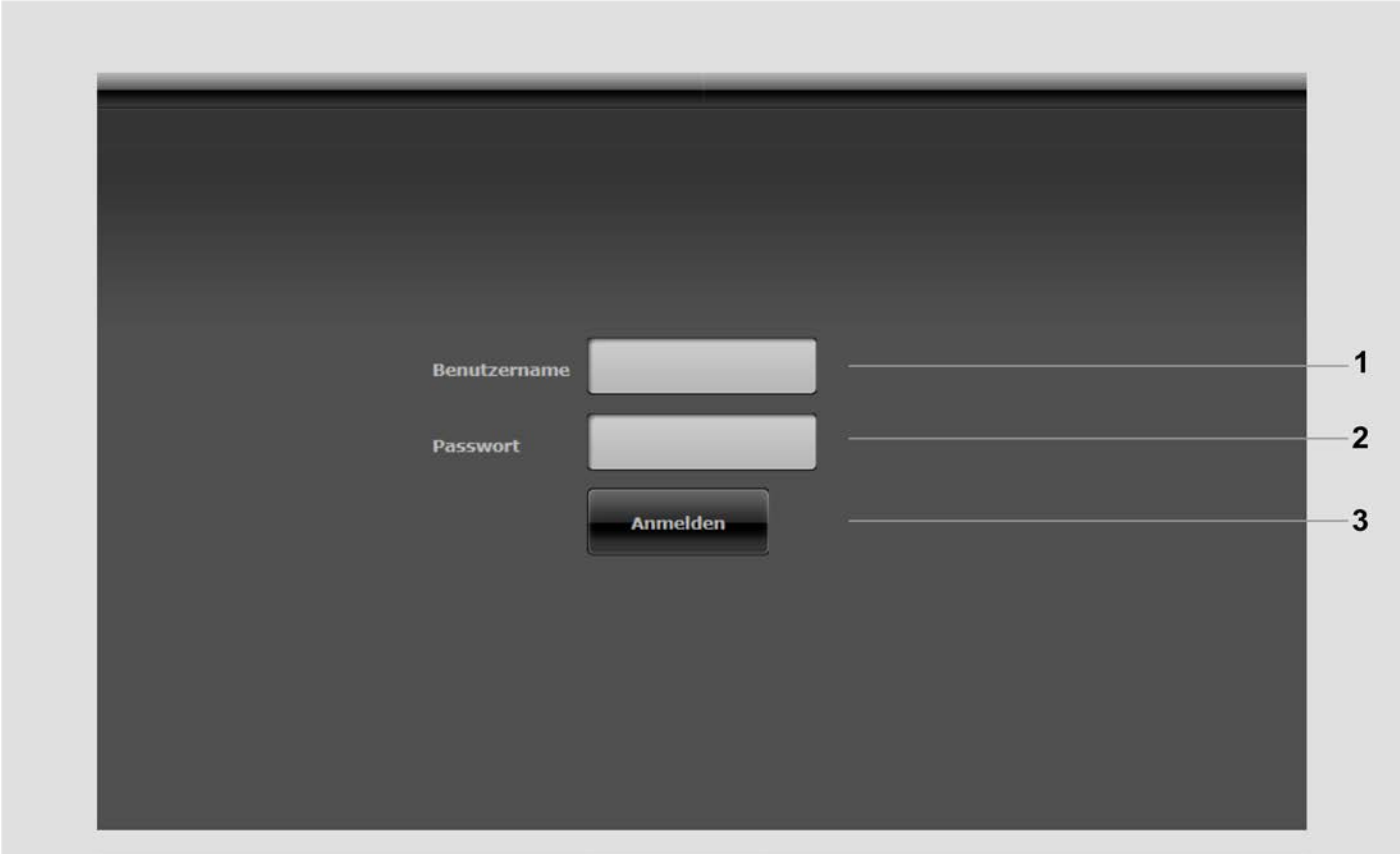
Communications.....	33
Network	109
Email setup	110
VoIP dialler setup	111
ARC Reporting	112
ARC Reporting, Phone Book	113
ARC Reporting, Account Numbers	114
ARC Reporting, Fast Fmt Channels (for "Fast Format" protocol only)	114
ARC Reporting, CID/SIA Events (for all protocols EXCEPT "Fast Format")	116
ARC Reporting, More.....	117
Social Care.....	120
Social Care, Phone Book.....	122
Social Care, Account Numbers	123
Speech Dialler	124
Speech Dialler, Triggers.....	125
Speech Dialler, Destinations	126
SMS.....	127
SMS, Triggers	128
SMS, Destinations.....	129
SMS, Destinations, Message	130
SMS, Destinations, Message, Telephone Recipients	131
SMS, Messages	132
SMS, PSTN SMS	133
Email	135
Email, Triggers	136
Email, Destinations	137
Email, Messages.....	138
Communication options.....	139
Contacts	142
Social Care.....	143
Test (only available on panel)	144
View Log	151
Virtual keypad	152

Menu control elements




No	Name/function	No	Name/function
1	Info bar <ul style="list-style-type: none"> Active main menu – here, "Info" with additional submenus 	4	Main menu list <ul style="list-style-type: none"> The main menus are displayed
2	Button for online help <ul style="list-style-type: none"> Click this button to open the current documentation as a PDF. This documentation can then be saved locally as well. 	5	Submenu list <ul style="list-style-type: none"> The submenus associated with the active main menu are displayed Click on a submenu to open it and access the settings
3	Logout button <ul style="list-style-type: none"> Click this button to log out of the system 		

Login screen

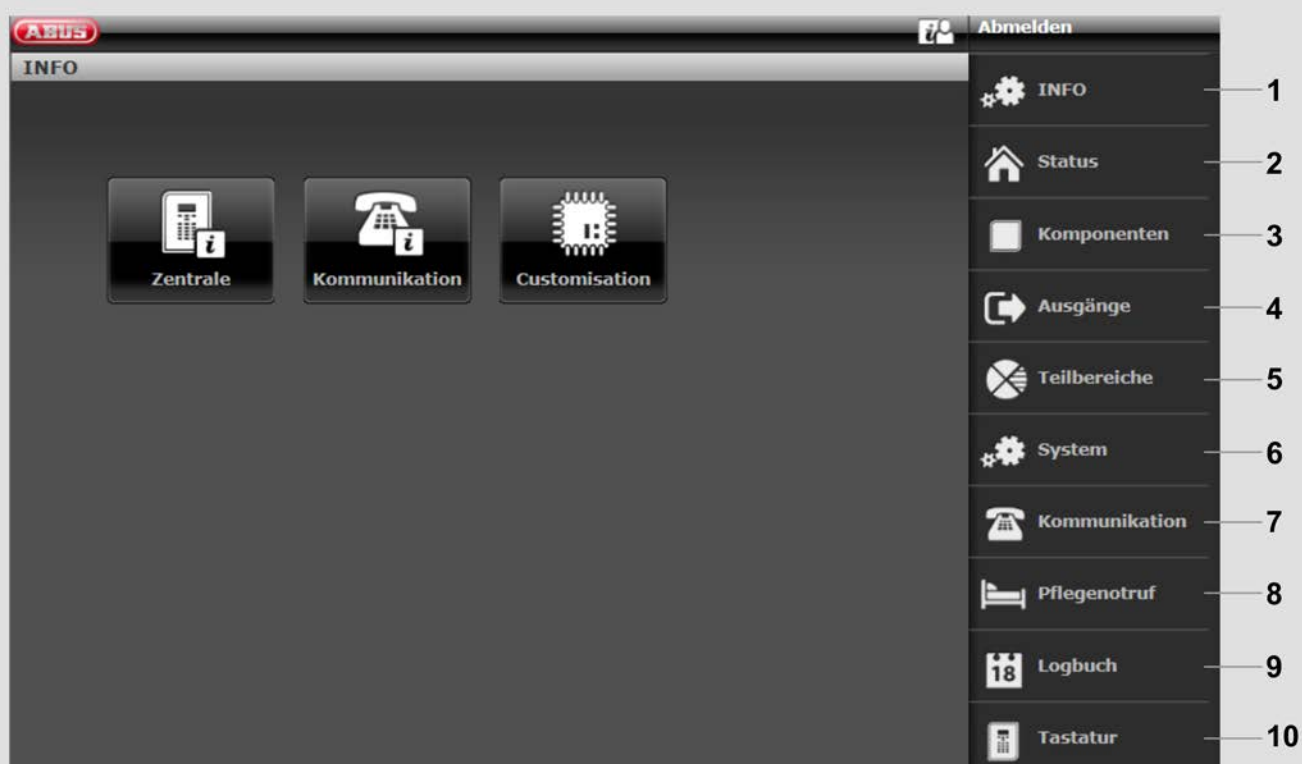


No	Name/function	No	Name/function
1	Input field for the user name <ul style="list-style-type: none">• Enter "999999" or "9999".• The entry is case-sensitive.	3	Login button
2	Input field for the password <ul style="list-style-type: none">• Enter "999999" or "9999" as an installer.• The entry is case-sensitive.		

**Note**

You are automatically logged out after 15 minutes of inactivity.
You must then log in again.

Main menu



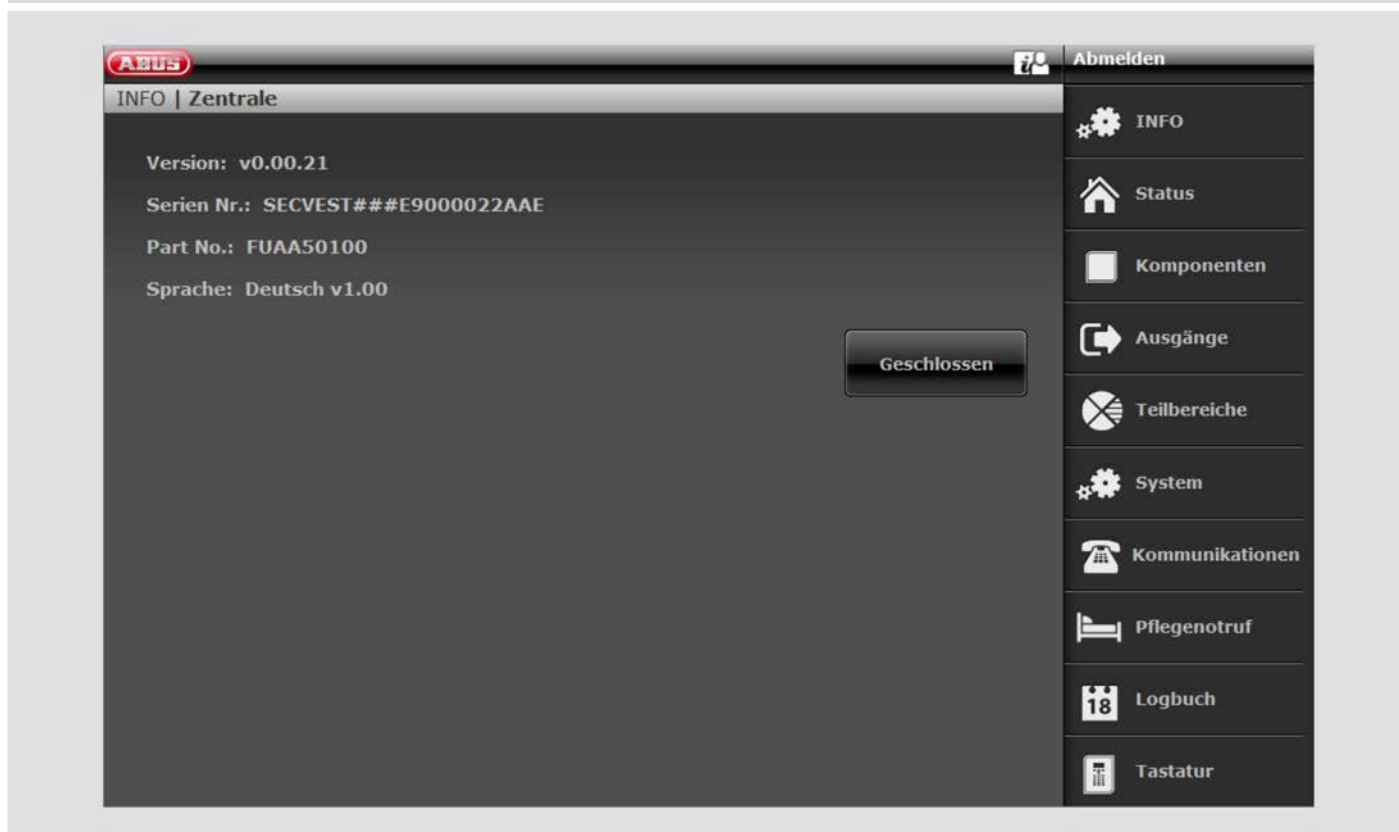
No	Name/function	Pg.	No	Name/function	Pg.
1	INFO General information about: <ul style="list-style-type: none"> • The alarm panel • Communications • Customisation • The software and hardware version 	33	4	Outputs Overview/configuration of the outputs: <ul style="list-style-type: none"> • Wired output • Wireless (radio) output 	58
2	Status Information about the status of the alarm system partitions	37	5	Partitions Overview/configuration of the partitions	69
3	Devices Overview/configuration of the components: <ul style="list-style-type: none"> • IP zones • Wireless Zones • Wired Zones • External sirens, wired sirens • External sirens, wireless (radio) sirens • Info module/indoor siren • WAM • Door Locks 	38	6	System Overview/configuration of the alarm system: <ul style="list-style-type: none"> • General • Installer details • User access • User reset • Confirmation • Hardware • Security settings • Backup/restore • Panel upgrade 	87

Configuration

No	Name/function	Pg.	No	Name/function	Pg.
7	Communications Overview/configuration of the communication interfaces and transmission methods <ul style="list-style-type: none">• Network• ARC reporting• Social Care• Speech Dialler• SMS• Email• Communication options• Contacts	110	9	View Log Overview of faults, events and processes on all components of the alarm system	152
8	Social Care Overview/configuration of social care alarm	121	10	Virtual keypad Virtual Secvest keypad. The virtual keypad can be used to operate the system in exactly the same way as the keypad on the front of the Secvest device.	89

INFO

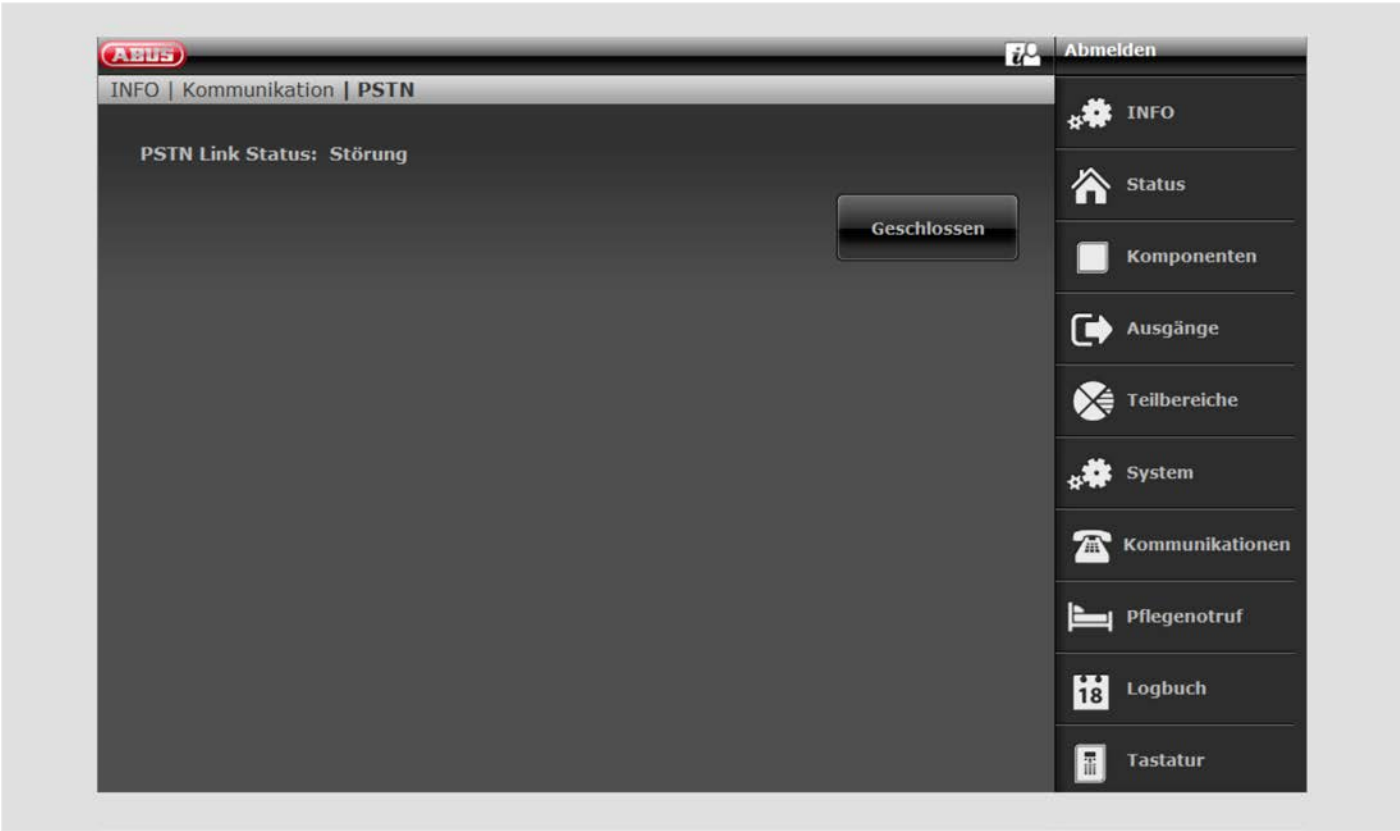
Panel



Name/function	Explanation
Version	Version number of the software currently installed on the alarm system
Serial Number	Serial number of the alarm system
Part No	Article number of the alarm system
Language	Set language including language version, e.g. English v1.00

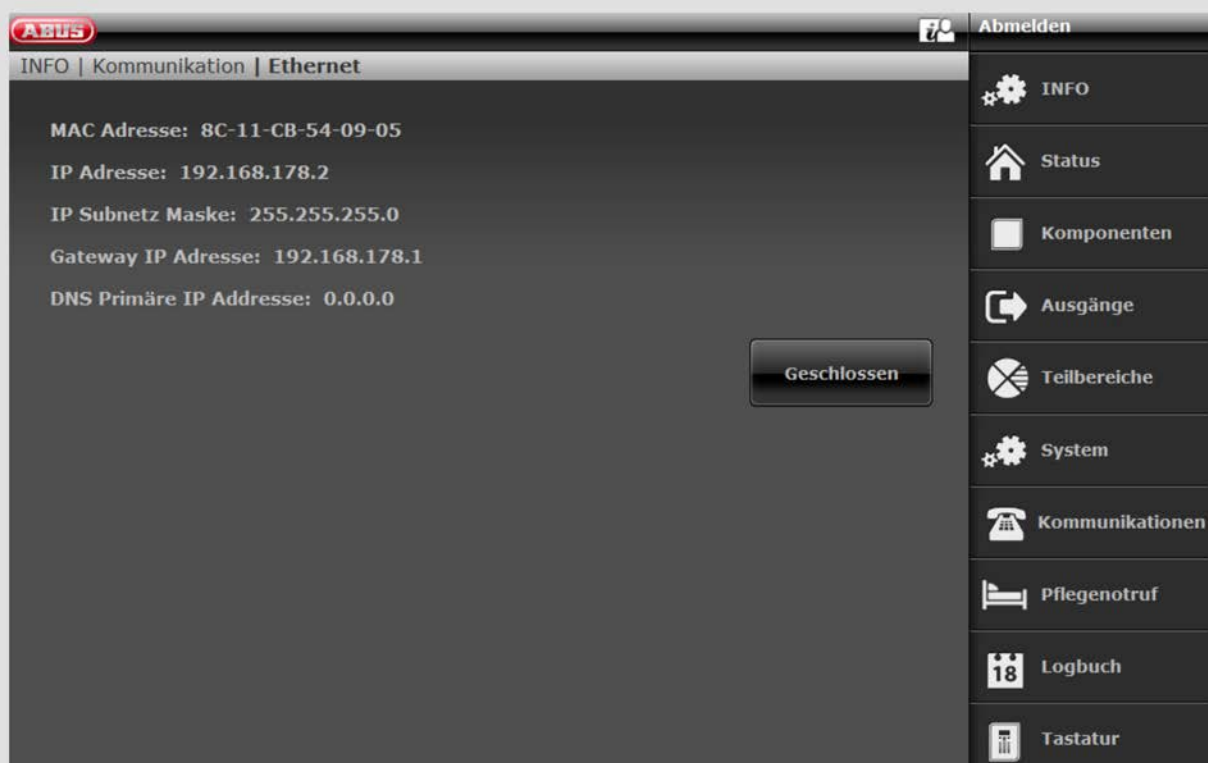
Communications

PSTN



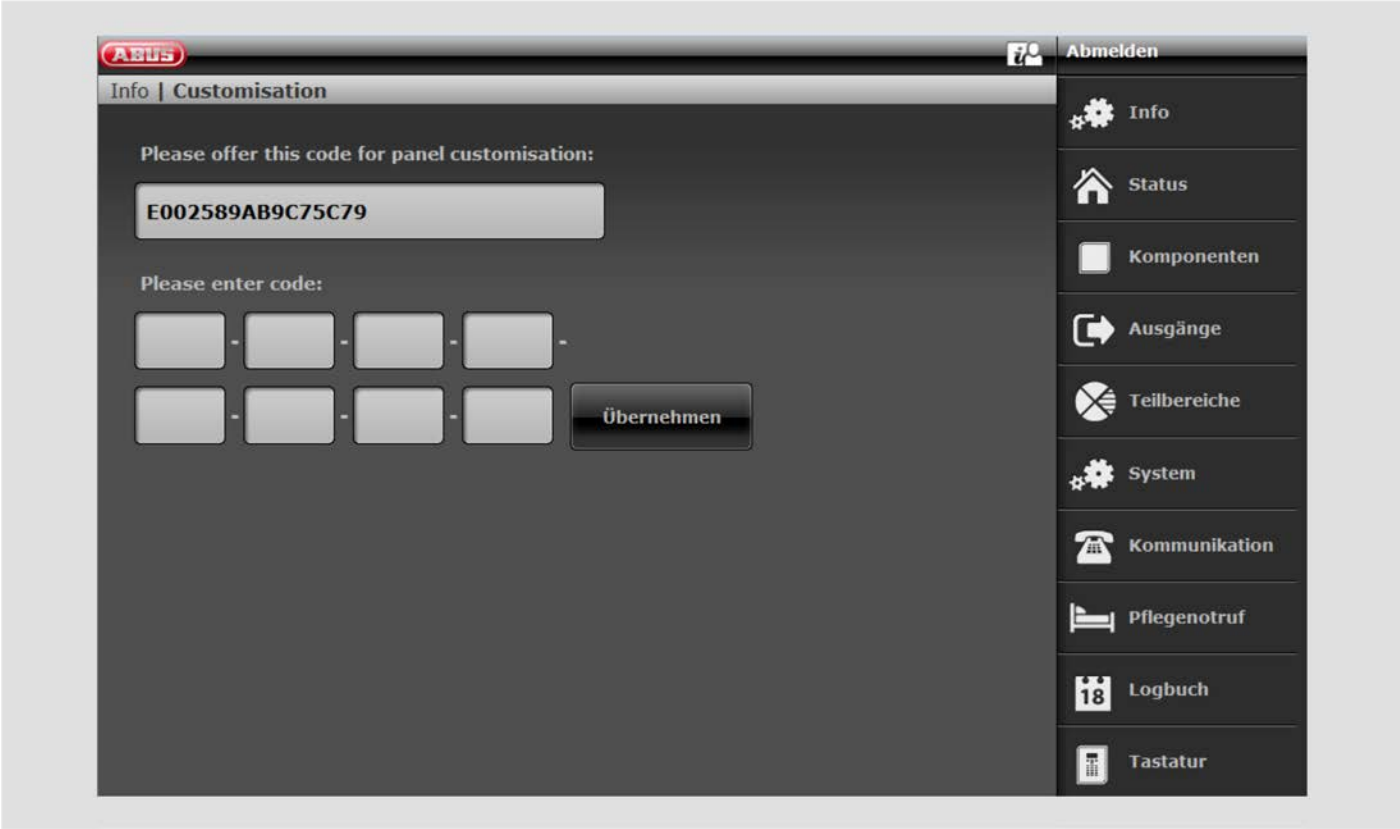
Name/function	Explanation
PSTN Link Status	Queries the PSTN link status. Secvest checks the connected telephone line. The message "OK" appears. If it is not connected, not enabled or is disrupted, the error message "Fault" appears.

Ethernet




Name/function	Explanation
MAC Address	The hardware address of the network adapter for the Secvest is given here. A MAC address is globally unique.
IP Address	If the Secvest is located on a network the IP address is shown here, e.g. 192.168.178.23. If (DCHP) is shown after this in brackets, the Secvest automatically obtains its IP address from a DHCP server, for example, in a router. If the Secvest is not networked, "0.0.0.0" is displayed here.
IP Subnet Mask	The subnet mask is displayed here. In a private network this is normally 255.255.255.0.
Gateway IP Address	If the Secvest is located on a network the IP address of the gateway is shown here. An example of a gateway in a private network is the router, e.g. the Fritz!Box.
DNS Primary IP Address	This is the IP address of the Domain Name System (DNS).

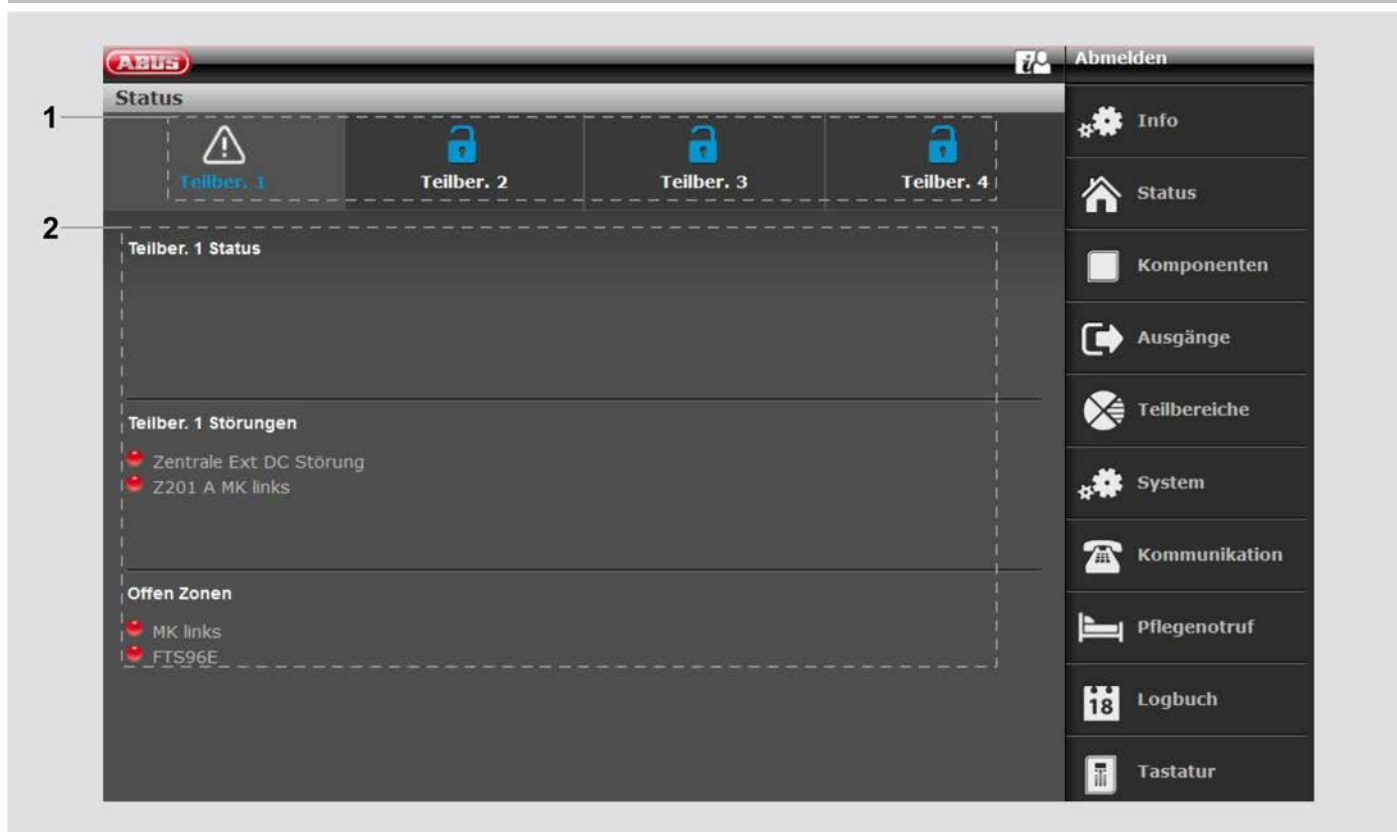
Customisation



Name/function	Explanation
Please offer... -> Installer Code	ID of the wireless alarm system (required for the licence key)
Please enter code	Input field for the licence key for customisation of the alarm system (language settings, for example)

**Note**
Customisation via this menu is currently not an option.

Status



No	Name/function	No	Name/function
1	Partition selection Selection fields/tabs for individual partitions: <ul style="list-style-type: none"> • An alarm that is confirmed by the user but not reset is displayed in the corresponding partition as a warning symbol. • Clicking this warning symbol resets this alarm. 	2	Status display The status display contains information including: <ul style="list-style-type: none"> • faults in the individual partitions • faults across partitions (e.g. "Ext DC fault") • open zones (across partitions)

Devices

Detectors

IP zones

ABUS

Abmelden

Komponenten | IP Zonen

Nummer	Name	Teilbereiche	Typ	Eigenschaften	Batterie schwach	Ausblenden	Aktiv	Aktiviert	Supervisionsstörung	Alarm	Sabotage	RSSI:
Z101 IP	"Zone 101"	Keine	nicht verwendet		*						*	*
Z102 IP	"Zone 102"	Keine	nicht verwendet		*						*	*
Z103 IP	"Zone 103"	Keine	nicht verwendet		*						*	*

Abmelden

INFO

Status

Komponenten

Ausgänge

Teilbereiche

System


Kommunikationen

Pflegenotruf

Logbuch

Tastatur

Name/function	Explanation
Number	The number comprises the zone name and the component type (IP).
Name	Unique name of the zone
Partition	Partition of the individual zone
Type	Type of the individual IP zone
Attributes	Overview of the attribute and status of the individual IP zone



Note

To integrate a network camera into a free IP zone, it must first be integrated and configured in the alarm panel network (see installation instructions TVIP41550).

Make a note of the settings defined for the camera in order to apply these when adding the camera to a free IP zone.

Select a free IP zone in which to integrate the network camera.

Add/delete

Select the desired IP zone in the menu "Devices → IP Zones". Use the "Add/delete..." button to open the following view where devices are integrated:

Name/function	Explanation
Device Type	Camera TVIP41550
Trigger Mode	Internal The camera starts recording as soon as the integrated PIR sensor is triggered. External The camera starts recording as soon as one of the defined trigger events occurs on the alarm panel. Int. + Ext. The camera starts recording as soon as the integrated PIR sensor is triggered or one of the defined trigger events occurs on the alarm panel.
Trigger Events	(for "External" or "Int. + Ext." trigger mode only) Events which cause the camera to start recording.
Trigger Partitions	(for "External" or "Int. + Ext." trigger mode only) Partitions to be monitored when trigger events occur.
IP Address	IP address of the camera in the internal network
HTTP Port Internal	HTTP port of the camera in the internal network (default setting: "80")
RTSP Port Internal	RTSP port of the camera in the internal network (default setting: "554")
HTTP Port External	External HTTP port for which port forwarding in the router is configured
RTSP Port External	External RTSP port for which port forwarding in the router is configured
User name	Default setting "Root"
Password	Default setting – no password assigned

Apply the settings with the "Submit" button.

Assigning a zone name



Note

It is useful to assign unique zone names so that if a fault occurs it is easier to identify the affected detector.

Example: MD stands for motion detector, location: office01, so detector name is **MD-office01**

1. Click in the **Name** text field.
2. Delete the preset name (Zone 01).
3. Assign a unique name for the zone with max. 12 characters.
4. Confirm the new name once the configuration is complete by selecting **Submit**.

Selecting the zone type



Note

The preset zone type can be changed here. Note the description of the zone types in this section.

A **zone** is a **detector** that is taught into the **wireless alarm panel**.



Zones can have different attributes.

The detector does not know whether the wireless alarm panel is armed or disarmed.

For this reason, detectors always send an alarm to the alarm panel if they register a change.

The alarm is only then analysed in the wireless alarm panel to determine whether the notification triggers an alarm response or not.

1. Select menu item **Type**

Type	Explanation
Not Used	A zone that is not used because no wireless detector is taught in (no "radio detector learned") or because its input is not wired to a detector should be configured as zone type "Not Used". The alarm system does not respond when an event triggers a detector in this zone.
Normal Alarm	If the wireless alarm panel is armed, this zone immediately triggers an alarm if a wireless detector sends a change to the alarm panel or the status of the alarm zone changes (e.g. alarm contact opens).
	 Note Zone type "Normal Alarm" with additional functionality of pry-attempt monitoring for ABUS mechatronics products such as the FOS 550 E window bar lock, additional door lock or FOS 400 E window lock. If using a mechatronics product intended for Secvest, configure zone type "Normal Alarm" in the alarm panel. When the alarm panel is disarmed, these detectors are monitored both for pry attempts and opening. For this, the window must be closed and the lock secured. Monitoring begins 30 seconds after locking, as a self-calibration time of 30 seconds is required. If the mechatronic additional lock is unlocked, monitoring stops. If an attempt is made to open the window without first unlocking the additional lock, an alarm may be triggered by the movement of the window leaf. Pry-attempt monitoring can be disabled in the attributes (see "Zone attributes" below). A passive glass breakage detector can also be connected to some mechatronic products. This detector sends an alarm when it detects glass breakage, which always leads to an alarm response on the alarm panel. The alarm panel carries out actions intended for an armed or disarmed status.
Zone Lock	The zone must be locked (closed) in order to arm or internally arm the wireless alarm panel. If the wireless alarm panel is armed or internally armed, opening this zone does not trigger an alarm. This zone is used with lock switch contacts.  Note This zone type was used in the Secvest 2WAY as a zone attribute rather than a zone type.
Exit Norm Alm	A zone configured as "Exit Norm Alm" behaves similarly to a "Normal Alarm" zone. A zone of this type, however, starts an alarm even when the detector is triggered during the exit time.
Hold Up Alarm	This zone always triggers an alarm, regardless of whether the alarm panel is armed or disarmed. A hold up alarm can also be transmitted silently (communications). The configuration menu can only be exited when this zone is closed. Teach in the hold up button (wireless or wall) in this zone.
Fire Alarm	This zone always triggers an alarm, regardless of whether the alarm panel is armed or disarmed. The alarm is triggered via the sounder in the wireless alarm panel and on the outdoor siren (external siren) as a pulsed fire alarm sound. Teach in only smoke alarm devices in this zone.
24 Hour Alarm	This zone always triggers an immediate alarm. When the alarm panel is disarmed, the alarm is first triggered via the integrated sounder in the alarm panel. When the alarm panel is armed, the siren output is also activated. If a 24 hour zone is disabled, it is only disabled when the alarm panel is disarmed.
Perimeter Warning	This zone triggers a pre-alarm when the alarm system is armed or internally armed. The alarm panel beeps twice every five seconds. "Perimeter Warning" appears on the display every five seconds. Teach in outdoor motion detectors in this zone, for example. The wireless outdoor sirens flash and sound for approx. 1 s every five seconds. The info module beeps every 1 s and the red alarm LED lights up. The indoor siren sounds every 1 s. This siren must be supplied by a power supply unit for this purpose, however, and the "alarm only" jumper must not be connected. (This tone is an "info" tone rather than an "alarm" tone.) All signals are active for a duration of 30 s. A "Perimeter Warning" output is activated for 30 s. When the system is disarmed only the doorbell ("chime") sounds, if configured.
Final Door	When the alarm panel is armed, this zone triggers an alarm once the set delay time (entry delay) has expired. Use this zone type for the magnetic contact on the entrance door, for example. When exiting the premises, closing this zone can also be used to end the exit delay. This detector can be used as a "Normal Alarm" when the system is armed internally.

Configuration

Type	Explanation
Entry Route	This zone does not trigger an alarm if a "Final Door" zone has previously activated the entry delay time. An immediate alarm is triggered if no entry delay has previously been activated. Use this zone type for a motion detector in the entrance area, directed at the entrance door (which is fitted with a magnetic contact), for example. This detector can be used as a "Final Door" detector when the system is armed internally. It is possible to exit the configuration menu when this zone is open.
Technical Alarm	A "Technical Alarm" zone triggers an alarm and communication when the system is disarmed. When the system is armed, only communication is sent; no alarm is triggered. If an alarm is triggered in this zone when the system is armed, it is displayed on the alarm panel when the system is disarmed. Use this zone type for flood detectors, for example. The wireless info module and the wireless indoor siren signal technical alarms with beeps, like the alarm panel.
Key Switch (Moment.)	Teach in a (momentary) key switch on the wireless alarm panel. A change to this zone changes the status of the alarm panel from set to unset, or from unset to set (after the delay time has expired).
Key Switch (Latched)	A (latched) key switch can be connected to the alarm panel. A change to this zone changes the status of the alarm panel from set to unset, or from unset to set (after the delay time has expired). Note that the alarm panel is only operated via the key switch. When the status is not known, e.g. when the key switch is closed but disabled on the control device at the same time, the alarm panel may return to the "Set" status.
Key Box	<p>This zone is mainly used in Scandinavia. If this zone is opened, this event is saved in the alarm panel memory. It can also be transmitted via the telephone dialler at the same time. It does not trigger an alarm.</p> <p>If a zone of this type is required, the installer usually connects the alarm wires of this zone (usually the auxiliary contacts of a door contact) to an external key box and the tamper wires to the tamper switch of the housing.</p> <p>If the housing is opened, the wireless alarm panel saves the event and reports it to the alarm reception centre.</p>
Tamper	This zone is used for tamper monitoring of external devices. Monitoring of this zone is permanently enabled. If the alarm panel is disarmed, only the internal siren is triggered. If the alarm panel is armed, the external siren and strobe are triggered and communication is sent according to the configuration.
Log Only	<p>If a "Log Only" zone is triggered (alarm or tampering), only a log book entry is created and an output that follows this zone is triggered. The zone can be triggered when the alarm panel is armed or disarmed.</p> <p>"Log Only" zones can be assigned to multiple partitions and can have the "Chime" attribute.</p>
Exit Terminate	This zone is used to cancel the exit delay for a partition with the "Exit Terminate" attribute. This zone type is typically used for key switch (NO). Note: this zone is enabled during the exit time but disabled when the wireless alarm panel is armed or disarmed. If the "Chime" attribute is assigned to this zone, the doorbell sounds both when the wireless alarm panel is armed and disarmed.
Lock Set	This zone is used to cancel the exit delay for a partition with the "Lock Set" attribute. This zone type is typically used for a switch (NO). Note: this zone is enabled during the exit time and when the wireless alarm panel is armed. This zone can be assigned to the "Inverted" attribute.
Ext WD Fault	This zone is used to monitor the fault output of external sounders. If a fault output with this zone type is triggered, "Ext WD Fault" appears on the display. This zone type is not available for wireless zones.
HUD Fault	This zone is used to monitor the fault output of wired hold up signalling devices. If a hold up device with this zone type is triggered, "HUD Fault" appears on the display. This message also appears on the display if the user tries to arm the wireless alarm panel while an alarm is active. The user can override the fault and arm the system. If this fault is triggered while the system is armed, a log book entry is created and the communication configured accordingly is started, but no alarm is triggered until the wireless alarm panel is disarmed. This zone type is not available for wireless zones.

Type	Explanation
Tamper Return	This zone is used to monitor the fault output of external sounders. Monitoring of this zone is permanently enabled. If a zone with this type is triggered when the wireless alarm panel is disarmed, only the internal siren is activated. If this alarm is triggered when the system is armed, the communication can be sent if configured accordingly and external sounders with strobe can be triggered. This zone type can have the following attributes: "Soak Test", "Part Set", "Omittable" and "Force Set". This zone type is not available for wireless zones.
Ext PSU A/C fault	This zone is used to monitor the AC fault output of an external power supply. If a zone of this type is triggered, the wireless alarm panel reacts as if there were a "Panel A/C fault" on the panel itself. The response depends on the configuration. This zone type is not available for wireless zones.
Ext PSU Batt Fault	This zone is used to monitor the battery fault output of an external power supply. If this fault is triggered, outputs configured for "Battery Fault" are activated and "Ext PSU Batt Fault" appears on the display. If this fault is triggered while the system is armed, a log book entry is created and the communication configured accordingly is started, but no alarm is triggered until the wireless alarm panel is disarmed. This zone type is not available for wireless zones.
Ext PSU Low Volts	This zone is used to monitor a fault output for "low battery" of an external power supply. If this fault is triggered, outputs configured for "Low Volts" are activated and "Ext PSU Low Volts" appears on the display. If this fault is triggered while the system is armed, a log book entry is created and the communication configured accordingly is started, but no alarm is triggered until the wireless alarm panel is disarmed. This zone type is not available for wireless zones.
Ext PSU Fault	This zone is used to monitor the fault output of an external power supply. If this fault is triggered, outputs configured for "Ext PSU Fault" are activated and "Ext PSU Fault" appears on the display. If this fault is triggered while the system is armed, a log book entry is created and the communication configured accordingly is started, but no alarm is triggered until the wireless alarm panel is disarmed. This zone type is not available for wireless zones.

Selecting a partition



Note

The taught-in detectors are assigned to **Partition 01** by **default**.

To assign the detector to another partition, proceed as follows:

1. Use the checkboxes to select the desired **partition(s)** in which this zone will be monitored.



Note

At least one partition must be selected.

Setting options for the partitions can be found in section "Configuring Secvest via web server -> Partitions" in this manual.

Zones of the following types can be assigned to one or more partitions: Normal Alarm, Zone Lock, Final Door, Entry Route, Key Switch, Key Box, Log Only, Exit Terminate, Lock Set and Exit Norm Alm.



Note

If you plan on using internally armed partitions, you must ensure that the internally armed options are the same for all zones used for more than one partition.

The wireless alarm panel does not allow zones of the following types to be assigned to more than one partition: 24 Hour Alarm, Fire Alarm, Hold Up Alarm, Perimeter Warning, Tamper and Technical Alarm.

Selecting zone attributes

1. Use the checkboxes to select the desired **attribute(s)**.

Attribute	Explanation
Chime	Each time this zone is triggered when the alarm panel is disarmed, the panel sounds an acoustic signal.
Force Set Omit	If a zone is given this attribute, this zone is automatically omitted if it was open when the system was armed.

Attribute	Explanation
Omittable	If a zone is given this attribute, a user can omit this zone before arming the system. If a user attempts to arm the system when a zone with this attribute is open, a warning appears and the arming process is interrupted. The user can acknowledge this warning and continue the arming process.
Dis. Sabotage	This attribute is an additional attribute for mechatronic ABUS door and window locks. The "Normal Alarm" zone type must be selected. When the "Dis. Sabotage" attribute is selected, pry-attempt monitoring of the supported mechatronic products is switched off when the alarm system is disarmed. This attribute is not recommended and is only necessary in special cases. A "W" appears in the attribute line on the alarm panel display.
Soak Test	If a detector tends to trigger a false alarm, activate the soak test. This setting resets automatically after 14 days. The detector does not trigger any alarms on the alarm panel during this time. However, all triggers are written to the memory (log book) for analysis purposes.
Part Set	This zone is monitored when the partition of this zone or all partitions are internally armed.
Activity Monitor	The function of the detector is reversed (inverted). This should only be used in connection with the social care emergency call. An alarm is triggered on the alarm panel when the detector does not register any alarm within a certain time period.



Note

The **Soak Test** function should only be set if a detector tends to trigger **false alarms**.

This function works automatically. To test the range of the detector, use the "walk test" function and do **not** activate the soak test, as this function **stops the detector from triggering any alarms when the wireless alarm system is armed** and only saves a message to the memory instead.

After 14 days the wireless alarm system resets the zone and brings it back to normal operation.



Note

The **Force Set Omit** function must **also** still be activated in menu **System -> Security Settings -> Force Set**.

Wireless Zones

Komponenten | Funk Zonen

Abmelden

Nummer	Name	Teilbereiche	Type	Eigenschaften	Batterie schwach	Ausblenden	Aktiv	Aktiviert	Supervisionsstörung	Alarm	Sabotage	RSSI:
Z201 FUNK	"MK"	1	Normal Alarm	Türgong, Intern überwacht, Ausblendbar								* *
Z202 FUNK	"FTS96E"	3	Normal Alarm	Türgong, Intern überwacht, Ausblendbar								* *
Z203 FUNK	"RWM"	2	Feuer									* *
Z204 FUNK	"Zone 204"	Keine	nicht verwendet									* *
Z205 FUNK	"Zone 205"	Keine	nicht verwendet									* *
Z206 FUNK	"Zone 206"	Keine	nicht verwendet									* *
Z207 FUNK	"Zone 207"	Keine	nicht verwendet									* *
Z208 FUNK	"Zone 208"	Keine	nicht verwendet									* *
Z209 FUNK	"Zone 209"	Keine	nicht verwendet									* *
Z210 FUNK	"Zone 210"	Keine	nicht verwendet									* *

<
...
1
2
3
4
5
...
>

INFO

Status

Komponenten

Ausgänge

Teilbereiche

System


Kommunikationen

Pflegenotruf

Logbuch

Tastatur

Name/function	Explanation
Number	The number comprises the zone name and the component type (wireless/radio).
Name	Unique name of the zone
Partition	Partition of the individual zone
Type	Type of the individual wireless zone
Attributes	Overview of the attributes for the individual wireless zone

 **Note** The description of the configuration of the zone name, partition, zone type and zone attributes can be found after the "IP zones" overview from page 41.

Function	Explanation
Edit Zones	This function provides the option of changing the parameters of the zone.
Delete All	All detectors can be deleted in one step. The zone type is reset to "Not Used".


Adding/deleting detectors (alarm panel only)

1. Select menu "Devices → Wireless Zones".
2. The following function is available:

Function	Explanation
Add/Del Detectors	<p>Select this item to view a list of all available zones.</p> <p>Select a zone in which you wish to teach in a detector or from which you wish to delete a detector.</p>

Adding detectors


1. Select a zone.
2. You will be prompted to enable the tamper contact of the detector.

 **Note** Ensure that no other active detector has the tamper status.

3. This display shows:
 - the zones in which the detector has been taught in
 - the zone type configured for this detector
 - the partition this detector monitors
 - the additional zone attributes that are available.
4. In addition, "SS:" (signal strength) and the received signal strength are displayed. To have good communication, this value should be higher than 3.



Note

If a detector have been successfully taught in, the alarm panel displays the symbol  next to the zone number.

For a taught-in zone with a WAM (WAM function 3 sender receiver), "w2" is displayed, for example.

Delete All (alarm panel only)

1. Select **Delete All**.
2. Confirm the selection with **Next**.
3. Confirm the security prompt with **Yes** to delete the detector/zone or **Back** if you are not sure.

Detector is already used



Note

In rare cases, the message **Detector is already used** may appear on the display when you are teaching in a detector, after you have received confirmation of the teach-in process, because the detector sends its signal more than once.

In this case the message can be ignored.

This detector may already be taught in in another zone.

Deleting detectors or detector + zone information

1. Select the zone in which the detector is registered.
2. Select:
 - **Delete Detector ID** when you only wish to delete the detector
 - **Default Zone** when you wish to delete the detector and the zone information.
3. Confirm the selection with **Next**.
4. Confirm the security prompt with **Yes** to delete the detector/zone or **Back** if you are not sure.

Wired Zones

ABUS

Abmelden

Komponenten | Draht Zonen

Nummer	Name	Teilbereiche	Typ	Eigenschaften								
					Batterie schwach	Ausblenden	Aktiv	Aktiviert	Supervisionsstörung	Alarm	Sabotage	RSST:
Z301 VERDRAHTET	"Zone 301"	Keine	nicht verwendet	✱							✱	✱
Z302 VERDRAHTET	"Zone 302"	Keine	nicht verwendet	✱							✱	✱
Z303 VERDRAHTET	"Zone 303"	Keine	nicht verwendet	✱							✱	✱
Z304 VERDRAHTET	"Zone 304"	Keine	nicht verwendet	✱							✱	✱

Abmelden

INFO

Status

Komponenten

Ausgänge

Teilbereiche

System

Kommunikationen

Pflegenotruf

18 Logbuch

Tastatur

Name/function	Explanation
Number	The number comprises the zone name and the component type (wired).
Name	Unique name of the zone
Partition	Partition of the individual zone
Type	Type of the individual wired zone
Attributes	Overview of the attributes for the individual wired zone

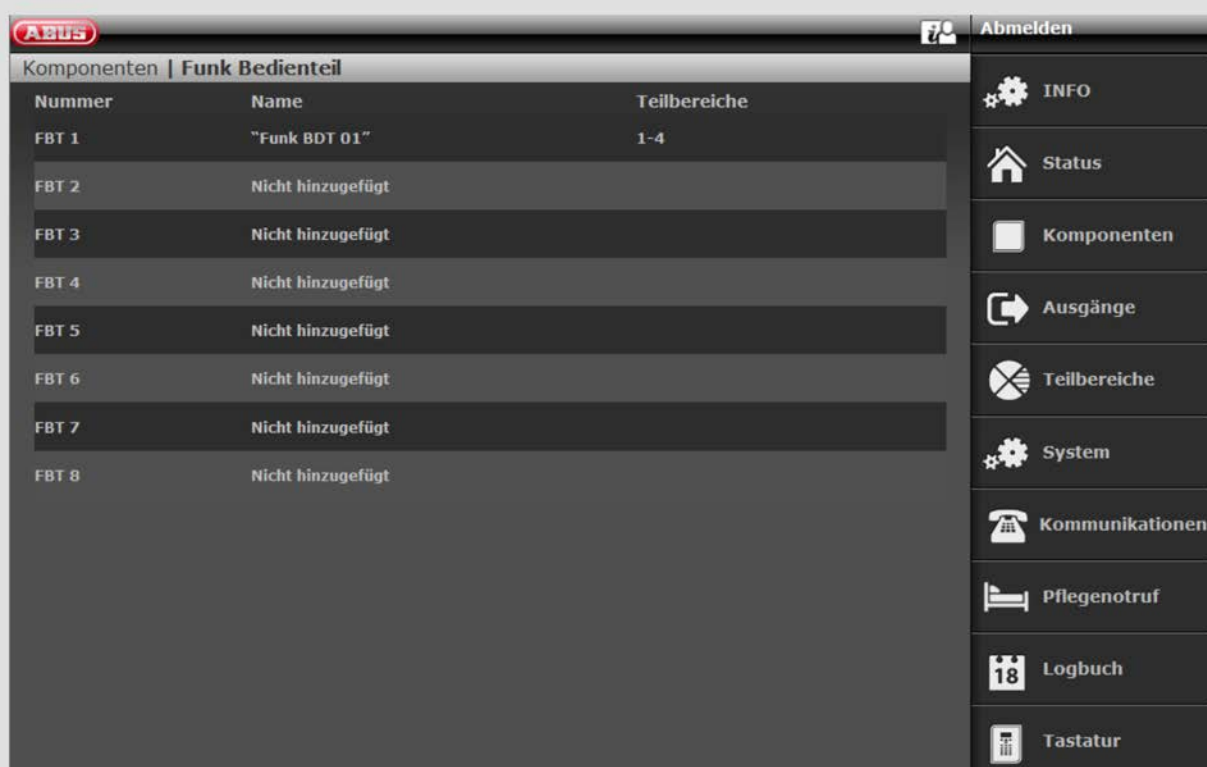
Delete All (alarm panel only)

1. Select **Delete All**.
2. Confirm the selection with **Next**.
3. Confirm the security prompt with **Yes** to delete the detector/zone or **Back** if you are not sure.

**Note**

The description of the configuration of the zone name, partition, zone type and zone attributes can be found after the "IP zones" overview from page 41.

Control Devices



Komponenten Funk Bedienteil		
Nummer	Name	Teilbereiche
FBT 1	"Funk BDT 01"	1-4
FBT 2	Nicht hinzugefügt	
FBT 3	Nicht hinzugefügt	
FBT 4	Nicht hinzugefügt	
FBT 5	Nicht hinzugefügt	
FBT 6	Nicht hinzugefügt	
FBT 7	Nicht hinzugefügt	
FBT 8	Nicht hinzugefügt	

Abmelden

INFO

Status

Komponenten

Ausgänge

Teilbereiche

System

Kommunikationen

Pflegenotruf

Logbuch

Tastatur

Name/function	Explanation
Number	The number comprises the component type (CDV) and a consecutive number.
Name	Unique name of the control device
Partitions	Assigned partitions of the individual control device

Adding control devices (alarm panel only)




Note

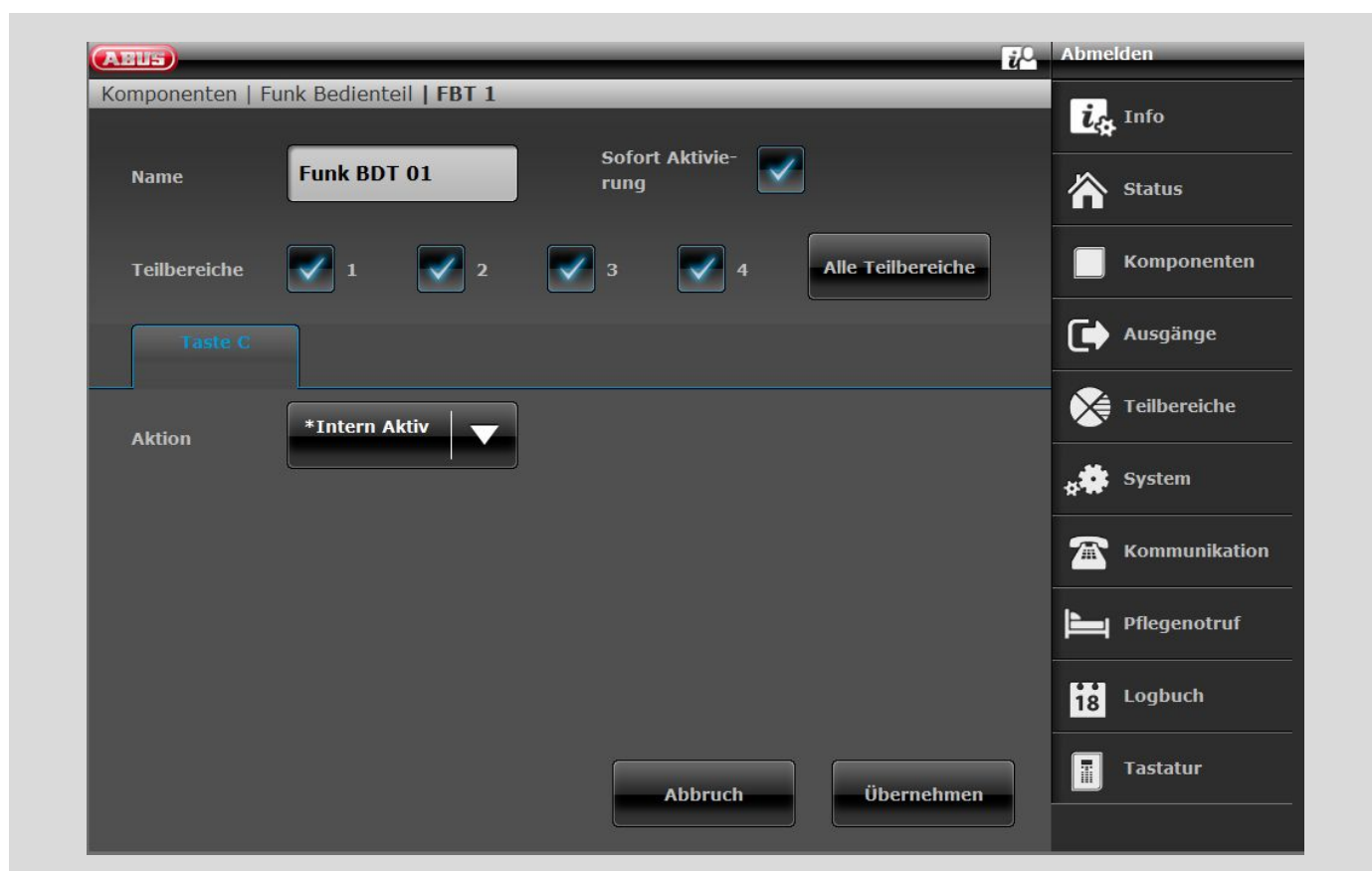
Up to eight wireless control devices can be taught in.

1. Select **Add/Del Ctrl Device**.
2. **Select** the corresponding control device.
3. Trigger the tamper contact of the control device (see separate instructions for the wireless control device).



Note

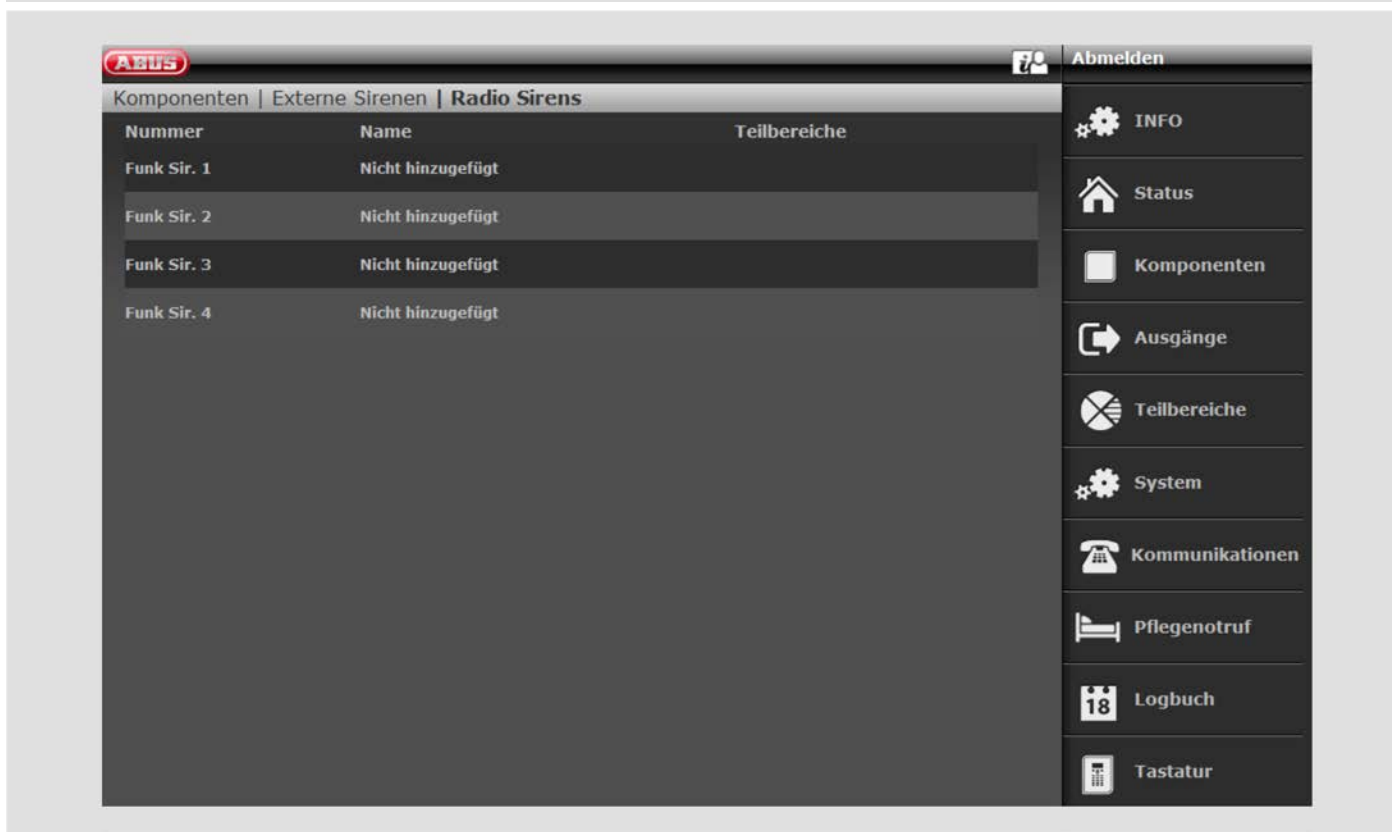
When the wireless control device has been taught in, the wireless alarm panel beeps twice to confirm. At the same time, the symbol  appears next to the control device number on the graphical display above.



Name/function	Explanation
Name	Unique name of the control device
Instant Set	Immediate arming of the individually assigned partitions (yes/no)
Partitions	Assigned partitions of the control device
C button Action	Selection of the action to be triggered when the "*" button is pressed:
	Not Used C button has no function
	Set Arm the assigned partitions
	Part Set Internally arm the assigned partitions
	Unset Disarm the assigned partitions
	Output On Switch on the assigned output
	Output Off Switch off the assigned output
	Output Toggle Toggle the assigned output
Output	(only available for "Output On", "Output Off" and "Output Toggle") Selection of the desired output to be switched on or off or toggled.

Outdoor (external) sirens

Radio Sirens



Name/function	Explanation
Number	The number comprises the component type (radio siren) and a consecutive number.
Name	Unique name of the radio (wireless) siren

Adding sirens

1. Select **Radio Siren**.
2. Select **Add/Del Siren**.
3. Select the corresponding siren.
4. Trigger the tamper contact of the siren.




Note

When the siren has been taught in, the wireless alarm panel beeps twice to confirm. A message appears on the display to confirm that the siren was added, and the value for the received signal strength is shown.

5. Exit the entry with **Back**.



Note

If a siren has been taught in the symbol  appears next to the siren number on the alarm panel display.

6. Exit this display with **Back**.
7. Select **Edit Ext. Siren**.
8. **Select** the taught-in **Ext. Siren**.



Note

If the external siren is activated, when the corresponding partition triggers a local or external alarm, the partition must be set to **Yes**.

Delete All (alarm panel only)

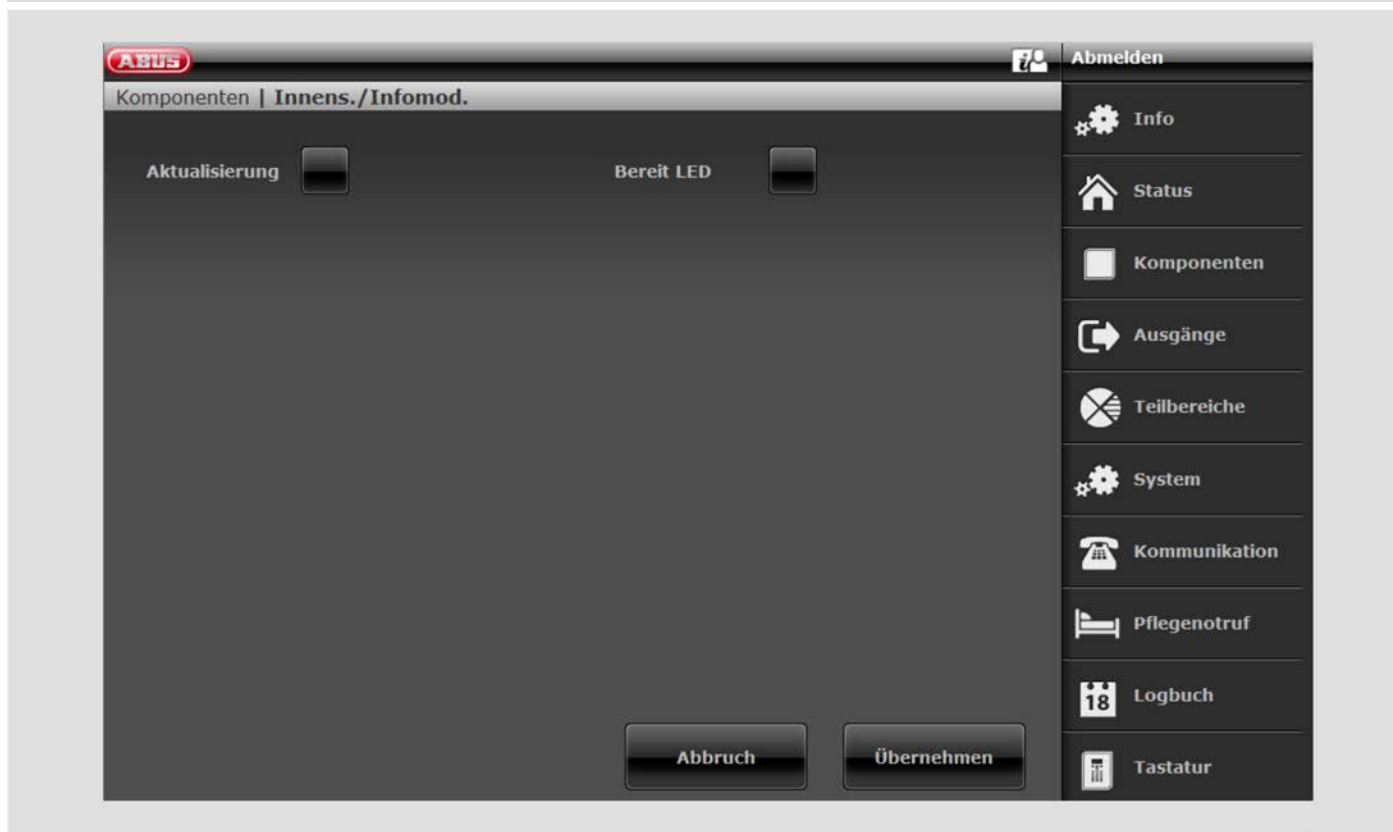
1. Select **Delete All**.
2. Confirm the selection with **Next**.
3. Confirm the security prompt with **Yes** to delete the siren or **Back** if you are not sure.

Wired Sirens

The screenshot displays the ABUS configuration software interface. At the top, there is a navigation bar with the ABUS logo and a user icon. Below this, a breadcrumb trail shows 'Komponenten | Externe Sirenen | Draht Sirenen'. The main content area is a table with two columns: 'Nummer' and 'Name'. The first row of the table lists 'Wired SRN 1' under 'Nummer' and '"Wired SRN 01"' under 'Name'. To the right of the table is a vertical sidebar with various icons and labels: 'Abmelden' (logout), 'INFO' (gear icon), 'Status' (house icon), 'Komponenten' (square icon), 'Ausgänge' (arrow icon), 'Teilbereiche' (circle with cross icon), 'System' (gear icon), 'Kommunikationen' (phone icon), 'Pflegenotruf' (bed icon), 'Logbuch' (calendar icon), and 'Tastatur' (keyboard icon).

Name/function	Explanation
Number	The number comprises the component type (Wired SRN) and a consecutive number.
Name	Unique name of the wired siren

Info module/indoor siren

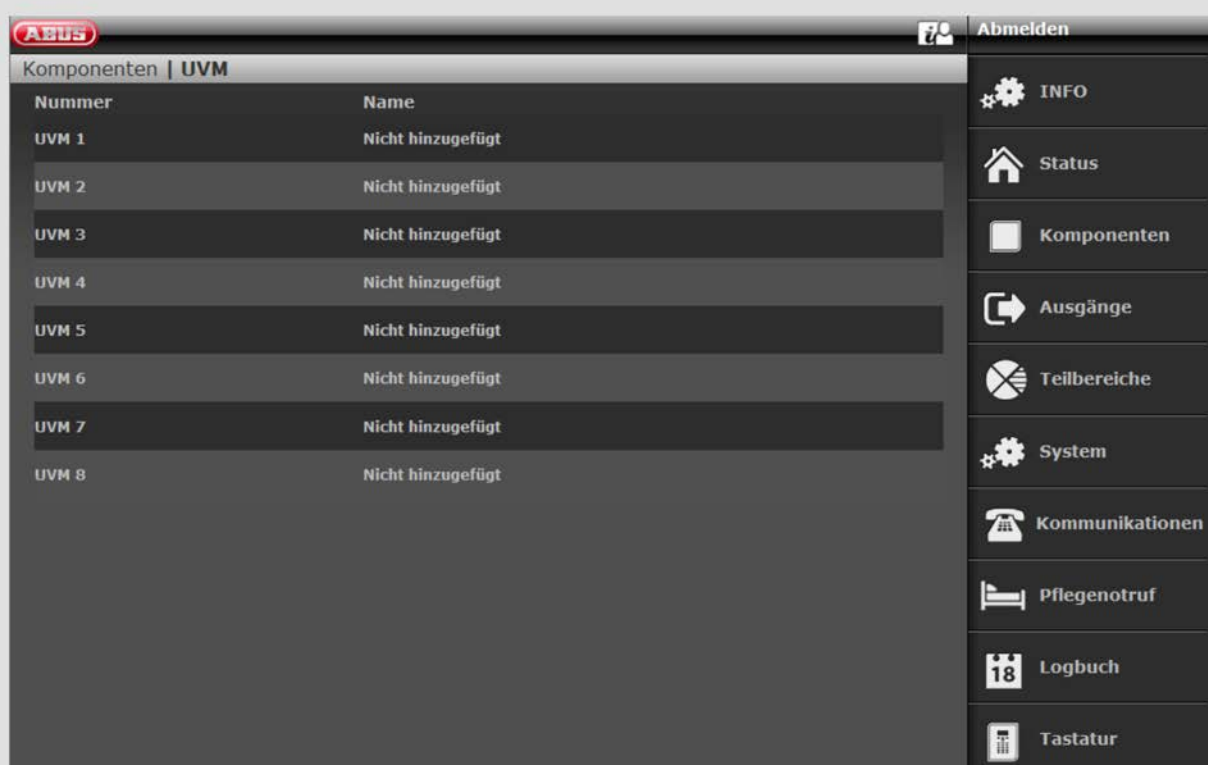


Name/function	Explanation
Updates	<p>Activated Status updates on the info module activated – a status change on the alarm system or zones is displayed "just in time".</p> <p>Deactivated No update on the info module and indoor siren – the indoor siren also does not trigger any alarm accordingly.</p>
Ready-to-Set LED	<p>Activated Ready-to-Set LED activated on the info module.</p> <p>Deactivated Ready-to-Set LED deactivated on the info module.</p>

Add Panel (alarm panel only)

- After selecting this menu item, the following display appears:
 - Select **Add/Del Siren**.
- Select the corresponding siren.
- After selecting this menu item, the following display appears:
 - Is the receiver in teach-in mode?
- Switch the indoor siren or info module to teach-in mode. Follow the instructions provided in the guide for the product.
- Activate the sending of wireless information from the alarm panel by pressing **Yes**.
- The following display appears: Did the receiver beep twice?
- Confirm with **Yes**.
- The teach-in message and therefore the IP of the alarm panel have been correctly received and successfully stored in the indoor siren or info module.
- To repeat or cancel, press **No**.

WAM (Wireless Accessory Module)



Name/function	Explanation
Number	The number comprises the component type (WAM) and a consecutive number.
Name	Unique name of the wireless accessory module

Adding a wireless accessory module.

**Note**

Ensure that reserved outputs and zones are assigned to each WAM.
See the table of reserved WAM outputs/zones below.


Wireless accessory module	Reserved outputs	Reserved Zones
WAM 1	229–232	248
WAM 2	225–228	247
WAM 3	221–224	246
WAM 4	217–220	245
WAM 5	213–216	244
WAM 6	209–212	243
WAM 7	205–208	242
WAM 8	201–204	241

**Note**

Configure the wireless accessory module as describe in the WAM installation instructions, e.g. as a wireless sender/receiver (function 3). Once the wireless accessory module has been configured as per the instructions, it can be added to the system.

1. Select **Add/Del WAM**.
2. **Select** the corresponding wireless accessory module (WAM). Up to **eight** wireless accessory modules can be taught in.
3. Select, for example, **WAM 1**.
4. Trigger the tamper contact on the WAM.

**Note**

When WAM modules are taught in, the **symbol**  appears next to the WAM number.
Check the information of the wireless accessory module.

5. Select **WAM Info**.
6. Select **WAM 1**.



Note

When the wireless accessory module is taught in, its configuration is also transferred, so it is possible to see under "WAM Info" which function the wireless accessory module had when it was taught in.

Function	Explanation
Not Used	The wireless accessory module is not taught in.
1 Wireless Repeater	Received wireless signals from taught-in wireless detectors (taught into the WAM) are forwarded to the alarm panel. No further settings are necessary here.
2 Output Module	Up to four relays of the WAM can be activated by the wireless alarm panel according to the configuration.
3 T/R Module	Zone and output module for connection of wired detectors (flood detectors) or a block lock/key switch.
4 Sounder Module	For connection of a wired external sounder or compact alert.

WAM as wireless repeater (WAM function 1)

If the wireless accessory module is taught in with the wireless repeater function, the wireless detectors with signals that this module should transmit should also be taught into the WAM.

See the instructions for the wireless accessory module (WAM) for this.

WAM as output module (WAM function 2)



Note

If the wireless accessory module is taught in with the output function, the alarm panel automatically reserves the corresponding outputs in the panel for this module.



Note

These outputs no longer have to be added manually. Simply define the settings for the output function as described in section **Editing outputs**.

These outputs only need to be configured but no longer have to be added.

See the instructions for the wireless accessory module (WAM) for this.

WAM as zone and output module (WAM function 3)



Note

If the wireless accessory module is taught in with function 3, the alarm panel automatically reserves the corresponding zone and outputs in the panel for this module.

- Input 1 and input 2 form the wired zone of the WAM.
- Input 1 functions as the connection for the alarm loop. Input 2 functions as the connection for the tamper zone.
- Both of these connections correspond to the associated wireless zone.
- During wiring see the instructions for the wireless accessory module (WAM) for this.

WAM as sounder module (WAM function 4)

If the WAM is configured as a sounder module, a display appears upon connection, where you have to configure the partitions for which the sounder will be activated. This setting is defined similarly to the setting for the external sirens.

The connection of the compact alert in the WAM can be found in the instructions for the wireless accessory module (WAM).



Note

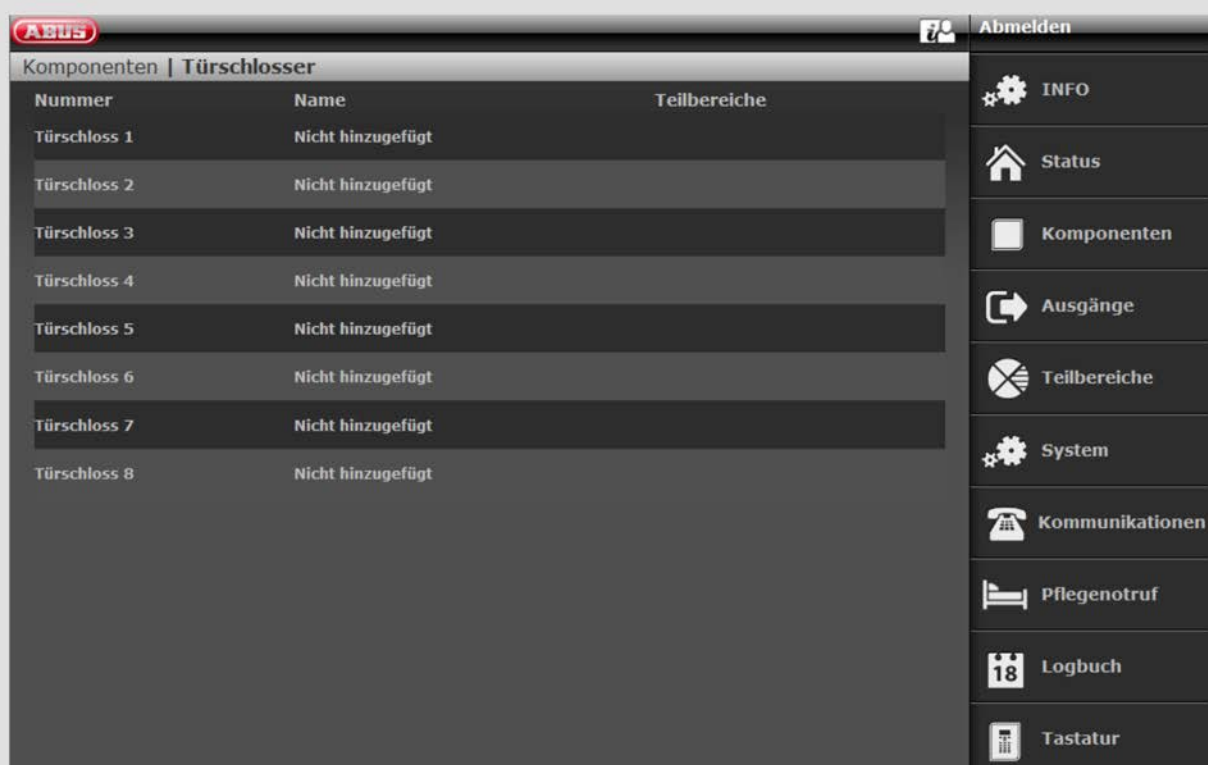
Ensure that the voltage-free outputs on the WAM can be loaded with **max. 500 mA at 24 volts**.

These outputs are optocouplers with a forward resistance of 2 Ω .

Delete All (alarm panel only)

1. Select **Delete All**.
2. Confirm the selection with **Next**.
3. Confirm the security prompt with **Yes** to delete the WAM or **Back** if you are not sure.

Door Locks



Name/function	Explanation
Number	The number comprises the component type (door lock) and a consecutive number.
Name	Unique name of the door locks (e.g. Secvest Key or additional door lock).
Partitions	Number of the partition to which the door lock is assigned.

Adding door locks (alarm panel only)

1. Select **Door Locks**.
2. Select **Add/Del Door Lock**.
3. Select the corresponding door lock.
4. Trigger the tamper contact of the door lock or insert a battery.




Note

When the door lock has been taught in, the wireless alarm panel beeps twice to confirm. A message appears on the display to confirm that the door lock was added, and the value for the received signal strength is shown.

5. Exit the entry with **Back**.



Note

If a door lock has been taught in the symbol  appears next to the door lock number on the alarm panel display.

6. Exit this display with **Back**.

Delete All (alarm panel only)

1. Select **Delete All**.
2. Confirm the selection with **Next**.
3. Confirm the security prompt with **Yes** to delete the door locks or **Back** if you are not sure.

Outputs

Radio Outputs

Ausgänge					Abmelden
Nummer	Name	Typ	Status	Eigenschaften	
Funk-Ausgang 201	"Ausgang 201"	nicht verwendet			INFO
Funk-Ausgang 202	"Ausgang 202"	nicht verwendet			Status
Funk-Ausgang 203	"Ausgang 203"	nicht verwendet			Komponenten
Funk-Ausgang 204	"Ausgang 204"	nicht verwendet			Ausgänge
Funk-Ausgang 205	"Ausgang 205"	nicht verwendet			Teilbereiche
Funk-Ausgang 206	"Ausgang 206"	nicht verwendet			System
Funk-Ausgang 207	"Ausgang 207"	nicht verwendet			Kommunikationen
Funk-Ausgang 208	"Ausgang 208"	nicht verwendet			Pflegenotruf
Funk-Ausgang 209	"Ausgang 209"	nicht verwendet			Logbuch
Funk-Ausgang 210	"Ausgang 210"	nicht verwendet			Tastatur

Name/function	Explanation
Number	The number comprises the component type (radio output) and a consecutive number.
Name	Unique name of the output
Type	Type of radio output
Status	Current status of the radio output
Attributes	Attributes of the radio output

Configuring radio outputs



Note

Secvest has up to 32 radio outputs.

Editing outputs

1. Click in the line of the desired output.



Note

It is useful to assign unique output names so that if a fault occurs it is easier to identify the affected output.

2. **Delete** the preset name.
3. Assign a unique name for the output with max. 12 characters.

Inverting outputs (polarity)



Note

You can choose here whether the function of the output in question is inverted or not. Select **Normal** or **Inverted**.

Selecting the output type



Note

This selection field also provides the option of automatically arming or disarming the alarm panel at a specific time.

An overview of the different output types can be found in the following table.

4. Confirm the selection once the configuration is complete by selecting **Submit**.

Wired Outputs

Ausgänge					Abmelden
Nummer	Name	Typ	Status	Eigenschaften	
Draht-Ausgang 301	"Ausgang 301"	nicht verwendet			INFO
Draht-Ausgang 302	"Ausgang 302"	nicht verwendet			Status
Draht-Ausgang 303	"Ausgang 303"	nicht verwendet			Komponenten
Draht-Ausgang 304	"Ausgang 304"	nicht verwendet			Ausgänge
					Teilbereiche
					System
					Kommunikationen
					Pflegenotruf
					Logbuch
					Tastatur

Name/function	Explanation
Number	The number comprises the component type (wired output) and a consecutive number.
Name	Unique name of the wired output
Type	Type of the wired output
Status	Current status of the wired output
Attributes	Attributes of the wired output

Configuring wired outputs



Note

Secvest has up to four wired outputs.

Editing outputs

1. Click in the line of the desired output.



Note

It is useful to assign unique output names so that if a fault occurs it is easier to identify the affected output.

2. **Delete** the preset name.
3. Assign a unique name for the output with max. 12 characters.
4. Confirm the selection once the configuration is complete by selecting **Submit**.

Inverting outputs (polarity)



Note

You can choose here whether the function of the output in question is inverted or not. Select **Normal** or **Inverted**.

Selecting the output type



Note

This selection field also provides the option of automatically arming or disarming the alarm panel at a specific time.
An overview of the different output types can be found in the following table.

1. Select menu item **Type**.

Configuration

Type	Explanation	Can be assigned to partitions
Not Used	This output is not used and not activated at any time.	Yes
Burglar Alarm	This output is activated when one of the following zone types or events is triggered and the system is armed: <ul style="list-style-type: none">• Normal Alarm• Tamper (only when system is armed)• Entry Route• Tamper zone (only when system is armed)• Entry delay expired• 24 Hour Alarm (only when system is armed)	Yes
Burg Confirm Alarm	This type only functions when confirmation mode BS8243 is selected under "System -> Confirmation". A confirmed burglar alarm has occurred (normal alarm). The alarm panel activates the output when: <ul style="list-style-type: none">• Two "normal alarms" are triggered in the same partition during the confirmation time• A "normal alarm" and a tamper alarm are triggered in the same partition during the confirmation time. This output type can be used for one or more partitions. Note that "normal alarms" and tamper alarms must be located in the same partition as the output. The output is deactivated when a user resets the system.	Yes
Burg Confirm Timer	This output is activated while the timer for confirmation of a burglar alarm is running and is deactivated as soon as the timer stops.	No
Perimeter Warning	The output is activated when a perimeter warning is triggered.	Yes
Hold Up Alarm	This output is activated when a hold up alarm is triggered.	Yes

Type	Explanation	Can be assigned to partitions
HUA Confirm	<p>A confirmed hold up alarm has occurred. The alarm panel activates the output under the following conditions:</p> <ul style="list-style-type: none"> • Users trigger an alarm at at least two different hold up transmitters during the hold up confirmation time. • A hold up transmitter is activated and a tamper alarm of a hold up transmitter is triggered during the confirmation time. <p>This output type can be assigned to one or more partitions. Note that the hold up transmitter (and tamper alarms) must be assigned to the same partition. The output is deactivated as soon as a user resets the system.</p>	No
HUA Confirm Timer	This output is activated while the timer for confirmation of a hold up alarm is running and is deactivated as soon as the timer has expired.	No
Duress Code	A duress code has been used. The alarm panel activates the output as soon as a user enters a duress code and deactivates the output again when the user resets the system.	Yes
Confirmed Alarm	This output is activated when an alarm is interrupted by the user in the selected partition during the possible time period. The output is deactivated again when the alarm is confirmed.	Yes
Fire Alarm	This output is activated when a fire alarm is triggered.	Yes
Technical Alarm	This output is activated when a zone with the attribute "Technical Alarm" triggers an alarm. It is only deactivated again when the zone triggering the alarm is reset (cause for the technical alarm has been corrected) AND the user confirms the technical alarm on the alarm panel with a valid code.	Yes
24 Hour Alarm	This output is activated when a zone with the attribute "24 Hour Alarm" triggers an alarm.	Yes
Zone Alarm	This output is activated when the selected zone reports an alarm and is deactivated again when the alarm is reset.	No

Configuration

Type	Explanation	Can be assigned to partitions
External Siren	This output is activated when there is a local alarm in the selected partition for the set siren time of the external siren. The output does not activate for a technical alarm or hold up alarm.	Yes
Internal Siren	This output is activated when there is a local alarm in the selected partition for the set siren time of the internal siren. The output does not activate for a technical alarm or hold up alarm.	Yes
External Strobe	This output is activated when there is a local alarm in the selected partition and remains activated until the wireless alarm panel is disarmed. The output is also activated for 10 seconds after the partition has been successfully armed if the EXTERNAL strobe signal for confirmation has been activated.	Yes
Internal Strobe	This output is activated when there is a local alarm in the selected partition and remains activated until the wireless alarm panel is disarmed. The output is also activated for 10 seconds after the partition has been successfully armed if the INTERNAL strobe signal for confirmation has been activated.	Yes
Alarm Abort	The output is activated when an alarm is interrupted by the user in the selected partition during the possible time period. The output is deactivated as soon as the alarm is confirmed.	Yes
Medical Alarm	This output is activated when a medical emergency call is triggered.	Yes
Social Care	This output is activated when a social care call is triggered.	Yes
Tamper	The output is activated when the alarm panel receives a tamper alarm from one of the following devices: <ul style="list-style-type: none">• Alarm panel (cover or wall tampering)• Control device (cover or wall tampering)• Zone with zone type "Tamper"• All wireless detectors or WAM• Sirens The alarm panel deactivates the output as soon as the cause of tampering has been corrected.	Yes

Type	Explanation	Can be assigned to partitions
RF Fault	This output is activated as soon as one of the three RF faults listed below occur: RF Low Battery, RF Supervision and RF Jamming. The output is deactivated only when the fault is reset on the alarm panel.	Yes
RF Supervision	This output is activated as soon as any wireless zone reports a monitoring failure (supervision fault). The output remains activated until all supervision faults have stopped.	Yes
RF Jamming	The corresponding output is activated when signal jamming is detected. The output remains activated until the signal jamming is corrected.	No
RF Low Battery	The output is activated as soon as a wireless detector sends a low battery message. The output remains activated until all detectors no longer send this message.	Yes
Battery Fault	The output is activated when the alarm panel identifies a fault with the backup battery OR a zone with zone type "Ext PSU Batt Fault" is triggered. If the alarm is triggered by a zone with "Ext PSU Batt Fault" the alarm panel only deactivates the output when the zone itself is reset and the user confirms the fault with a valid code on the alarm panel. If the alarm is triggered by a fault with the backup battery, the output is only deactivated again as soon as the alarm panel detects a suitable and functioning battery. Note: check the function of the battery using the test function available in the menu on the alarm panel.	No
A/C fault	The output is activated when the alarm panel does not have voltage OR any zone with type "Ext PSU A/C fault" is triggered. The delay until this output is activated depends on the value set under "System -> A/C fault Delay (minutes)".	No

Configuration

Type	Explanation	Can be assigned to partitions
Ext PSU Fault	<p>The output is activated when an external power supply detects a fault and reports the fault using zone type "Ext PSU Fault".</p> <p>The output is only deactivated when the fault is corrected and the user confirms the alarm with a valid code on the alarm panel.</p>	No
Ext PSU Low Volts	<p>The output is activated when an external power supply detects a correspondingly low voltage using zone type "Ext PSU Low Volts".</p> <p>The alarm panel deactivates the output as soon as the zone is reset and the user confirms the fault with a valid code.</p>	No
General Fault	<p>The output is activated as soon as an event occurs that causes a fault.</p> <p>This includes:</p> <ul style="list-style-type: none">• RF Low Battery• RF Supervision• RF Jamming• A/C Fault• Battery Fault• Ext PSU Fault• Tamper <p>Note that in the event of an A/C Fault the output is already activated a few seconds after the fault is detected and is NOT influenced by the set delay time.</p>	Yes
Fault comm. path	<p>The output is activated as soon as the alarm panel identifies a fault in the communication method and is deactivated when the fault no longer exists.</p>	No
Full Set Ready	<p>This output is activated when the partition is ready to be armed.</p> <p>If a detector is assigned to more than one partition, the partition in question is ready even if this detector is still open.</p>	Yes
Full Setting Complete	<p>The output is activated as soon as the system is successfully armed. The output is activated for approx. 10 seconds.</p>	Yes

Type	Explanation	Can be assigned to partitions
Full Set	This output is only activated when all of the partitions configured in the system are armed.	Yes
Setting Complete	This output is activated (for approx. 10 seconds) when the system or partition is armed or internally armed.	Yes
Armed	This output is activated when the partition is armed. The output is activated for approx. 10 seconds.	Yes
Rearmed	The output is activated in an internally armed system when the system is rearmed at least once. If the confirmation mode has been set to DD243 or BS8243, the alarm panel activates the output as soon as the system is rearmed (after the confirmation timer). If the confirmation mode "Basic" is selected, the alarm panel activates the output as soon as the system is rearmed (after the siren time has expired). In a system with partitions, the output can be assigned to different partitions. The output is deactivated again when a user or installer resets the system or the partition.	Yes
Part Set Ready	This output is activated when the partition is ready to be internally armed. If a detector is assigned to more than one partition, the partition in question is ready even if this detector is still open.	Yes
Part Setting Complete	This output is activated (for approx. 10 seconds) when the system or partition is INTERNALLY armed.	Yes
Part Set	This output is activated when a partition is internally armed.	Yes
Set Fault	This output is activated when arming fails. It remains activated until the user confirms the fault.	Yes
Autoset Warning	This output is activated when the warning time for automatic arming is running. (See menu "Schedulers Set/Unset".) This output is deactivated when the system is armed or a user delays or cancels automatic arming.	Yes

Configuration

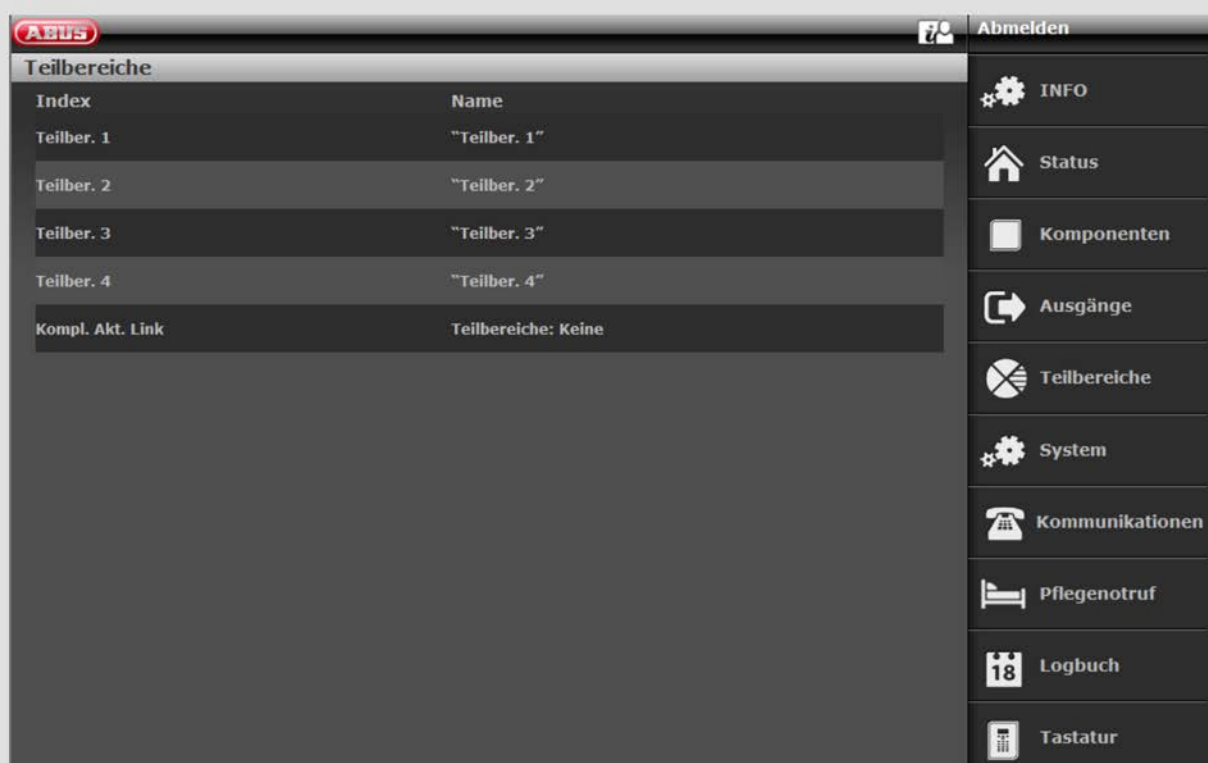
Type	Explanation	Can be assigned to partitions
Unset Complete	The output is activated as soon as the system is disarmed or deactivated after an alarm. The output is activated for approx. 10 seconds.	Yes
Zone Omit (Setting)	This output is activated when the user omits a zone while arming the system. The output is deactivated as soon as the alarm panel resets the zone.	Yes
Zone Omit (System)	(Output only functions when confirmation mode DD243 or BS8243 is selected.) When there is an unconfirmed alarm the alarm panel rearms when the confirmation time has expired. When the zone that triggered the unconfirmed alarm is still open at the time of rearming, the alarm panel omits this zone and activates this output. The alarm panel restores the zone and resets the output when a user or installer resets the system.	
Entry Exit Follow	This output is activated for the duration of the delay time (entry delay or exit delay). The output is not activated if the partition has been configured in "Instant Set" or "Silent Set" mode.	Yes
Lockset Unlocked	A zone lock exists. The alarm panel activates the output as soon as a zone with type "Zone Lock" is triggered and deactivates the output when the zone is closed.	No
Open/Close	The output is activated when the system (or partition) is disarmed. It is deactivated when the system (or partition) is armed. If this output is assigned to more than one partition, it is deactivated as soon as one of these partitions is armed or internally armed. Note: the function of this output is already inverted by default compared to the other outputs. There are 0 volts at this output when the system is disarmed.	Yes

Type	Explanation	Can be assigned to partitions
Zone Follow	This output follows the status of a zone. If this type is selected, an overview of the zones is provided. Select a corresponding zone.	No
User Defined	This zone can be controlled remotely via different user-defined components such as remote control or code keypad. The output can also be assigned a time at which it should be activated or deactivated. If this output type is selected, the time at which the output is activated or deactivated again can be entered in the connection.	No
Courtesy Light	This output is activated while the entry/exit delay time is running and deactivated 10 seconds after the entry/exit delay time has expired.	Yes
Installer on Site	The output is activated as soon as the alarm panel is in installer mode and deactivated as soon as the installer has successfully exited this menu.	No
Walk Test	The output is activated when a user starts a walk test both as an installer and as a normal user. The output is also activated in the time between an alarm being muted and the alarm confirmation.	No
Smoke Sensor Reset	This output is always activated (0 V) except when a user confirms a fire alarm. After this confirmation, the alarm panel deactivates the output for 3 seconds. The output type is designed to facilitate interaction with low voltage reset connections on wired smoke detectors. Note that there are also smoke detectors common on the market that require a second confirmation in order to be reset (detectors that require time to reset the alarm contacts after the reset pulse).	Yes

Configuration

Type	Explanation	Can be assigned to partitions
PIR Set Latch	<p>This type requires the system or partition to have been armed.</p> <p>This output is deactivated when the system or partition is disarmed or an alarm event occurs.</p> <p>The output is activated for one second when either the system is reset or installer mode is exited on the alarm panel.</p> <p>Note: if "Normal" polarity is selected, the output is actuated with +12 V when activated and 0 V when deactivated. Use the "Inverted" polarity to reverse the function of this output.</p>	Yes

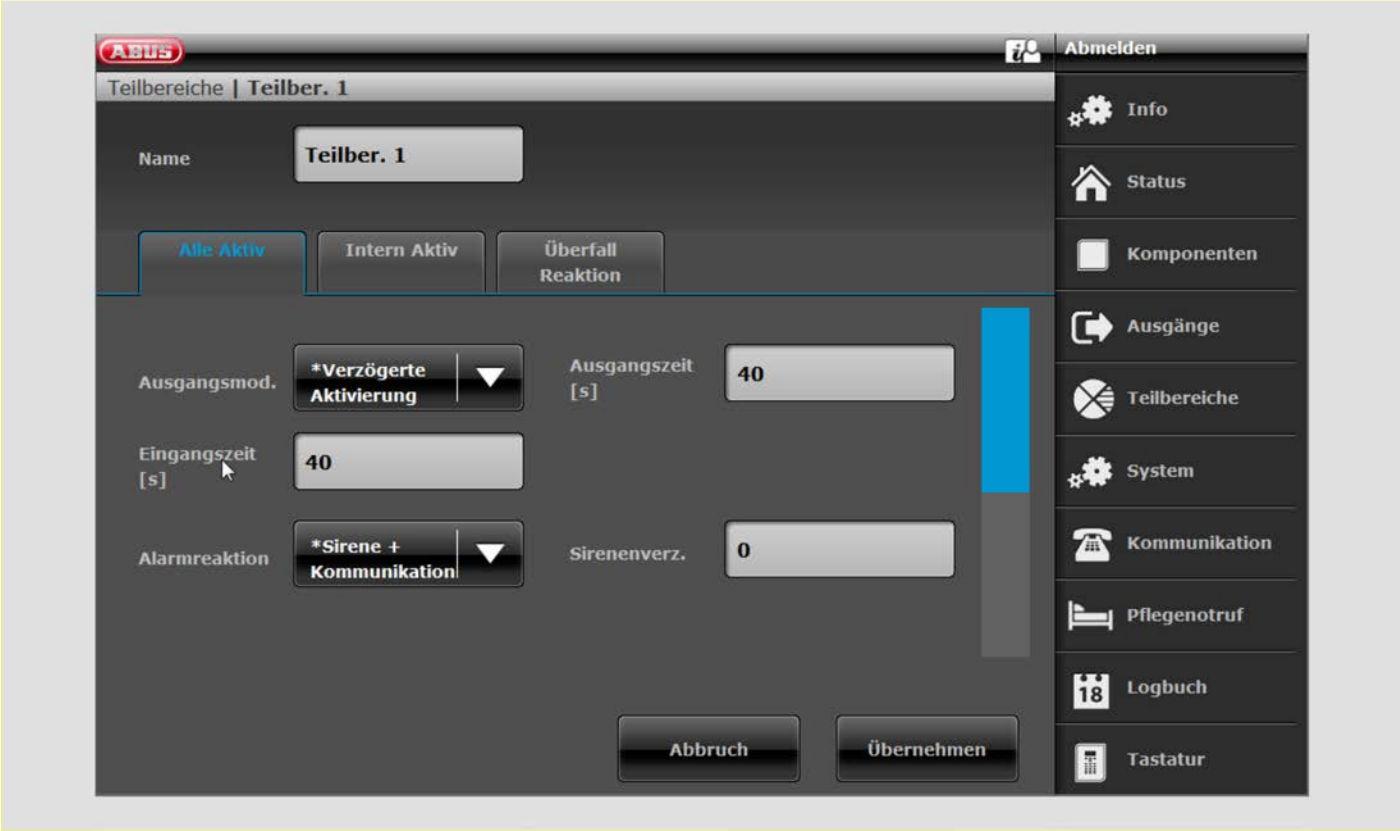
Partitions



Name/function	Explanation
Index	List of partitions Partition 1 to partition 4 and Full set link
Name	Name of the partition assigned during configuration. The selected partitions appear in the "Full set link" line.
Full set link	Use this option to define a common partition. Partition 1 is always the common partition. Partition 1 can be connected (linked) to other partitions. This means that when all connected partitions are armed, partition 1 is also automatically armed. The system responds to an alarm according to the configured alarm response for partition 1.

Configuring partitions

Full Set

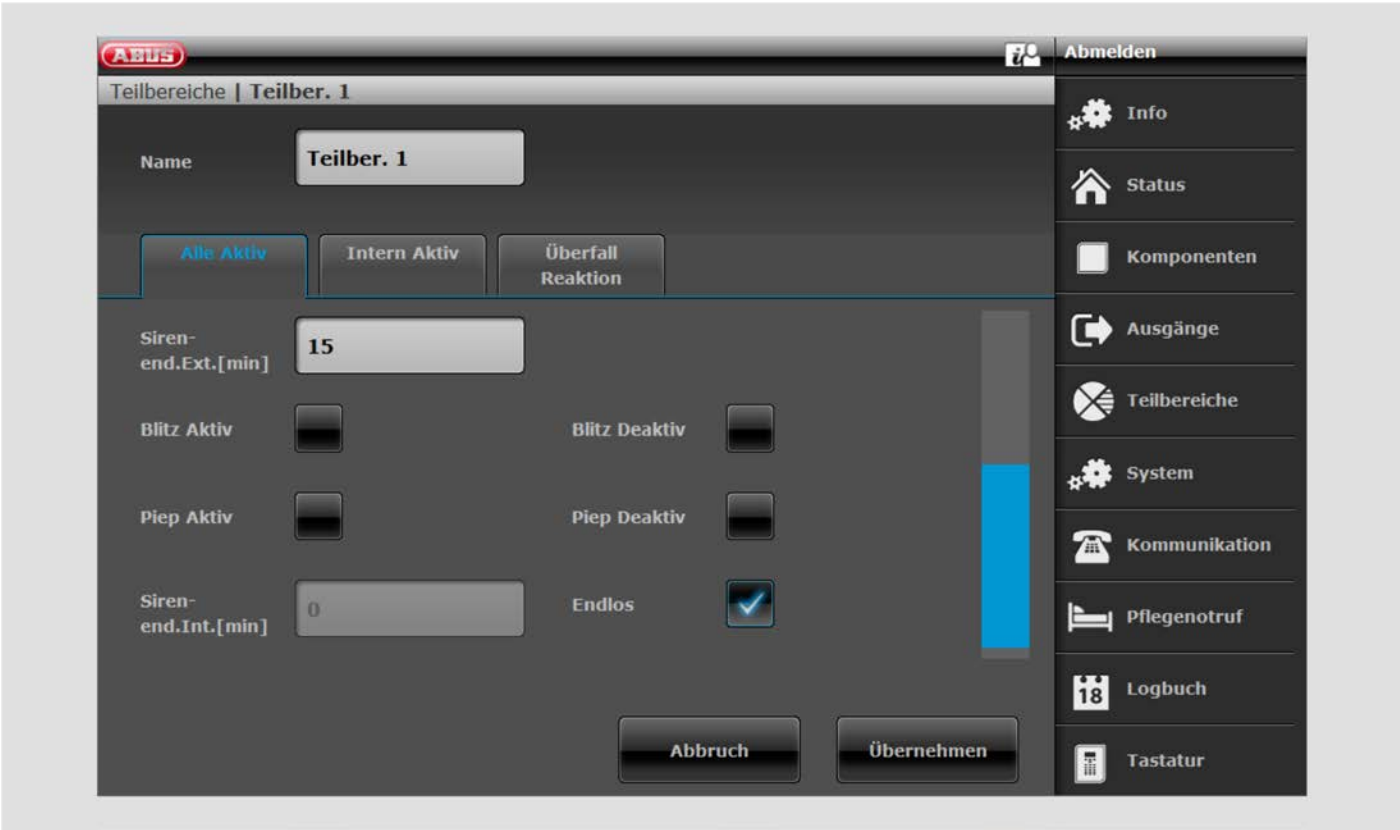


Name/function	Explanation
Name	Unique name of the partition. The partition can be assigned an individual name here, e.g. apartment, workshop, office. Max. 12 characters are allowed. The alarm panel displays this name during arming.
Full Set	Settings for the complete arming of the partition
Exit Mode	Select the mode of arming when exiting the premises. Timed Set <ul style="list-style-type: none">Use this option to arm the partition only after a set delay time. Under "Exit time" select the corresponding time. The alarm panel logs the start of this timed arming.This option does not comply with BS8243:2010.

Name/function	Explanation
Exit Mode, cont.	<p>Final Door Set</p> <ul style="list-style-type: none"> • Use this option to complete arming of a partition by closing the last exit door. This door has a detector with zone type "Final Door". When the door is closed, the partition is armed once the settle time has expired. • Note that the exit time for this option is unlimited, i.e. when the zone is closed (closed door) the alarm panel waits until this zone is opened and then closed again before arming. • The alarm panel saves the start time of arming (and not the arming itself) in the log book. • Do not attempt to use a PIR zone as a "Final Door" for a partition. PIR wireless detectors has a "lock" time period after each arming, in order to save battery power. If a partition is armed (or internally armed), a PIR detector may still be locked. During this time it cannot send signals to complete the arming process. <p>Instant Set</p> <ul style="list-style-type: none"> • The partition is armed immediately without any acoustic warning tone. If the partition has been armed, an acoustic confirmation sounds. • Note: This option does not comply with BS8243:2010. <p>Silent Set</p> <ul style="list-style-type: none"> • The partition is armed after the exit time has expired. Under "Exit time" select the corresponding time. However, no warning tone sounds during this time. If the partition has been armed, an acoustic confirmation sounds. The alarm panel saves the start time in the log book. • During entry time the acoustic warning tone can be heard. • Note: This option does not comply with BS8243:2010. <p>Lock Set</p> <ul style="list-style-type: none"> • The "Lock Set" mode affects both arming and disarming of the partition. For this mode, a detector with zone type "Lock Set" and a detector with zone type "Final Door" must be assigned at the last exit door. The detector with zone type "Lock Set" is operated with a lock switch contact on a suitable lock. <p>Arming the partition</p> <ul style="list-style-type: none"> • The user must first start the arming sequence using the user code, proximity keyfob or remote control. The alarm panel then sounds the exit tone and saves the start time in the log book. If the "Final Door" zone is open, the alarm panel emits a continuous exit tone. The exit tone sounds until the user: <ul style="list-style-type: none"> a) closes the last exit door and then b) locks the door and therefore activates the lock switch contact. After the lock switch contact is activated, the partition is armed once the settle time has expired. The "Final Door" zone is also converted into a "Normal Alarm" zone. The alarm panel saves the activation of the "Lock Set" zone in the log book.

Name/function	Explanation
Exit Mode, cont.	<p>Disarming the partition</p> <ul style="list-style-type: none"> The user unlocks the door and therefore activates the lock switch contact. The "Lock Set" zone is opened. The alarm panel saves the activation of the "Lock Set" zone in the log book. The original "Final Door" zone which was converted into a "Normal Alarm" zone is switched back into a "Final Door" zone. The entry time starts when the door is opened. The entry tone sounding at this point is different from a normal entry tone. If the user locks the door again without starting the entry time, the alarm panel remains armed and the "Final Door" zone is converted again into a "Normal Alarm" zone. The alarm panel stops the warning tone. To comply with BS8243, "After Entry" must be set to "Never" in order to prevent confirmation. <p>Exit Terminate</p> <ul style="list-style-type: none"> Arming the partition The user must first start the arming sequence. Then the user ends the arming process after exiting the monitoring area. The user can start the arming sequence using the user code, proximity keyfob or remote control. (Note: arming with remote control must not be set to "Instant", Installer Mode->System->User Access->Remote Inst. Set). The user ends arming by activating a zone with type "Exit Terminate" (see explanation of zone types). Note that the exit time is unlimited with this option, i.e. the alarm panel waits until it receives the signal to end the arming process before it arms. The alarm panel emits the exit tone during this time. The alarm panel saves the start time of arming (and not the arming itself) in the log book. The partition is armed after the settle time has expired. Disarming the partition The user can use the remote control. The user can also open the door. The "Final Door" zone at this door starts the entry time. During entry time the user must disarm the partition using the user code or proximity keyfob at the alarm panel or control device. (The last method is not compliant with BS8243 clause 6.4.) <p>As Prtn 1</p> <p>This option is available for partitions 2, 3 and 4. If this option is selected, the alarm panel uses the same type as for partition 1.</p>

Name/function	Explanation
Settle Time	<p>This option only appears for modes "Final Door Set", "Lock Set" and "Exit Terminate".</p> <p>Use this option to define a time delay so that detectors can settle before the partition is armed. This may be necessary if detectors have triggered, send an alarm signal and have still not been reset. During this time the alarm panel ignores alarm signals from detectors and sirens are not triggered. Enter the time in seconds as a 2-digit number: 01–30. The factory default for the settle time is 15 s. In this time the wireless PIRs located at the exit which have triggered can settle and be reset.</p>
Exit Time [s]	<p>This option only appears for modes "Timed Set" and "Silent Set".</p> <p>Time for the exit delay in seconds</p> <p>The exit time can be any value between 10 s and 120 s.</p>
Entry Time [s]	<p>Time for the entry delay in seconds</p> <p>The entry time can be any value between 10 s and 120 s.</p>
Alarm Response	<p>Select the response here for when an alarm occurs in this partition.</p> <p>Internal</p> <ul style="list-style-type: none"> • Alarm panel, indoor siren, info module and control device. <p>Siren</p> <ul style="list-style-type: none"> • Alarm panel, indoor siren, info module and control device. • External Sirens. <p>Siren + Comms</p> <ul style="list-style-type: none"> • Alarm panel, indoor siren, info module and control device. • External Sirens. • Communications. <p>A siren delay only goes into effect for alarm response "Siren + Comms".</p>
Siren Delay	<p>Time for the delay duration of the siren(s).</p> <p>The siren delay can be set to a value between 0 and 10 min.</p> <p>When an alarm has been triggered the alarm panel waits until this time has expired before it activates the sirens.</p> <p>Note</p> <p>The siren delay only goes into effect when the alarm response includes comms. The siren delay does not go into effect when a comms fault occurs.</p> <p>The siren delay does not go into effect when "Installer Mode->System->Confirmation->Confirmation Mode->DD243 or BS8243" <u>and</u> "Installer Mode->System->Confirmation->Siren On ->Unconfirm" are set.</p> <p>If sounders are assigned to multiple partitions, the alarm panel uses the shortest siren delay set for the partitions in question.</p>



Name/function	Explanation
Siren time ext. [min]	<p>Time for the duration of the external siren(s) in minutes.</p> <p>The siren time can be set to a value between 0 and 15 min.</p> <p>If sounders are assigned to multiple partitions, the alarm panel uses the longest siren time set for the partitions in question.</p>
Strobe on Set	<p>On</p> <p>After successfully arming the partition, there is one visual acknowledgement on the wireless external siren.</p> <p>"Strobe" outputs are activated for 10 s after successfully arming the partition.</p> <p>Off</p> <p>After successfully arming the partition, there is no visual acknowledgement on the wireless external siren.</p>
Strobe on Unset	<p>On</p> <p>After successfully disarming the partition, there is one visual acknowledgement on the wireless external siren.</p> <p>"Strobe" outputs are activated for 10 s after successfully arming the partition.</p> <p>Off</p> <p>After successfully disarming the partition, there is no visual acknowledgement on the wireless external siren.</p>

Name/function	Explanation
Beep on Set	<p>On</p> <p>After successfully arming the partition, there is one acoustic acknowledgement on the wireless external siren.</p> <p>"Siren" outputs are activated for 10 s after successfully arming the partition.</p> <p>Off</p> <p>After successfully arming the partition, there is no acoustic acknowledgement on the wireless external siren.</p>
Beep on Unset	<p>On</p> <p>After successfully disarming the partition, there is one acoustic acknowledgement on the wireless external siren.</p> <p>"Siren" outputs are activated for 10 s after successfully arming the partition.</p> <p>Off</p> <p>After successfully disarming the partition, there is no acoustic acknowledgement on the wireless external siren.</p>
Siren time int. [min]	<p>Time for the duration of the internal siren(s) in minutes after a burglar alarm. The siren time can be set to a value between 0 and 20 min.</p> <p>If sounders are assigned to multiple partitions, the alarm panel uses the longest siren time set for the partitions in question.</p> <p>Note</p> <p>Internal sirens always sound after a fire or hold up alarm until the alarm is confirmed by a user for safety reasons.</p> <p>For safety reasons there is no time limit for a fire alarm or hold up alarm.</p> <p>Special response when an entry delay is used:</p> <p>Requirement</p> <ul style="list-style-type: none"> • The internal sounders (alarm panel, wireless indoor siren, wireless info module) are muted again after the internal siren time has expired. • The alarm panel has automatically rearmed. • (See also "Installer Mode → System -> Security → Auto Rearm".) <p>Response</p> <ul style="list-style-type: none"> • If you now enter the entrance area ("Final Door" and "Entry/Exit Follow" detectors are opened), the internal sounders (alarm panel, wireless indoor siren, wireless info module) emit an alarm tone. • The normal entry tone is not signalled in this case.

Configuration

Name/function	Explanation
Siren time int. [min], cont.	<p>Note</p> <p>When the entry delay is used, you would usually expect to hear the normal entry tone.</p> <p>This entry tone should be heard as long as the entry delay is running.</p> <p>If you hear an alarm tone after opening the entrance door, you know immediately that the alarm panel has detected an intrusion during your absence.</p> <p>The delay time runs anyway. Disarm the alarm panel within the delay time.</p> <p>Do so only if you feel it is safe, however. An intruder could still be inside the property!</p> <p>If you do not disarm the system, an additional burglar alarm is triggered once the delay time has expired.</p> <p>Notify others who have access to your property of this response of the alarm panel.</p>
Endless	<p>On</p> <p>Internal sirens signal the alarm tone until an alarm is confirmed by a user.</p> <p>Off</p> <p>The time for the duration of the internal siren(s) is used.</p>

Configuring partitions

Part Set

The screenshot shows the ABUS configuration interface for 'Teilbereiche | Teilber. 1'. The interface is divided into a main configuration area and a sidebar on the right. The main area includes fields for 'Name' (Teilber. 1), 'Ausgangsmod.' (set to *Sofort Aktivierung), 'Alarmreaktion' (set to *Sirene), 'Siren- end.Ext.[min]' (set to 15), 'Eingangszeit [s]' (set to 40), 'Sirenenverz.' (set to 0), and 'Ein/Aus bei Intern als' (set to *Ein/Ausgang). There are buttons for 'Alle Aktiv', 'Intern Aktiv' (highlighted), and 'Überfall Reaktion'. At the bottom are 'Abbruch' and 'Übernehmen' buttons. The sidebar on the right contains a list of navigation options: Info, Status, Komponenten, Ausgänge, Teilbereiche, System, Kommunikation, Pflegenotruf, Logbuch, and Tastatur.

Name/function	Explanation
Name	<p>Unique name of the partition.</p> <p>The partition can be assigned an individual name here, e.g. apartment, workshop, office. Max. 12 characters are allowed.</p> <p>The alarm panel displays this name during arming.</p>
Part Set	Settings for the internal arming of the partition
Exit Mode	<p>Select the mode of internal arming when exiting the premises.</p> <p>Timed Set</p> <ul style="list-style-type: none"> Use this option to internally arm the partition only after a set delay time. Under "Exit time" select the corresponding time. The alarm panel logs the start of this timed internal arming. This option does not comply with BS8243:2010.

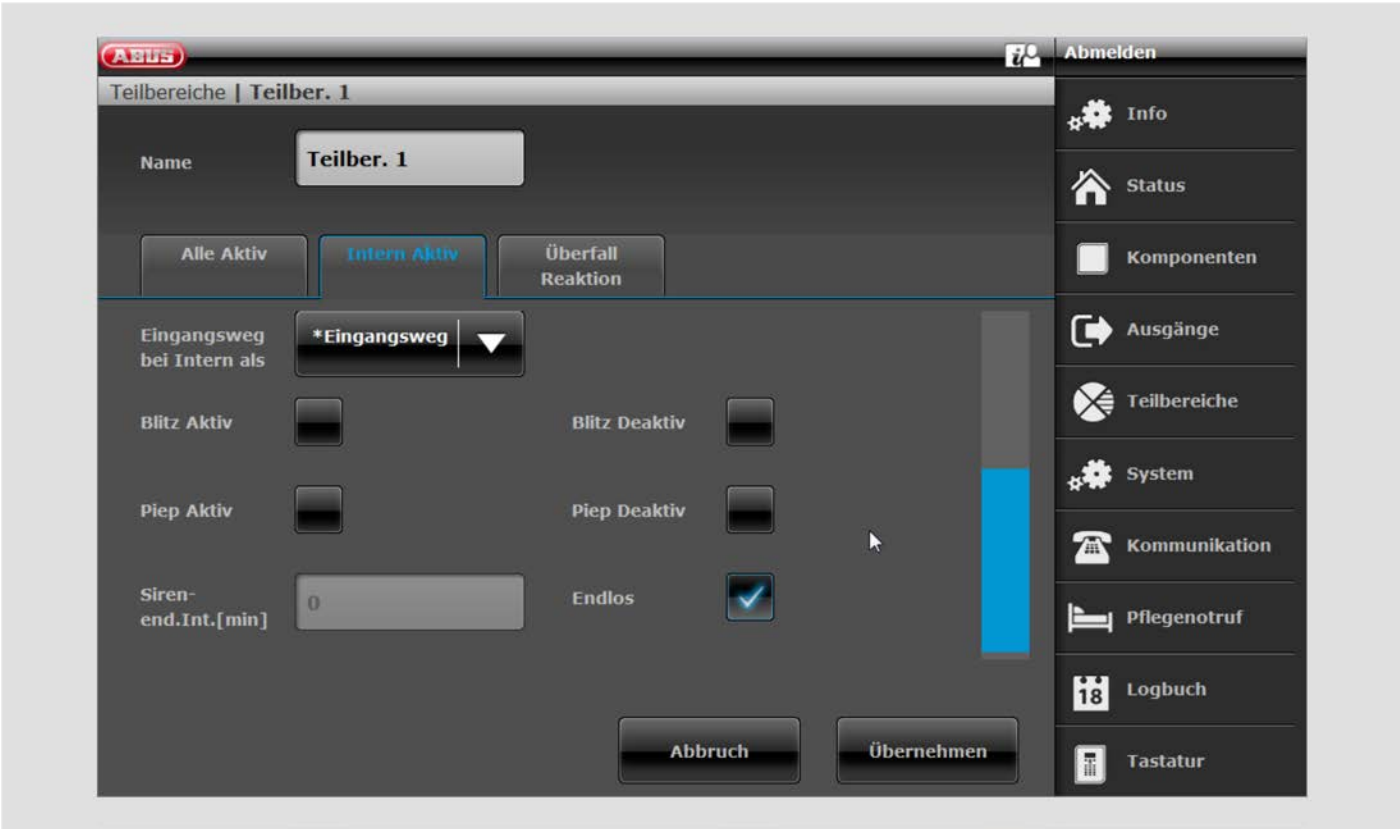
Name/function	Explanation
Exit Mode, cont.	<p>Final Door Set</p> <ul style="list-style-type: none">• Use this option to complete internal arming of a partition by closing the last exit door. This door has a detector with zone type "Final Door". When the door is closed, the partition is internally armed once the settle time has expired.• Note that the exit time for this option is unlimited, i.e. when the zone is closed (closed door) the alarm panel waits until this zone is opened and then closed again before internally arming.• The alarm panel saves the start time of internal arming (and not the internal arming itself) in the log book.• Do not attempt to use a PIR zone as a "Final Door" for a partition. PIR wireless detectors has a "lock" time period after each arming, in order to save battery power. If a partition is armed (or internally armed), a PIR detector may still be locked. During this time it cannot send signals to complete the arming process. <p>Instant Set</p> <ul style="list-style-type: none">• The partition is internally armed immediately without any acoustic warning tone. If the partition has been internally armed, an acoustic confirmation sounds.• Note: This option does not comply with BS8243:2010. <p>Silent Set</p> <ul style="list-style-type: none">• The partition is internally armed after the exit time has expired. Under "Exit time" select the corresponding time. However, no warning tone sounds during this time. If the partition has been internally armed, an acoustic confirmation sounds. The alarm panel saves the start time in the log book.• During entry time the acoustic warning tone can be heard.• Note: This option does not comply with BS8243:2010. <p>Lock Set</p> <ul style="list-style-type: none">• The "Lock Set" mode affects both internal arming and disarming of the partition.• For this mode, a detector with zone type "Lock Set" and a detector with zone type "Final Door" must be assigned at the last exit door. The detector with zone type "Lock Set" is operated with a lock switch contact on a suitable lock.

Name/function	Explanation
Exit Mode, cont.	<p>Internally arming the partition</p> <ul style="list-style-type: none"> The user must first start the arming sequence using the user code, proximity keyfob or remote control. <p>The alarm panel then sounds the exit tone and saves the start time in the log book.</p> <p>If the "Final Door" zone is open, the alarm panel emits a continuous exit tone. The exit tone sounds until the user:</p> <ol style="list-style-type: none"> closes the last exit door and then locks the door and therefore activates the lock switch contact. <p>After the lock switch contact is activated, the partition is internally armed once the settle time has expired.</p> <p>The "Final Door" zone is also converted into a "Normal Alarm" zone.</p> <p>The alarm panel saves the activation of the "Lock Set" zone in the log book.</p> <p>Disarming the partition</p> <ul style="list-style-type: none"> The user unlocks the door and therefore activates the lock switch contact. The "Lock Set" zone is opened. The alarm panel saves the activation of the "Lock Set" zone in the log book. The original "Final Door" zone which was converted into a "Normal Alarm" zone is switched back into a "Final Door" zone. The entry time starts when the door is opened. The entry tone sounding at this point is different from a normal entry tone. If the user locks the door again without starting the entry time, the alarm panel remains armed and the "Final Door" zone is converted again into a "Normal Alarm" zone. The alarm panel stops the warning tone. To comply with BS8243, "After Entry" must be set to "Never" in order to prevent confirmation. <p>Exit Terminate</p> <p>Internally arming the partition</p> <ul style="list-style-type: none"> The user must first start the arming sequence. Then the user ends the arming process after existing the monitoring area. The user can start the arming sequence using the user code, proximity keyfob or remote control. (Note: arming with remote control must not be set to "Instant", Installer Mode->System->User Access->Remote Inst. Set). The user ends arming by activating a zone with type "Exit Terminate" (see explanation of zone types). Note that the exit time is unlimited with this option, i.e. the alarm panel waits until it receives the signal to end the arming process before it arms. The alarm panel emits the exit tone during this time. The alarm panel saves the start time of arming (and not the arming itself) in the log book. The partition is armed after the settle time has expired.

Configuration

Name/function	Explanation
Exit Mode, cont.	Disarming the partition <ul style="list-style-type: none">The user can use the remote control. The user can also open the door. The "Final Door" zone at this door starts the entry time. During entry time the user must disarm the partition using the user code or proximity keyfob at the alarm panel or control device. (The last method is not compliant with BS8243 clause 6.4.) As Prtn 1 <p>This option is available for partitions 2, 3 and 4. If this option is selected, the alarm panel uses the same type as for partition 1.</p>
Settle Time	<p>This option only appears for modes "Final Door Set", "Lock Set" and "Exit Terminate". Use this option to define a time delay so that detectors can settle before the partition is internally armed.</p> <p>This may be necessary if detectors have triggered, send an alarm signal and have still not been reset.</p> <p>During this time the alarm panel ignores alarm signals from detectors and sirens are not triggered.</p> <p>Enter the time in seconds as a 2-digit number: 01–30. The factory default for the settle time is 15 s.</p> <p>In this time the wireless PIRs located at the exit which have triggered can settle and be reset.</p>
Exit Time [s]	<p>This option only appears for modes "Timed Set" and "Silent Set".</p> <p>Time for the exit delay in seconds.</p> <p>The exit time can be any value between 10 s and 120 s.</p>
Entry Time [s]	<p>Time for the entry delay in seconds.</p> <p>The entry time can be any value between 10 s and 120 s.</p>
Alarm Response	<p>Select the response here for when an alarm occurs in this partition.</p> Internal <ul style="list-style-type: none">Alarm panel, indoor siren, info module and control device. Siren <ul style="list-style-type: none">Alarm panel, indoor siren, info module and control device.External Sirens. Siren + Comms <ul style="list-style-type: none">Alarm panel, indoor siren, info module and control device.External Sirens.Communications.A siren delay only goes into effect for alarm response "Siren + Comms".

Name/function	Explanation
Siren Delay	<p>Time for the delay duration of the siren(s). The siren delay can be set to a value between 0 and 10 min. When an alarm has been triggered the alarm panel waits until this time has expired before it activates the sirens.</p> <p>Note The siren delay only goes into effect when the alarm response includes comms. The siren delay does not go into effect when a comms fault occurs. The siren delay does not go into effect when "Installer Mode->System ->Confirmation->Confirmation Mode->DD243 or BS8243" and "Installer Mode->System->Confirmation->Siren On ->Unconfirm" are set. If sounders (or just control devices?) are assigned to multiple partitions, the alarm panel uses the shortest siren delay set for the partitions in question.</p>
Siren time ext. [min]	<p>Time for the duration of the external siren(s) in minutes. The siren time can be set to a value between 0 and 15 min. If sounders (or just control devices?) are assigned to multiple partitions, the alarm panel uses the longest siren time set for the partitions in question. The time that the sounders are active for may also be extended by the longest of the siren delays that the assigned partitions possess.</p>
Pt.Set Final Exit	<p>This option controls how a "Final Door" zone is handled when the system is internally armed.</p> <p>Final Door</p> <ul style="list-style-type: none"> • Every zone in this partition with type "Final Door" and the attribute "Part Set" continues to function as a "Final Door" zone. <p>Normal Alarm</p> <ul style="list-style-type: none"> • Every zone in this partition with type "Final Door" and the attribute "Part Set" functions as a "Normal Alarm" zone.



Name/function	Explanation
Pt.Set Entry Route	<p>This option controls how an "Entry Route" zone is handled when the system is internally armed.</p> <p>Entry Route</p> <ul style="list-style-type: none">• Every zone in this partition with type "Entry Route" and the attribute "Part Set" continues to function as an "Entry Route" zone. <p>Final Door</p> <ul style="list-style-type: none">• Every zone in this partition with type "Entry Route" and the attribute "Part Set" functions as a "Final Door" zone.
Strobe on Set	<p>On</p> <p>After successfully internally arming the partition, there is one visual acknowledgement on the wireless external siren.</p> <p>"Strobe" outputs are activated for 10 s after successfully arming the partition.</p> <p>Off</p> <p>After successfully internally arming the partition, there is no visual acknowledgement on the wireless external siren.</p>
Strobe on Unset	<p>On</p> <p>After successfully disarming the partition, there is one visual acknowledgement on the wireless external siren.</p> <p>"Strobe" outputs are activated for 10 s after successfully arming the partition.</p> <p>Off</p> <p>After successfully disarming the partition, there is no visual acknowledgement on the wireless external siren.</p>

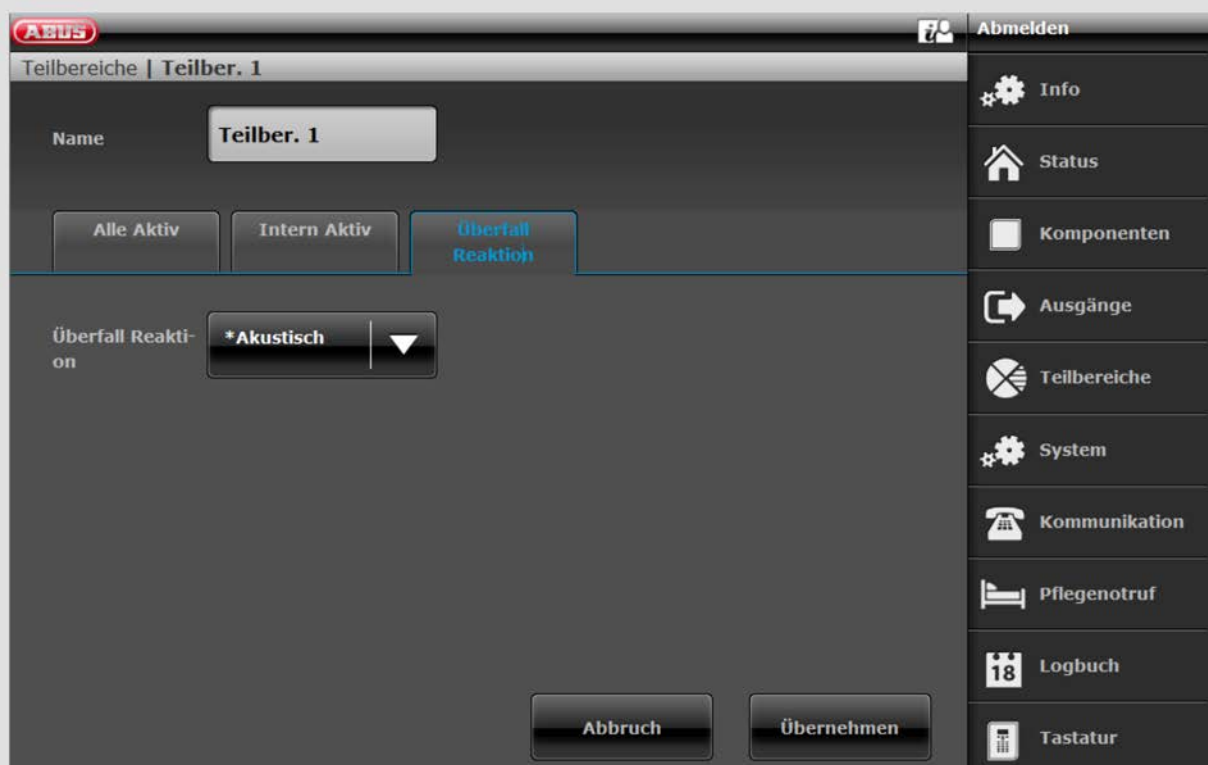
Name/function	Explanation
Beep on Set	<p>On</p> <p>After successfully internally arming the partition, there is one acoustic acknowledgement on the wireless external siren.</p> <p>"Siren" outputs are activated for 10 s after successfully arming the partition.</p> <p>Off</p> <p>After successfully internally arming the partition, there is no acoustic acknowledgement on the wireless external siren.</p>
Beep on Unset	<p>On</p> <p>After successfully disarming the partition, there is one acoustic acknowledgement on the wireless external siren.</p> <p>"Siren" outputs are activated for 10 s after successfully arming the partition.</p> <p>Off</p> <p>After successfully disarming the partition, there is no acoustic acknowledgement on the wireless external siren.</p>
Siren time int. [min]	<p>Time for the duration of the internal siren(s) in minutes after a burglar alarm. The siren time can be set to a value between 0 and 20 min.</p> <p>If sounders are assigned to multiple partitions, the alarm panel uses the longest siren time set for the partitions in question.</p> <p>Note</p> <p>For safety reasons, internal sirens always sound after a fire or hold up alarm until the alarm is acknowledged by a user, and there is no time limit for a fire alarm or hold up alarm.</p> <p>Special response when an entry delay is used</p> <p>Requirement</p> <ul style="list-style-type: none"> • The internal sounders (alarm panel, wireless indoor siren, wireless info module) are muted again after the internal siren time has expired. • The alarm panel has automatically rearmed (see also "Installer Mode → System -> Security → Auto Rearm"). <p>Response</p> <ul style="list-style-type: none"> • If you now enter the entrance area ("Final Door" and "Entry/Exit Follow" detectors are opened), the internal sounders (alarm panel, wireless indoor siren, wireless info module) emit an alarm tone. • The normal entry tone is not signalled in this case.

Configuration

Name/function	Explanation
Siren time int. [min], cont.	<p>Note</p> <p>When the entry delay is used, you would usually expect to hear the normal entry tone. This entry tone should be heard as long as the entry delay is running. If you hear an alarm tone after opening the entrance door, you know immediately that the alarm panel has detected an intrusion during your absence.</p> <p>The delay time runs anyway. Disarm the alarm panel within the delay time. Do so only if you feel it is safe, however. An intruder could still be inside the property! If you do not disarm the system, an additional burglar alarm is triggered once the delay time has expired.</p> <p>Notify others who have access to your property of this response of the alarm panel.</p>
Endless	<p>On</p> <p>Internal sirens signal the alarm tone until an alarm is acknowledged by a user.</p> <p>Off</p> <p>The time for the duration of the internal siren(s) is used.</p>

Configuring partitions

HUA response



Name/function	Explanation
Name	Unique name of the partition
HUA response	<p>Select here the type of signalling used for a hold up alarm in the selected partition:</p> <p>Audible</p> <ul style="list-style-type: none"> When a hold up alarm is triggered, communication is sent and the acoustic alarm is sounded via the applicable sounders and the connected sirens (according to the set siren time). A triangle warning appears on the alarm panel display to indicate the hold up alarm. Details are displayed after a user code is entered. The acoustic alarm is muted after a user code is entered. <p>Silent</p> <ul style="list-style-type: none"> The hold up alarm is only signalled using communication messages. There is no audible acoustic alarm. "Siren" and "Hold Up" outputs are not activated. The hold up alarm is not shown on the alarm panel display. The display only indicates the hold up alarm when a user operates the alarm panel.

Name/function	Explanation
HUA response, cont.	<p>Displayed</p> <ul style="list-style-type: none">• When a hold up alarm is triggered, communication is sent and the acoustic alarm is sounded via the applicable sounders and the connected sirens (according to the set siren time).• The hold up alarm and details are shown on the alarm panel display. (No user code must be entered to view the details.) The acoustic warning is triggered on the alarm panel at the same time. "Siren" and "Hold Up" outputs are activated. <p>Note</p> <p>No hold up alarms can be triggered or communicated when the system is in installer mode.</p>

System

General

ABUS System | Allgemeines

Display Text:

Meldung AC Störung: ☐

Meldung Ext DC Störung: ☒

Verz. AC Störung [min] (Minuten):

Verz. Ext DC Störung [min] (Minuten):

Abmelden

- Info
- Status
- Komponenten
- Ausgänge
- Teilbereiche
- System
- Kommunikation
- Pflegenotruf
- Logbuch
- Tastatur

Abbruch Übernehmen

Name/function	Explanation (checkbox)
Language	Only available on the alarm panel. Select the desired language with the desired version.
Display Text	Name (max. 20 characters) shown on the Secvest display.
Restore Defaults	<p>Only available on the alarm panel. This menu item resets the device back to its factory defaults. After confirmation the following menus appear:</p> <p>Language</p> <ul style="list-style-type: none"> • Deutsch x.yz • English x.yz • Duits x.yz • Francais x.yz • Dansk x.yt • etc. <p>Note Only the languages available for the corresponding article number are shown.</p>

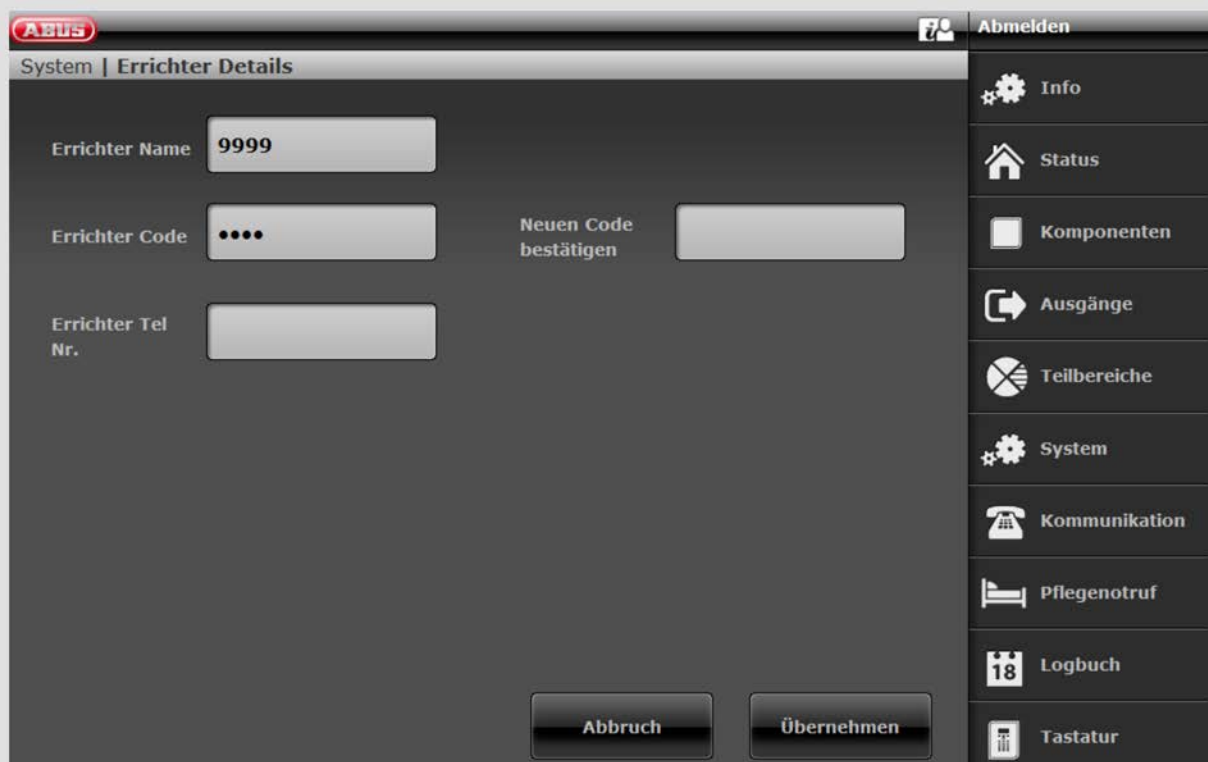
Name/function	Explanation (checkbox)
Factory Defaults	<div>Country Defaults<ul style="list-style-type: none">• UK• Italy• Spain• Portugal• Netherlands• France• Belgium• Germany• Switzerland• Austria• Ireland• Norway• Denmark• Sweden• Greece• Luxembourg</div> <div>Note<p>Every country has different settings for PSTN communication and alarm reporting or the start and end of summer/winter time (daylight saving time). Changing the country settings does not change the selected language.</p></div> <div>Access Code Length<ul style="list-style-type: none">• 4 Digit User Codes• 6 Digit User Codes</div> <div>Wired Zone Type<ul style="list-style-type: none">• 2-wire FSL 2K2/4K7• 2-wire FSL 1K/1K• 2-wire FSL 2K/2K• 2-wire FSL 4K7/4K7• 4-wire CC• 2-wire CC</div> <div>Overview<ul style="list-style-type: none">• IP address: 192.168.178.002• DHCP: on• Version: v1.01.01• S/N: SECVEST###E9000139AAE• Part No.: FUAA50000</div> <div>Note<p>Here you can see an overview of the most important data for the alarm panel.</p></div> <div>Login<ul style="list-style-type: none">• Installer<ul style="list-style-type: none">- Name (Web Server): 9999- Code: 9999• Administrator<ul style="list-style-type: none">- Name (Web Server): 1234- Code: 1234</div> <div>Note<p>Here you can see an overview of the current data for this user. The details are described in the individual chapters.</p></div>

Name/function	Explanation (checkbox)
Factory Defaults, cont.	<p>Note</p> <p>Restoring the factory defaults:</p> <ul style="list-style-type: none"> • deletes all taught-in and configured components, names and saved text and numbers • does not delete the log book • does not delete the users with their codes and components • does not delete the installer name or installer code
A/C Fault Reporting	<p>Activated</p> <p>Reports that a fault has occurred with the 230 V power supply.</p> <p>Deactivated</p> <p>Function not possible.</p>
A/C Fault Delay (minutes)	<p>Delay time in minutes (0–60 minutes) until the message is sent.</p> <p>If an A/C Fault occurs the alarm panel displays an error message after a few seconds, "General Fault" outputs activate and a log book entry is created (Mandatory Events).</p> <p>Power disruptions that last less than 9 s are not reported.</p> <p>If the power supply is restored within these 9 seconds, the "General Fault" outputs are reset and a log book entry is created: "Power supply restored".</p> <p>If the power disruption lasts longer than 9 s, the following occurs:</p> <ul style="list-style-type: none"> • If the value is set to 0 min, a warning tone is sounded after 10 s and the alarm panel reports the failure. • "A/C Fault" outputs are activated. • If the value is set to higher than 0 min, this timer is started 10 s after the disruption occurs. <p>If the power supply is restored before the end of the set delay time, "General Fault" outputs are reset and a log book entry is created about the power restore.</p> <p>No errors are reported.</p> <p>If the fault still exists after the end of the configured time, a warning tone sounds and the error is reported.</p> <p>"A/C Fault" outputs are activated.</p> <p>A user can stop the warning tone by entering their code.</p> <p>The alarm panel display shows details of the warning. "General Fault" and "A/C Fault" outputs remain activated.</p> <p>If the fault has been corrected, the alarm panel deactivates the "A/C Fault" outputs and creates a log book entry about the power restore.</p> <p>A user can reset the alarm and the "General Fault" outputs after entering their user code.</p>

Configuration

Name/function	Explanation (checkbox)
Ext DC Fault Reporting	Activated Reports that a fault has occurred with the external DC power supply. Deactivated Function not possible.
Ext DC Fault Delay (minutes)	<p>Delay time in minutes (0–60 minutes) until the message is sent.</p> <p>If a DC Fault occurs the alarm panel displays an error message after a few seconds, "General Fault" outputs activate and a log book entry is created (Mandatory Events).</p> <p>Power disruptions that last less than 9 s are not reported.</p> <p>If the power supply is restored within these 9 seconds, the "General Fault" outputs are reset and a log book entry is created: "Power supply restored".</p> <p>If the power disruption lasts longer than 9 s, the following occurs:</p> <ul style="list-style-type: none">• If the value is set to 0 min, a warning tone is sounded after 10 s and the alarm panel reports the failure. "DC Fault" outputs are activated.• If the value is set to higher than 0 min, this timer is started 10 s after the disruption occurs. <p>If the power supply is restored before the end of the set delay time, "General Fault" outputs are reset and a log book entry is created about the power restore.</p> <p>No errors are reported.</p> <p>If the fault still exists after the end of the configured time, a warning tone sounds and the error is reported. "DC Fault" outputs are activated.</p> <p>A user can stop the warning tone by entering their code. The alarm panel display shows details of the warning. "General Fault" and "DC Fault" outputs remain activated.</p> <p>If the fault has been corrected, the alarm panel deactivates the "DC Fault" outputs and creates a log book entry about the power restore. A user can reset the alarm and the "General Fault" outputs after entering their user code.</p>

Installer details



Name/function	Explanation
Installer Name	User name, number or character sequence used by the installer to log into the alarm system using a web browser. This entry is case-sensitive. Max. 12 characters
Installer Code	Password for the installer on the web server, access code on the alarm panel. Factory Defaults <ul style="list-style-type: none"> • 9999 (4 digit user code) • 999999 (6 digit user code) It is a good idea to change this code. The installer code can be used to access installer mode and perform an installer reset. The installer code cannot be used to arm or disarm the alarm panel.
Confirm New Code	Password confirmation for the installer when entering a new code
Installer Tel No	The telephone number of the installer can be stored here for user reference in the event of a fault.

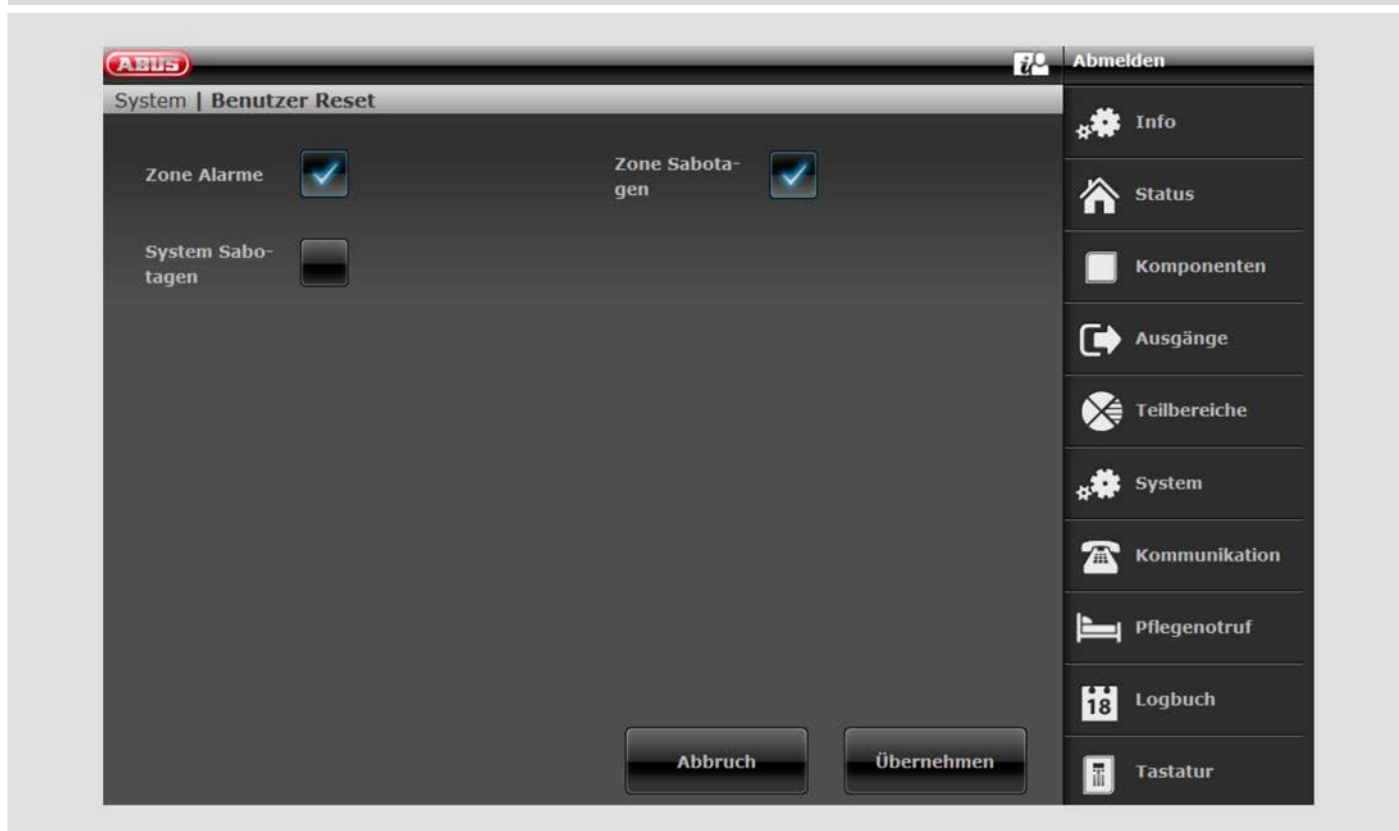
User access

Name/function	Explanation (checkbox)
Record Memo	Activated Allows the user to record a memo message. Menu -> Voice Memo Deactivated Function not possible.
Dual Key Function	Activated Manual triggering of alarms is possible by simultaneously pressing the corresponding dual keys (fire alarm, hold up alarm, medical alarm) on the alarm system or control device. Deactivated Function not possible.
Social Care Key	Activated Manual triggering of a social care alarm is possible by simultaneously pressing the corresponding dual keys on the alarm system or control device. Deactivated Function not possible.
Omit All	Activated All open zones can be omitted manually together when the alarm panel is armed. Deactivated Open zones must be individually omitted manually when the alarm panel is armed.

Name/function	Explanation (checkbox)
Quick Set	<p>Activated Alarm system can be armed using the symbol keys without entering the user code first.</p> <p>Deactivated Alarm system can only be armed after the user code has been entered.</p>
Quick Omit	<p>Activated Open zones are automatically omitted when the alarm system is armed (if the zone attributes for omission allow).</p> <p>Deactivated Open zones must be manually omitted when the alarm system is armed.</p>
User Code Req'd	<p>Use this option to ensure that an installer only has access to the system when a user is present.</p> <p>Activated After the installer has entered their code, the system prompts the user to enter their user code. Only once a user code has also been entered does the installer gain access to the system.</p> <p>Deactivated The installer can access installer mode after entering their code; no additional user code is required.</p> <p>Note This setting is not compliant with EN 50131. This setting only complies with BS8243 when the user has provided written consent.</p>
2 Way Replies	<p>Activated There is active status feedback from the wireless alarm system to the wireless remote control, wireless control device, Secvest key and additional door lock.</p> <p>Deactivated 2 Way Replies are deactivated.</p>

Name/function	Explanation (checkbox)
Remote Inst. Set	<p>Use this option to decide whether the alarm panel is armed or internally armed after the remote control is operated.</p> <p>Activated The possible partitions are armed or internally armed immediately. If an exit delay is configured, this is overridden and the alarm system is armed immediately as soon as the "arm" button on the remote control is pressed.</p> <p>Deactivated The possible partitions are armed or internally armed according to the set exit mode.</p>
Duress Enable	<p>Activated The administrator has the option of creating a "Duress Code User". The system can be armed or disarmed using a duress code.</p> <p>Important If a user is forced by an intruder to disarm the alarm system, they should disarm the system using a duress code. The alarm panel then responds as follows:</p> <ul style="list-style-type: none">• The configured communication for duress is started.• No sounders are activated.• The alarm panel siren is not activated, and no triangle warning appears on the display. <p>The alarm panel can also be rearmed or internally armed again using the HUA code. This is useful if the intruder forces you to rearm the alarm panel. In this case the intruder is checking whether the code you entered is a "normal" code. "Duress" outputs are activated. Corresponding log book entries are generated.</p> <p>Deactivated There is no option to create a "Duress Code User".</p>

User reset



Name/function	Explanation (checkbox)
	These menus determine the circumstances under which a user or installer can reset the system after an alarm or after tampering.
Zone Alarms	Activated Allows the user to reset this alarm triggered for zones or detectors. Deactivated User cannot perform a reset. The installer must reset the system after an alarm.
Zone Tamperers	Activated Allows the user to reset tamper alarms triggered for zones or detectors. Deactivated User cannot perform a reset. The installer must reset the system. This setting is required for INCERT certification.

Configuration

Name/function	Explanation (checkbox)
System Tamper	<p>Activated</p> <p>Allows the user to reset tamper alarms that affect the system.</p> <p>Deactivated</p> <p>User cannot perform a reset. The installer must reset the system. This setting is required for INCERT certification.</p> <p>System tampers can be caused by:</p> <ul style="list-style-type: none">• Housing and wall tamper switches on the alarm panel• Housing and wall tamper switches on control devices• Tampering with connected wired sirens when the voltage at terminal TR is higher than approx. 3 V• Jamming or supervision when set to "Tamper"

Confirmation

Name/function	Explanation (checkbox)
Confirmation Mode	Dropdown selection field for: <ul style="list-style-type: none"> • Basic • DD243 • BS8243
Sounder On	Dropdown selection field for: <ul style="list-style-type: none"> • Unconfirm • Confirm <p>Note "Confirm" can only be selected if "Siren On" is configured to "Unconfirm".</p>
Siren On	Dropdown selection field for: <ul style="list-style-type: none"> • Unconfirm • Confirm <p>Note "Confirm" can only be selected if "Sounder On" is configured to "Unconfirm".</p>
Confirmation Time (Confirmation Mode DD243 and BS8243 only)	Input field for the confirmation time for burglar alarms in minutes. The confirmation time can be set to between 1 and 60 minutes. <p>Note Confirmation times < 30 minutes do not meet the requirements set out in DD243 and BS8243.</p>

Configuration

Name/function	Explanation (checkbox)
Entry Keypad Lock (Confirmation Mode DD243 and BS8243 only)	Activated The user must disarm the system using an alternative device (not control device or alarm system), e.g. a remote control or key switch (relevant for DD243 and BS8243). Deactivated The user can disarm the system by entering their access code on the keypad (on control device or alarm system) after the entrance door has been opened (relevant for DD234).
Unconfirmed Reset (Confirmation Mode DD243 and BS8243 only)	Dropdown selection field for: <ul style="list-style-type: none">• Installer• User
After Entry (Confirmation Mode DD243 and BS8243 only)	Dropdown selection field for: <ul style="list-style-type: none">• Never• 2 zones (DD243 only)• 1 zone
Confirmed Reset (Confirmation Mode DD243 and BS8243 only)	Dropdown selection field for: <ul style="list-style-type: none">• Installer• User
HUA Confirm Time (Confirmation Mode BS8243 only)	Input field for the confirmation time for hold up alarms in hours. Note As per BS8243 confirmation time must be set to between 8 and 20 hours.
Tamp as Tamp-Only (Confirmation Mode BS8243 only)	Activated Deactivated

Hardware

ABUS System | Hardware

Zonentyp (Zentrale) **Nicht ändern** ▼

Funksirenen Optionen ***Sirene+Blitz** ▼

Akku 2 ☐

Abbruch Übernehmen

Abmelden


- Info
- Status
- Komponenten
- Ausgänge
- Teilbereiche
- System
- Kommunikation
- Pflegenotruf
- Logbuch
- Tastatur

Name/function	Explanation (checkbox)
Zone type (alarm panel)	<p>Dropdown selection field for:</p> <p>Use of inputs for wired zones</p> <ul style="list-style-type: none"> • Don't change • 2-wire FSL 2K2/4K7 • 2-wire FSL 1K/1K • 2-wire FSL 2K/2K • 2-wire FSL 4K7/4K7 • 4-wire CC • 2-wire CC
RF Siren Options	<p>Dropdown selection field for:</p> <p>Siren configuration. Select here how the wireless siren responds to fire alarms, burglar alarms and hold up alarms.</p> <ul style="list-style-type: none"> • Siren+Strobe The wireless siren operates the siren and strobe when an alarm is triggered. • Strobe The wireless siren operates only the strobe when an alarm is triggered.
Battery 2	<p>When a second battery is connected, this option enables or disables warning messages for the second backup battery.</p> <p>Activated The alarm panel displays warning messages when battery 2 is missing or has low voltage.</p> <p>Deactivated The alarm panel ignores the presence or absence of the second additional battery.</p>

Configuration

Name/function	Explanation (checkbox)
SD Card	<p>Only available on the alarm panel.</p> <p>Safely Remove Hardware</p> <ul style="list-style-type: none">• Any ongoing read or write operations are stopped properly.• The SD card can then be safely removed. <p>Enable Hardware</p> <ul style="list-style-type: none">• After insertion, the SD card is brought into operation again.• Read and write operations can run again.
GSM antenna	<p>The menu only appears when a GSM module is installed.</p> <p>Internal</p> <ul style="list-style-type: none">• The antenna located directly on the GSM module is used. <p>External</p> <ul style="list-style-type: none">• The antenna connected to the antenna connection of the GSM module is used.

Security settings

Name/function	Explanation (checkbox)
6 Digit User Codes	<p>Activated 6-digit numerical code for installer and user</p> <p>Deactivated 4-digit numerical code for installer and user</p> <p> Note</p> <ul style="list-style-type: none"> Switching from 4 to 6 digits When switching from 4 to 6-digit numerical codes, "00" is automatically added to the end of the existing 4-digit codes. Example: "1234" becomes "123400". Switching from 6 to 4 digits When switching from 6 to 4-digit numerical codes, all codes are reset to their defaults ("1234" or "9999"). When the numerical codes are reset (from 6 to 4 digits), all users and installers are reset to their factory defaults (remote controls, chip keys, etc. are deleted).

Name/function	Explanation (checkbox)												
Supervision	Dropdown selection field for alarm system response for supervision If a wireless detector has had no contact with the alarm panel for more than 20 min, the alarm panel creates a log entry: "RF warning". The alarm panel also prevents the system from being armed. If a user overrides this warning and arms the alarm panel, the log entry "RF warning overridden" is generated.												
	If a wireless detector has had no contact with the alarm panel for more than 2 h, corresponding processes are activated as follows:												
	<table><tr><th></th><th>Alarm panel is armed</th><th>Alarm panel is disarmed</th></tr><tr><td>Disabled</td><td>No response</td><td>No response</td></tr><tr><td>Fault</td><td><ul style="list-style-type: none">Log book entry of this eventNo display and no warning tones"RF Supervision" or "RF Fault" outputs are activated</td><td><ul style="list-style-type: none">Log book entry of this eventDisplay and warning tones"RF Supervision" or "RF Fault" outputs are activated</td></tr><tr><td>Tamper</td><td><ul style="list-style-type: none">Tamper alarmSupervision is reported<p>Note: If "Tamp as Tamp-Only" is disabled, the "Supervision" or "Fault" outputs are also activated. If no tamper channel is assigned in FF, an "unconfirmed alarm" is sent.</p></td><td><ul style="list-style-type: none">Tamper alarmSupervision is reported<p>Note If "Tamp as Tamp-Only" is disabled, the "Supervision" or "Fault" outputs are also activated. If no tamper channel is assigned in FF, an "unconfirmed alarm" is sent.</p></td></tr></table>		Alarm panel is armed	Alarm panel is disarmed	Disabled	No response	No response	Fault	<ul style="list-style-type: none">Log book entry of this eventNo display and no warning tones"RF Supervision" or "RF Fault" outputs are activated	<ul style="list-style-type: none">Log book entry of this eventDisplay and warning tones"RF Supervision" or "RF Fault" outputs are activated	Tamper	<ul style="list-style-type: none">Tamper alarmSupervision is reported <p>Note: If "Tamp as Tamp-Only" is disabled, the "Supervision" or "Fault" outputs are also activated. If no tamper channel is assigned in FF, an "unconfirmed alarm" is sent.</p>	<ul style="list-style-type: none">Tamper alarmSupervision is reported <p>Note If "Tamp as Tamp-Only" is disabled, the "Supervision" or "Fault" outputs are also activated. If no tamper channel is assigned in FF, an "unconfirmed alarm" is sent.</p>
		Alarm panel is armed	Alarm panel is disarmed										
	Disabled	No response	No response										
Fault	<ul style="list-style-type: none">Log book entry of this eventNo display and no warning tones"RF Supervision" or "RF Fault" outputs are activated	<ul style="list-style-type: none">Log book entry of this eventDisplay and warning tones"RF Supervision" or "RF Fault" outputs are activated											
Tamper	<ul style="list-style-type: none">Tamper alarmSupervision is reported <p>Note: If "Tamp as Tamp-Only" is disabled, the "Supervision" or "Fault" outputs are also activated. If no tamper channel is assigned in FF, an "unconfirmed alarm" is sent.</p>	<ul style="list-style-type: none">Tamper alarmSupervision is reported <p>Note If "Tamp as Tamp-Only" is disabled, the "Supervision" or "Fault" outputs are also activated. If no tamper channel is assigned in FF, an "unconfirmed alarm" is sent.</p>											
Note The "Tamper" option is required in Grade 2 systems in order to comply with EN 50131-1:2006+A1:2009.													
If the "Tamper" option is used along with the following setting: System -> User Reset -> System Tamper = No the user cannot reset the system.													

Name/function	Explanation (checkbox)		
RF Jamming	Dropdown selection field for alarm system response for jamming:		
	The alarm panel can detect jamming of wireless signals.		
	Corresponding processes are activated as follows:		
		Alarm panel is armed	Alarm panel is disarmed
	Disabled	No response	No response
	Fault	<ul style="list-style-type: none">Log book entry of this eventNo display and no warning tones	<ul style="list-style-type: none">Log book entry of this eventDisplay and warning tones
	Tamper	<ul style="list-style-type: none">Tamper alarmJamming is reported <p>Note: If "Tamp as Tamp-Only" is disabled, the "Jamming" or "Fault" outputs are also activated. If no tamper channel is assigned in FF, an "unconfirmed alarm" is sent.</p>	<ul style="list-style-type: none">Tamper alarmJamming is reported <p>Note If "Tamp as Tamp-Only" is disabled, the "Jamming" or "Fault" outputs are also activated. If no tamper channel is assigned in FF, an "unconfirmed alarm" is sent.</p>
	<p>Note The "Tamper" option is required in order to comply with PD 6662:2010. If the "Tamper" option is used along with the following setting: System -> User Reset -> System Tamper = No the user cannot reset the system.</p>		
Tamper Omit	<p>If a user omits a zone it may be necessary to also omit the associated tamper circuit for this zone.</p> <p>Activated The tamper contact is also omitted within an omitted zone.</p> <p>Deactivated The tamper contact continues to be monitored within an omitted zone.</p>		

Name/function	Explanation (checkbox)
Force Set	<p>A user can be permitted to arm the alarm panel using the remote control even if one or more zones are not working or are open.</p> <p>Note If Force Set is enabled, the system is no longer compliant with EN 50131.</p> <p>Dropdown selection field for:</p> <ul style="list-style-type: none">• Off<ul style="list-style-type: none">• The user cannot force the system to arm with the remote control even if the corresponding zones have been given attribute "Force Set". Confirm• The user can force the system to arm with the remote control. To do so, proceed as follows:<ol style="list-style-type: none">1. The user presses the "arm" button on the remote control.2. The system does not start arming.3. The user presses the same button on the remote control again to confirm that the system should arm.• On<ul style="list-style-type: none">• The user only has to press the corresponding button on the remote control once to start the arming process. <p>Note With the "Confirm" and "On" options, the user is also permitted to arm the system with the remote control even if it would need to be reset after an alarm.</p>
Remote Unset Full Set	<p>Select whether armed partitions can only be disarmed using the remote control when the delay time has been started beforehand ("Final Door" zone is triggered).</p> <p>Dropdown selection field for:</p> <ul style="list-style-type: none">• Always<ul style="list-style-type: none">• The user can always disarm the possible partitions without the entry time being started first.• During entry time<ul style="list-style-type: none">• The user must first open a "Final Door" zone. This starts the entry delay. The user can now disarm the possible partitions.• Partitions for which no entry delay has started remain armed.

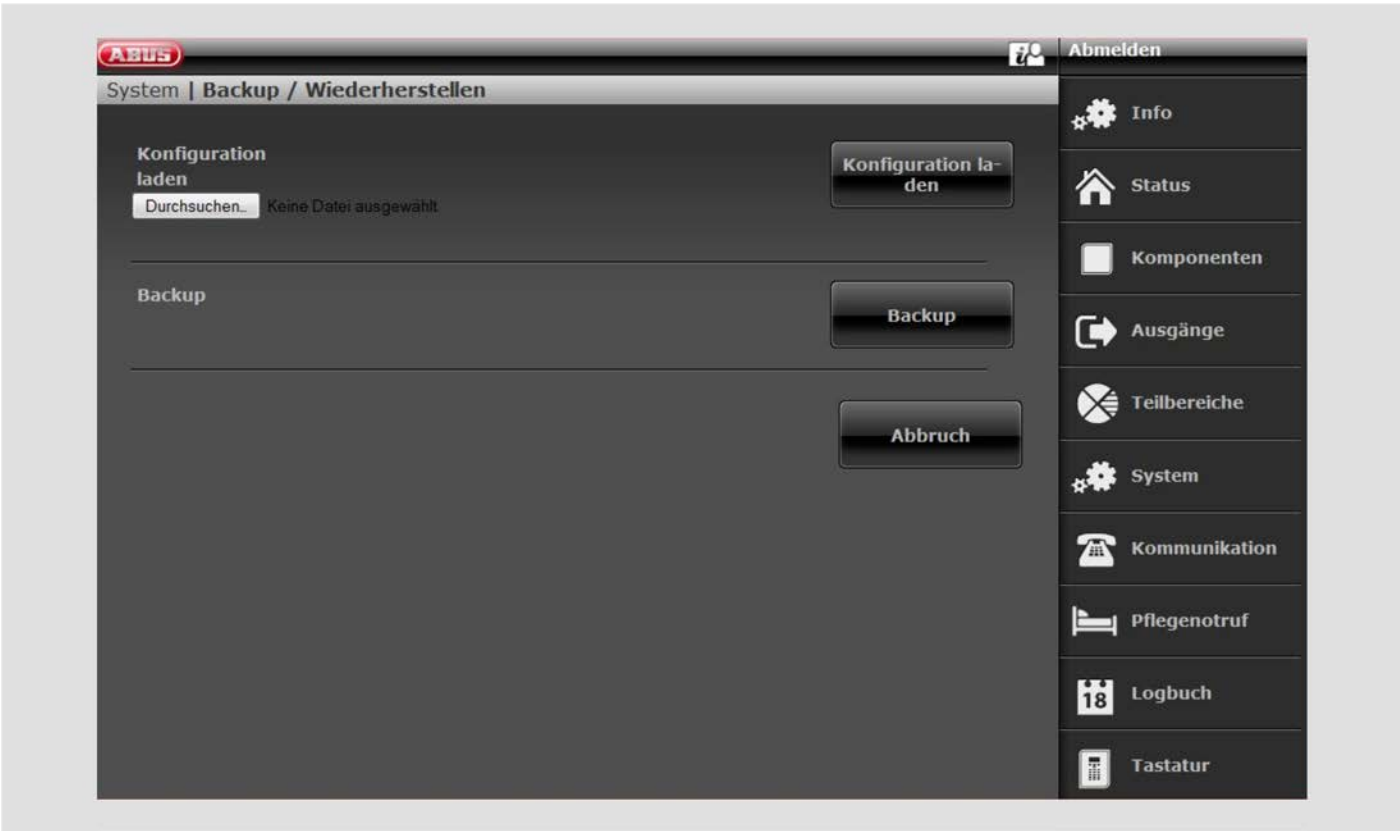
Name/function	Explanation (checkbox)
Remote Unset Part Set	<p>Select whether internally armed partitions can only be disarmed using the remote control when the delay time has been started beforehand ("Final Door" zone is triggered).</p> <p>Dropdown selection field for:</p> <ul style="list-style-type: none"> • Always <ul style="list-style-type: none"> • The user can always disarm the possible partitions without the entry time being started first. • During entry time <ul style="list-style-type: none"> • The user must first open a "Final Door" zone. This starts the entry delay. The user can now disarm the possible partitions. • Partitions for which no entry delay has started remain armed.
Ctrl Device Unset Full Set	<p>Select whether armed partitions can only be disarmed using the wireless control device when the delay time has been started beforehand ("Final Door" zone is triggered).</p> <p>Dropdown selection field for:</p> <ul style="list-style-type: none"> • Always <ul style="list-style-type: none"> • The user can always disarm the possible partitions without the entry time being started first. • During entry time <ul style="list-style-type: none"> • The user must first open a "Final Door" zone. This starts the entry delay. The user can now disarm the possible partitions. • Partitions for which no entry delay has started remain armed.
Ctrl Device Unset Part Set	<p>Select whether internally armed partitions can only be disarmed using the wireless control device when the delay time has been started beforehand ("Final Door" zone is triggered).</p> <p>Dropdown selection field for:</p> <ul style="list-style-type: none"> • Always <ul style="list-style-type: none"> • The user can always disarm the possible partitions without the entry time being started first. • During entry time <ul style="list-style-type: none"> • The user must first open a "Final Door" zone. This starts the entry delay. The user can now disarm the possible partitions. • Partitions for which no entry delay has started remain armed.

Configuration

Name/function	Explanation (checkbox)
Auto Rearm	<p>Appears when the following is set: System->Confirmation->Confirmation Mode->Basic</p> <p>Select how often the system automatically rearms after the siren time has expired.</p> <p>Dropdown selection field for:</p> <ul style="list-style-type: none">• Never<ul style="list-style-type: none">• The alarm panel never rearms. The alarm panel switches to the alarm status just one time.• 1 x, 2 x, 3 x, 4 x, 5 x• Always<ul style="list-style-type: none">• The system rearms all closed zones but not the detectors still sending alarm signals.• One of these settings is required in order to comply with EN 50131.• If the system is rearmed, an acoustic internal alarm instead of the normal entry tone is generated by the wireless alarm panel if a user enters through the entry route.
Silence Alerts (silent warnings)	<p>This option controls the length of time in which warning tones (a brief "beep" every few minutes) are sounded.</p> <p>Dropdown selection field for:</p> <ul style="list-style-type: none">• User Code<ul style="list-style-type: none">• Warnings are sounded until a user enters their code to confirm the warning.• 30 minutes• 60 minutes• 120 minutes<ul style="list-style-type: none">• Warnings are sounded for the set amount of time. The warning tones can be stopped by entering a user code.• No alert tones<ul style="list-style-type: none">• No acoustic alerts are sounded. <p>Note The alarm panel does not display any warnings as long as a partition is still armed.</p>
Abort time	<p>Input field for the alarm abort time in seconds (value between 0 and 120).</p> <p>The alarm panel always starts this time when an alarm has been triggered. If a user mutes the alarm during this time, no installer reset is required.</p> <p>If an alarm occurs and a user disarms the system within this time, "Alarm Abort" outputs are activated and an alarm abort is reported.</p>

Name/function	Explanation (checkbox)
Entry Alarm Delay	<p data-bbox="528 192 1150 221">Additional delay when deviating from the entry route.</p> <p data-bbox="528 264 1422 327">Select whether the user is permitted an additional time of 30 seconds when deviating from the entry route, before an external alarm is started.</p> <p data-bbox="528 369 647 398">Activated</p> <p data-bbox="528 405 1342 434">Additional delay (30 s) activated when deviating from the entry route.</p> <p data-bbox="528 477 1493 575">If a user deviates from the entry route within the entry delay time, the alarm panel waits 30 s before triggering a full alarm. Only an internal alarm is triggered first within these 30 s.</p> <p data-bbox="528 582 1414 611">If a user enters their code within these 30 s, the user can reset the system.</p> <p data-bbox="528 618 1002 647">This setting is compliant with EN 50131.</p> <p data-bbox="528 689 679 719">Deactivated</p> <p data-bbox="528 725 1190 754">No additional delay when deviating from the entry route.</p> <p data-bbox="528 761 1457 824">An alarm is immediately triggered if a user deviates from the entry route and is caught by another detector in the process.</p> <p data-bbox="528 831 1046 860">This setting is not compliant with EN 50131.</p>
Broadcast Panel Status	<p data-bbox="528 880 647 909">Activated</p> <p data-bbox="528 916 1481 1014">A status change to the alarm system is always transmitted to the wireless control device. The control device signals the status of the partitions, alarms and entry and exit delays "just in time".</p> <p data-bbox="528 1057 679 1086">Deactivated</p> <p data-bbox="528 1093 1517 1191">The status of the alarm panel is only transmitted to the control device when queried ("?" button on the control device). The status of the partitions, alarms and entry and exit delays are not displayed or signalled on the control device.</p>

Backup/restore



Name/function	Explanation (checkbox)
Load Configuration	<p>Click the Browse button to specify the path and file name of the configuration to be restored.</p> <p>Click the Load Configuration button to import the configuration to be restored into the wireless alarm system.</p> <p>The wireless alarm system must then be restarted.</p>
Backup	<p>Click the Backup button to create a backup of the entire system configuration (including detector IDs). The backup file (config.config) is saved in the default Downloads folder.</p>

Panel upgrade

Name/function	Explanation (checkbox)
Language File	<p>Click the Browse button to specify the path and file name of the language file to be loaded.</p> <p>Click the Submit button to import the selected file into the wireless alarm system.</p>
Application File	<p>Click the Browse button to specify the path and file name of the application file to be loaded.</p> <p>Click the Submit button to import the selected file into the wireless alarm system.</p> <p>The wireless alarm system must then be restarted.</p>

Communications

Network

ABUS Abmelden

Kommunikation | **Netzwerk**

IP Port Nummer: IP Adresse:

ABUS Server freigegeben: ☒ ABUS Server Benutzername:

Externer Port: ABUS Server Passwort:

Menu: Info, Status, Komponenten, Ausgänge, Teilbereiche, System, Kommunikation, Pflegenotruf, Logbuch, Tastatur

Name/function	Explanation (checkbox)
IP Port Number	IP port number
IP Address	IP address
IP Subnet Mask	IP subnet mask
Gateway IP Address	Gateway IP address
DNS Primary IP Address	DNS primary IP address
ABUS Server Enabled	Activated Establishes a connection to the ABUS server. An account for Secvest must be created. Deactivated Function not possible.
External Port	Port number of the external port.
ABUS Server User Name	User name on the ABUS server.
ABUS Server Password	Password on the ABUS server.

Email setup

The screenshot shows the 'E-Mail Setup' configuration window for an ABUS device. The window is titled 'Kommunikation | Netzwerk | E-Mail Setup'. It features a sidebar on the right with various system functions like 'Info', 'Status', 'Komponenten', 'Ausgänge', 'Teilbereiche', 'System', 'Kommunikation', 'Pflegenotruf', 'Logbuch', and 'Tastatur'. The main configuration area includes fields for 'Server Name' (smtp.web.de), 'IP Port Nummer' (587), 'Konto' (abusmailex@web.d), 'Benutzername' (abusmailex@web.d), 'Passwort' (Ab1924bA), and an 'SSL' checkbox. At the bottom, there are 'Abbruch' (Cancel) and 'Übernehmen' (Apply) buttons.

Name/function	Explanation (checkbox)
Server Name	SMTP server name of the email service provider.
IP Port Number	IP port number
Account	Name of the email account (usually the email address)
User name	User name (depending on the provider, either the entire email address or a separate user name)
Password	Password for the email account
	Note This entry is case-sensitive.
SSL	Activated An encrypted connection (SSL) to the provider is established. Deactivated An unencrypted connection (SSL) to the provider is established.

The appendix contains some recommended and tested settings.

The FAQs of the email provider in question will also have additional information about the parameters used.

VoIP dialler setup

The screenshot displays the 'VoIP Wähler Setup' configuration window. It includes input fields for 'SIP Server Name', 'SIP Benutzer Passwort', 'RTP Port' (set to 4000), 'SIP Ben. ID', 'SIP Port' (set to 5060), and 'SIP Test Ruf Ziel Benutzer ID'. There are also checkboxes for 'SIP Wähler freigeben' and 'RFC 2833 DTMF Detektion', both of which are currently checked. A sidebar on the right provides navigation options: 'Abmelden', 'Info', 'Status', 'Komponenten', 'Ausgänge', 'Teilbereiche', 'System', 'Kommunikation', 'Pflegenotruf', 'Logbuch', and 'Tastatur'. At the bottom of the main window are 'Abbruch' and 'Übernehmen' buttons.

Name/function	Explanation (checkbox)
SIP Server Name	SIP server name of the SIP service provider
SIP User ID	User ID of the SIP service provider
SIP User Password	SIP user password of the SIP service provider
SIP Port	Port of the SIP service provider
RTP Port	RTP port number
SIP Test Call Dest. User ID	User ID for a test call via SIP
SIP Dialler Enable	Activated The SIP dialler is enabled. Deactivated
RFC 2833 DTMF Detection	Activated DTMF tones are also detected for SIP under certain requirements. Deactivated No detection of DTMF tones.

ARC reporting

Name/function	Explanation (checkbox)
Call Mode	Dropdown selection field for: <ul style="list-style-type: none"> • Disabled • Single • Alternate
Protocol	Dropdown selection field for: <ul style="list-style-type: none"> • Fast Format • Contact ID • SIA 1 • SIA 2 • SC SIA 3 • Ex SIA 3 • Ex SIA 3 v2 • Contact ID in SMS

Abmelden

Kommunikation | NSL Reporting

Anrufmodus

*Gesperrt ▼

Protokoll

*Fast Format ▼

Telefonbuch

Kunden ID

FF Kanäle

Mehr...

Tel. Empfänger 1

Keine

Tel. Empfänger 2

Keine

IP Empfänger 1

Keine

IP Empfänger 2

Keine

Abbruch

Übernehmen

Info

Status

Komponenten

Ausgänge

Teilbereiche

System

Kommunikation

Pflegenotruf

18 Logbuch

Tastatur

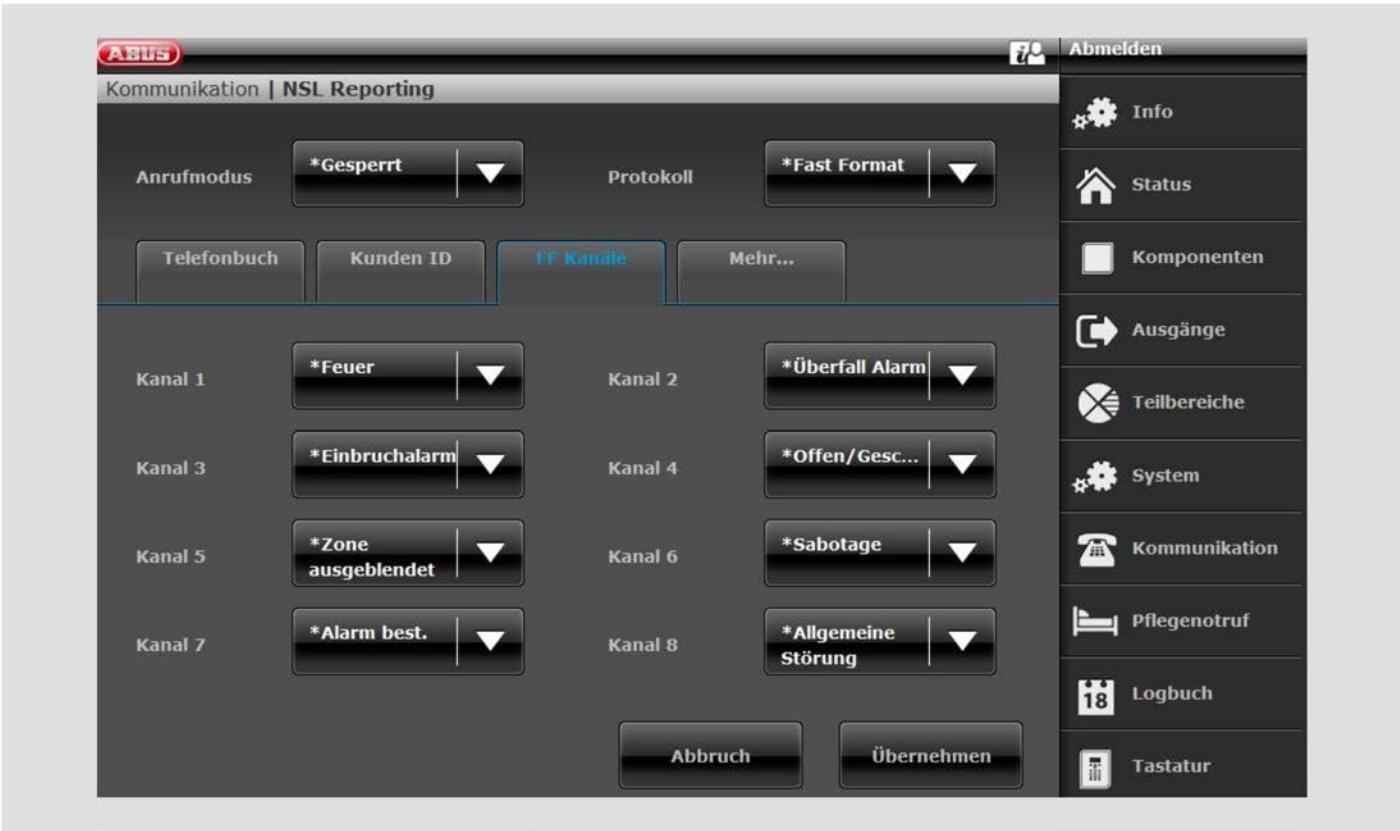
Name/function	Explanation (checkbox)
Tel Recipient #	Name of the recipient

ARC Reporting, Account Numbers

The screenshot displays the 'Kommunikation | NSL Reporting' configuration window. At the top, the 'Anrufmodus' is set to '*Gesperrt' and the 'Protokoll' is set to '*Fast Format'. Below these are four buttons: 'Telefonbuch', 'Kunden ID' (which is highlighted in blue), 'FF Kanäle', and 'Mehr...'. The main configuration area contains four input fields labeled 'Kunden-ID TB 1' through 'Kunden-ID TB 4', each containing the text '000000'. At the bottom of the main area are two buttons: 'Abbruch' and 'Übernehmen'. On the right side, there is a vertical sidebar with a list of menu items, each with an icon: 'Abmelden' (logout), 'Info' (gear), 'Status' (house), 'Komponenten' (square), 'Ausgänge' (arrow), 'Teilbereiche' (pie chart), 'System' (gear), 'Kommunikation' (phone), 'Pflegenotruf' (bed), 'Logbuch' (calendar), and 'Tastatur' (keyboard).

Name/function	Explanation (checkbox)
Account No P#	<p>Input field for a customer ID (account number up to 6 digits) for the partition in question.</p> <p>CID uses 4-digit account numbers.</p> <p>With Fast Format you can use four, five or six-digit account numbers.</p> <p>The alarm panel adds a leading zero to turn five-digit account numbers into six-digit codes.</p> <p>The alarm panel does not alter four or six-digit account numbers.</p>

ARC Reporting, Fast Fmt Channels (for "Fast Format" protocol only)



Name/function	Explanation (checkbox)	
Channel 1 to 8	Dropdown selection field for:	
	<ul style="list-style-type: none">• Not Used• Burglar Alarm• Burg Confirm Alarm• Burglar Alarm P1• Burglar Alarm P2• Burglar Alarm P3• Burglar Alarm P4• HU Alarm• HUA Confirm• Duress Code• Confirmed Alarm• Fire Alarm• Technical Alarm• Alarm Abort	<ul style="list-style-type: none">• Medical Alarm• Key Box• Tamper• RF Supervision• RF Jamming• RF Low Battery• Mains Fault• General Fault• Open/Close• Open• Close• Zone Omit (Setting)• Zone Omit (System)
Factory Defaults	Channel 1	Fire Alarm
	Channel 2	HU Alarm
	Channel 3	Burglar Alarm
	Channel 4	Open/Close
	Channel 5	Zone Omit (Setting)
	Channel 6	Tamper
	Channel 7	Confirmed Alarm
	Channel 8	General Fault

ARC Reporting, CID/SIA Events (for all protocols EXCEPT "Fast Format")

ABUS Abmelden

Kommunikation | NSL Reporting

Anrufmodus: *Gesperrt Protokoll: Contact ID

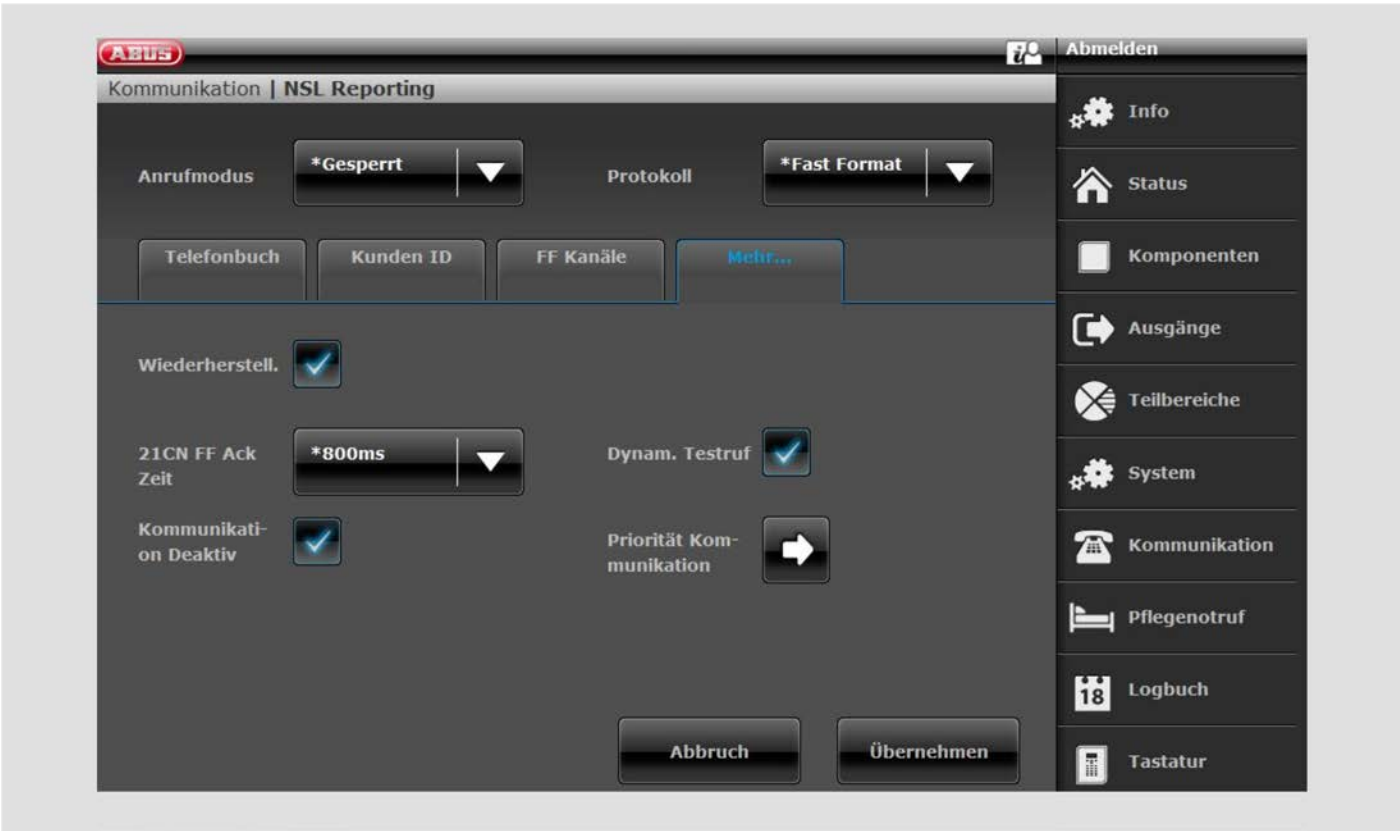
Telefonbuch Kunden ID **CID/SIA Ereignisse** Mehr...

Feuer	<input checked="" type="checkbox"/>	Überfall Alarm	<input checked="" type="checkbox"/>
Medizin. Alarm	<input checked="" type="checkbox"/>	Einbruchalarm	<input checked="" type="checkbox"/>
Technik	<input type="checkbox"/>	Sabotagen	<input checked="" type="checkbox"/>
Aktiv./Deaktiv.	<input checked="" type="checkbox"/>	Intern Aktiv	<input checked="" type="checkbox"/>

Abbruch Übernehmen

Name/function	Explanation (checkbox)
Fire Alarm	Activated
Medical Alarm	The selected event is transmitted to the ARC.
Technical Alarm	Deactivated
Set/Unset	The selected event is not transmitted to the ARC.
Reset	
Omit	
RF Supervision	
RF Battery/PSU	
Mains Fault	
Installer Mode	
Time/Date Reset	
HU Alarm	
Burglar Alarm	
Tampers	
Part Set	
Exit Timeout	
Key Box	
RF Jamming	
Panel Battery	
Faults	
User Code Chnge	

ARC Reporting, More



Name/function	Explanation (checkbox)
Restorals	<p>If an event occurs that should be reported to the ARC, two bits of information are transmitted to the ARC:</p> <ul style="list-style-type: none">• Type and time of the event taking place• Event reset <p>The event reset is called a "restoral".</p> <p>Activated</p> <p>The information about the event reset (restoral) is transmitted to the ARC.</p> <p>Deactivated</p> <p>The information about the event reset (restoral) is not transmitted to the ARC.</p>

Name/function	Explanation (checkbox)
21CN Ack Time	<p>An analogue telephone connection to the ARC, directed via the new public telephone networks, sometimes takes more time than a conventional analogue connection to transmit the information including confirmation with the Fast Format protocol.</p> <p>Use this option to set the wait time for the confirmation.</p> <p>Dropdown selection field for:</p> <ul style="list-style-type: none"> • 400 ms • 500 ms • 600 ms • 700 ms • 800 ms • 900 ms • 1000 ms • 1100 ms • 1200 ms
Unset Comms	<p>Activated</p> <p>The alarm system transmits all status messages to the ARC, regardless of whether the system is armed or disarmed.</p> <p>Deactivated</p> <p>The alarm system transmits tamper, network failure and other status messages to the ARC while it is armed. When disarmed, the status messages are not transmitted to the ARC.</p>
Burg Comms Rearm	<p>Appears only when the following is set: "System → Confirmation → Confirmation Mode = Basic" and "Communications → Protocol = Fast Format"</p> <p>Activated</p> <ul style="list-style-type: none"> • The alarm system activates channel 3 again as soon as the siren time has expired. After channel 3 has been reactivated, an event can be transmitted again if it occurs. The system automatically omits triggered zones in this case. • Note: if a "Final Door" zone is triggered, channel 3 is activated at the end of the configured entry/exit time. <p>Deactivated</p> <p>Channel 3 remains activated until a user or installer resets the system.</p>
Dynamic Test Call	<p>Activated</p> <p>The dynamic test call is activated.</p> <p>Deactivated</p> <p>The dynamic test call is deactivated. The "Static Test Call" dropdown selection field appears.</p>
Telecoms Priority	<p>Set the order in which the communication methods should be used here.</p> <ul style="list-style-type: none"> • Ethernet 1, 2, 3 or No • PSTN 1, 2, 3 or No • GSM 1, 2, 3 or No

Configuration

Name/function	Explanation (checkbox)
Static Test Call Only when "Dynamic Test Call" is deactivated	Dropdown selection field for: <ul style="list-style-type: none">• Disabled• Daily• Weekly• Monthly
SET THE HOUR For "Static Test Call" only <ul style="list-style-type: none">• Daily• Weekly• Monthly	Input field for the time of the daily test call (hh:mm)
SET THE DAY For "Static Test Call" only <ul style="list-style-type: none">• Weekly	Dropdown selection field for: <ul style="list-style-type: none">• Sunday• Monday• Tuesday• Wednesday• Thursday• Friday• Saturday
SET THE DAY For "Static Test Call" only <ul style="list-style-type: none">• Monthly	Input field for the day of the month on which the test call should be carried out (1–31)

Social Care

The screenshot shows a software interface for 'Social Care' configuration. At the top, there's a header bar with 'ABUS' on the left and 'Abmelden' on the right. Below this is a sub-header 'Kommunikation | Pflegenotruf'. The main area contains several settings: 'Anrufmodus' set to '*Gesperrt', 'Protokoll' set to '*Scancom', 'Priorität Kommunikation' with a right arrow icon, 'Ruf Quittierung' with a checked checkbox, and '21CN FF Ack Zeit' set to '*800ms'. Below these are two tabs: 'Telefonbuch' (active) and 'Kunden ID'. Under 'Telefonbuch', there are two input fields for 'Tel. Empfänger 1' and 'Tel. Empfänger 2', both containing the text 'Keine'. At the bottom right of the main area are two buttons: 'Abbruch' and 'Übernehmen'. On the right side of the interface is a vertical sidebar with icons and labels: 'Info', 'Status', 'Komponenten', 'Ausgänge', 'Teilbereiche', 'System', 'Kommunikation', 'Pflegenotruf', 'Logbuch', and 'Tastatur'.

Name/function	Explanation (checkbox)
Call Mode	Dropdown selection field for: <ul style="list-style-type: none"> • Disabled • Single • Alternate
Protocol	Dropdown selection field for: <ul style="list-style-type: none"> • Scancom • Scanfast • Tunstall
Telecoms Priority	Set the order in which the communication methods should be used here. <ul style="list-style-type: none"> • PSTN 1, 2 or No • GSM 1, 2 or No
21CN Ack Time	An analogue telephone connection to the ARC, directed via the new public telephone networks, sometimes takes more time than a conventional analogue connection to transmit the information including confirmation with the Fast Format protocol. Use this option to set the wait time for the confirmation. Dropdown selection field for: <ul style="list-style-type: none"> • 400 ms • 500 ms • 600 ms • 700 ms • 800 ms • 900 ms • 1000 ms • 1100 ms • 1200 ms

Configuration

Name/function	Explanation (checkbox)
Call Acknowledge	<p>Activated</p> <p>A social care alarm transmission must be confirmed by the recipient by pressing DTMF button"5", otherwise the calls will be repeated.</p> <p>Deactivated</p> <p>If the function is deactivated, the emergency call is treated like a transmission when the called line is answered.</p>

Social Care, Phone Book

ABUS Abmelden

Kommunikation | **Pflegenotruf**

Anrufmodus: *Gesperrt ▼

Protokoll: *Scancom ▼

Priorität Kommunikation:

Ruf Quittierung: ☒

21CN FF Ack Zeit: *800ms ▼

Telefonbuch Kunden ID

Tel. Empfänger 1: Keine

Tel. Empfänger 2: Keine

Abbruch Übernehmen

Menu:

- Info
- Status
- Komponenten
- Ausgänge
- Teilbereiche
- System
- Kommunikation
- Pflegenotruf
- Logbuch
- Tastatur

Name/function	Explanation (checkbox)
Tel Recipients 1 to 2	After clicking in the selection field, a pop-up window appears, where the desired telephone number of a recipient can be selected from the contacts in the phone book.

ABUS		Abmelden	
Kommunikation Pflegenotruf			
Anrufmodus	*Gesperrt ▼	Protokoll	*Scancom ▼
Priorität Kommunikation	➡	Ruf Quittierung	<input checked="" type="checkbox"/>
21CN FF Ack Zeit	*800ms ▼		
Telefonbuch	Kunden ID		
Kunden-ID TB 1	00000000	Kunden-ID TB 2	00000000
Kunden-ID TB 3	00000000	Kunden-ID TB 4	00000000
Abbruch		Übernehmen	

Info
Status
Komponenten
Ausgänge
Teilbereiche
System
Kommunikation
Pflegenotruf
Logbuch
Tastatur

Name/function	Explanation (checkbox)
Account No P#	Store an 8-digit account number (factory default = 00000000) for switching to a social care alarm centre or alarm receiving centre for the partition in question.

Speech Dialler

ABUS Abmelden

Kommunikation | Sprachwahlgerät

Freigegeben ☐ Ruf Quittierung ☒

Priorität Kommunikation

Ereignis

Ziele

Info

Status

Komponenten

Ausgänge

Teilbereiche

System

Kommunikation

Pflegenotruf

Logbuch

Tastatur

Name/function	Explanation (checkbox)
Enabled	Activated The speech dialler function is available. Deactivated The speech dialler function is not available.
Telecoms Priority	Set the order in which the communication methods should be used here. <ul style="list-style-type: none"> Ethernet 1, 2, 3 or No PSTN 1, 2, 3 or No GSM 1, 2, 3 or No
Call Acknowledge	Activated The alarm transmission must be confirmed by the recipient with "5" or "9" Pressing DTMF button "5": calls to this number are ended. Otherwise the calls are repeated and additional numbers are called. Pressing DTMF button "9": the calling sequence on the alarm panel is terminated. Deactivated If the function is deactivated, the call is treated like a transmission when the called line is answered.

Speech Dialler, Triggers



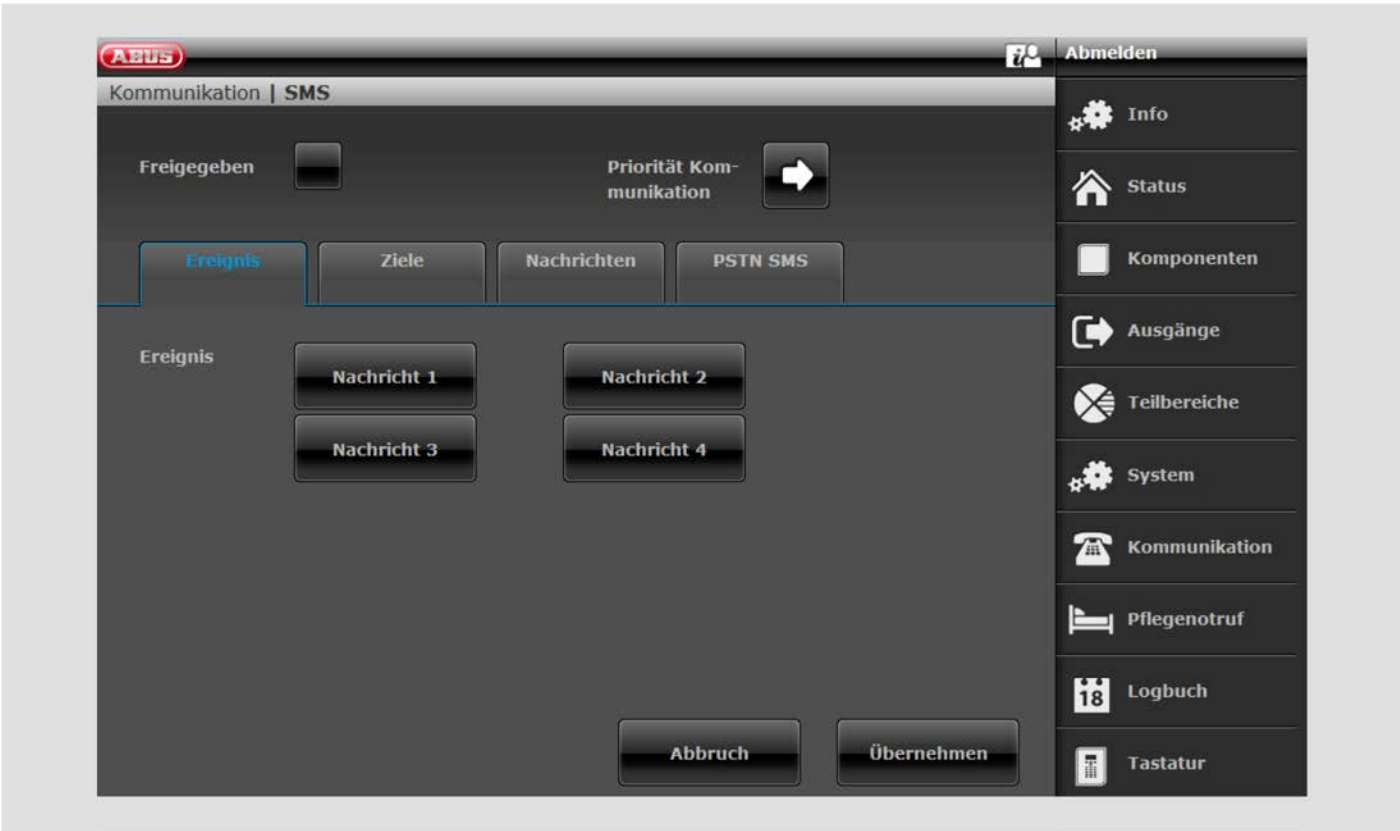
Name/function	Explanation (checkbox)
Trigger #	<div>Dropdown selection field for:</div> <ul style="list-style-type: none">• None• Burglar Alarm• Hold Up Alarm• Fire Alarm• Medical Alarm• Social Care Alarm• Social Inactivity• Technical Alarm• Soak Test Fault• Mains Fault• Tamper• Jamming

Speech Dialler, Destinations

The screenshot shows a software interface for configuring a speech dialler. A central pop-up window is displayed over the main configuration area. The pop-up window has a title bar with 'Ruf Quittierung' and a checked checkbox. It contains a list of eight recipients, each with a label 'Empfänger 1' through 'Empfänger 8' and a text input field containing the word 'Keine'. At the bottom of the pop-up are two buttons: 'Abbruch' and 'Übernehmen'. The background interface includes a sidebar on the left with options like 'Freigegeben', 'Priorität Kommunikation', 'Ereignis', and 'Ziele', and a sidebar on the right with icons for 'Status', 'Komponenten', 'Ausgänge', 'Teilbereiche', 'System', 'Kommunikation', 'Pflegenotruf', 'Logbuch', and 'Tastatur'.

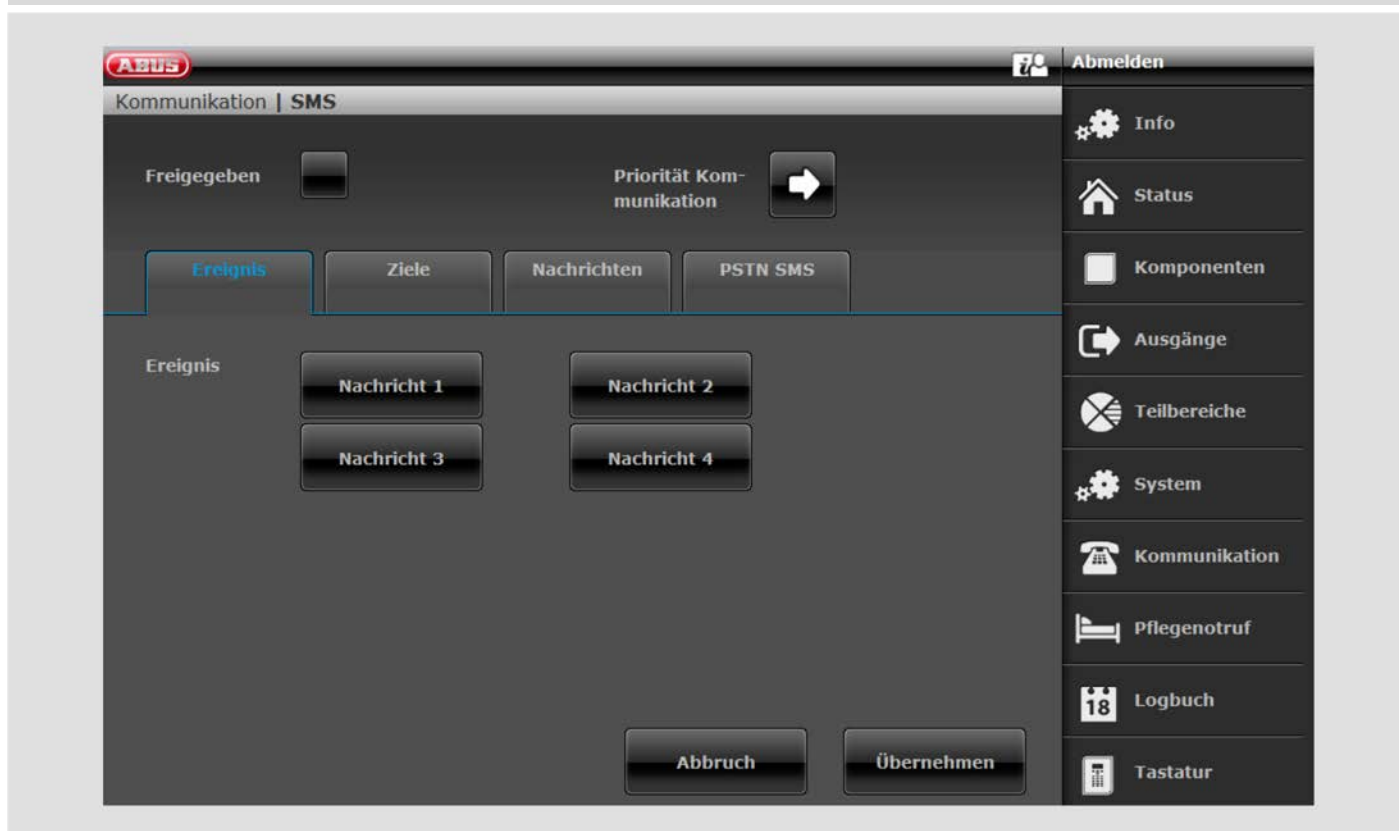
Name/function	Explanation (checkbox)
Recipient #	After clicking in the selection field, a pop-up window appears, where the desired telephone number or SIP ID of a recipient can be selected from the contacts in the phone book.

SMS



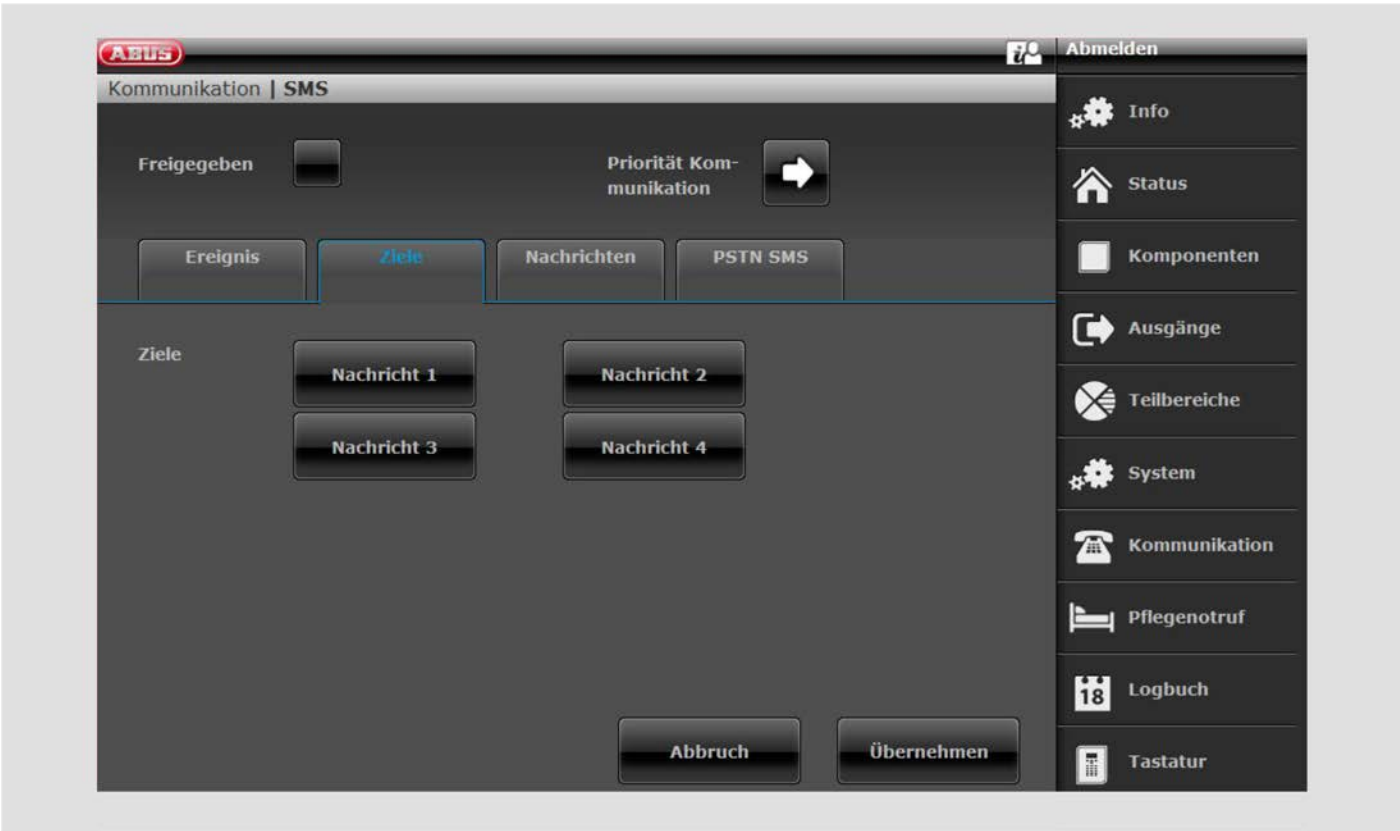
Name/function	Explanation (checkbox)
Enabled	Activated The SMS function is available. Deactivated The SMS function is not available.
Telecoms Priority	Set the order in which the communication methods should be used here. <ul style="list-style-type: none">• PSTN 1, 2, 3 or No• GSM 1, 2, 3 or No

SMS, Triggers



Name/function	Explanation (checkbox)
Message #	<p>After clicking in a selection field, a pop-up window appears, where the desired trigger for message 1 to 4 can be selected:</p> <ul style="list-style-type: none"> • Tamper • Alarms • Sets/Unsets • System

SMS, Destinations



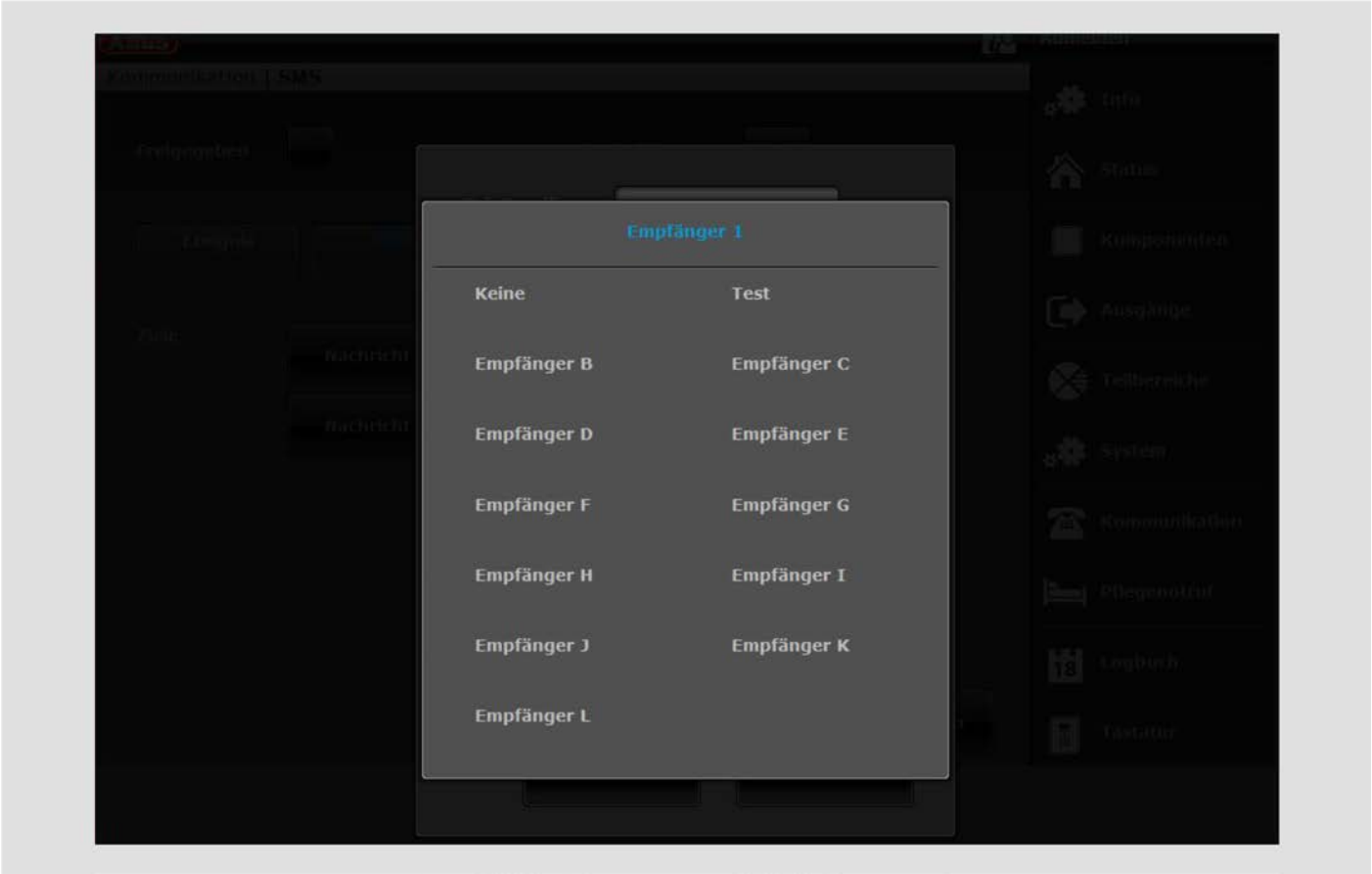
Name/function	Explanation (checkbox)
Message #	After clicking in the selection field, a pop-up window appears, where the desired telephone number of a recipient can be selected from the contacts in the phone book.

SMS, Destinations, Message

The screenshot shows a software interface for SMS configuration. A central dialog box is open, titled 'SMS', with a list of eight recipients labeled 'Tel. Empfänger 1' through 'Tel. Empfänger 8'. Each label is followed by a button labeled 'Keine'. At the bottom of the dialog are two buttons: 'Abbruch' and 'Übernehmen'. The background interface includes a top bar with 'Kommunikation | SMS' and 'Abmelden'. On the left, there are sections for 'Freigegeben', 'Ereignis', 'Ziele', and 'Nachricht'. On the right, a sidebar contains icons and labels for 'Info', 'Status', 'Komponenten', 'Ausgänge', 'Teilbereiche', 'System', 'Kommunikation', 'Pflegenotruf', 'Logbuch', and 'Tastatur'.

Name/function	Explanation (checkbox)
Tel Recipient #	Selection of recipient 1 to 8 for message 1 to 4.

SMS, Destinations, Message, Telephone Recipients



Name/function	Explanation (checkbox)
None	Do not select any recipients
Recipient #	Select contact data for recipient A to L

SMS, Messages

ABUS

Kommunikation | SMS

Freigegeben ☐

Priorität Kommunikation

Ereignis Ziele **Nachrichten** PSTN SMS

Standortnachr.

Nachricht 1 Nachricht 2

Nachricht 3 Nachricht 4

Abbruch Übernehmen

Abmelden

- Info
- Status
- Komponenten
- Ausgänge
- Teilbereiche
- System
- Kommunikation
- Pflegetruf
- Logbuch
- Tastatur

Name/function	Explanation (checkbox)
Home Message	Store a home message (max. 30 characters)
Message #	Store message 1 to 4 (max. 30 characters)

SMS, PSTN SMS

ABUS

Abmelden

Kommunikation | SMS

Freigegeben

Priorität Kommunikation

Ereignis

Ziele

Nachrichten

PSTN SMS

Protokoll

*ETSI Protocol 1

TAP 8N1

TAP 7E1

UCP 8N1

UCP 7E1

*ETSI Protocol 1

SMSC Ruf Nr.

1470,17094009

Abbruch

Übernehmen

Info

Status

Komponenten

Ausgänge

Teilbereiche

System

Kommunikation

Pflegenotruf

Logbuch

Tastatur

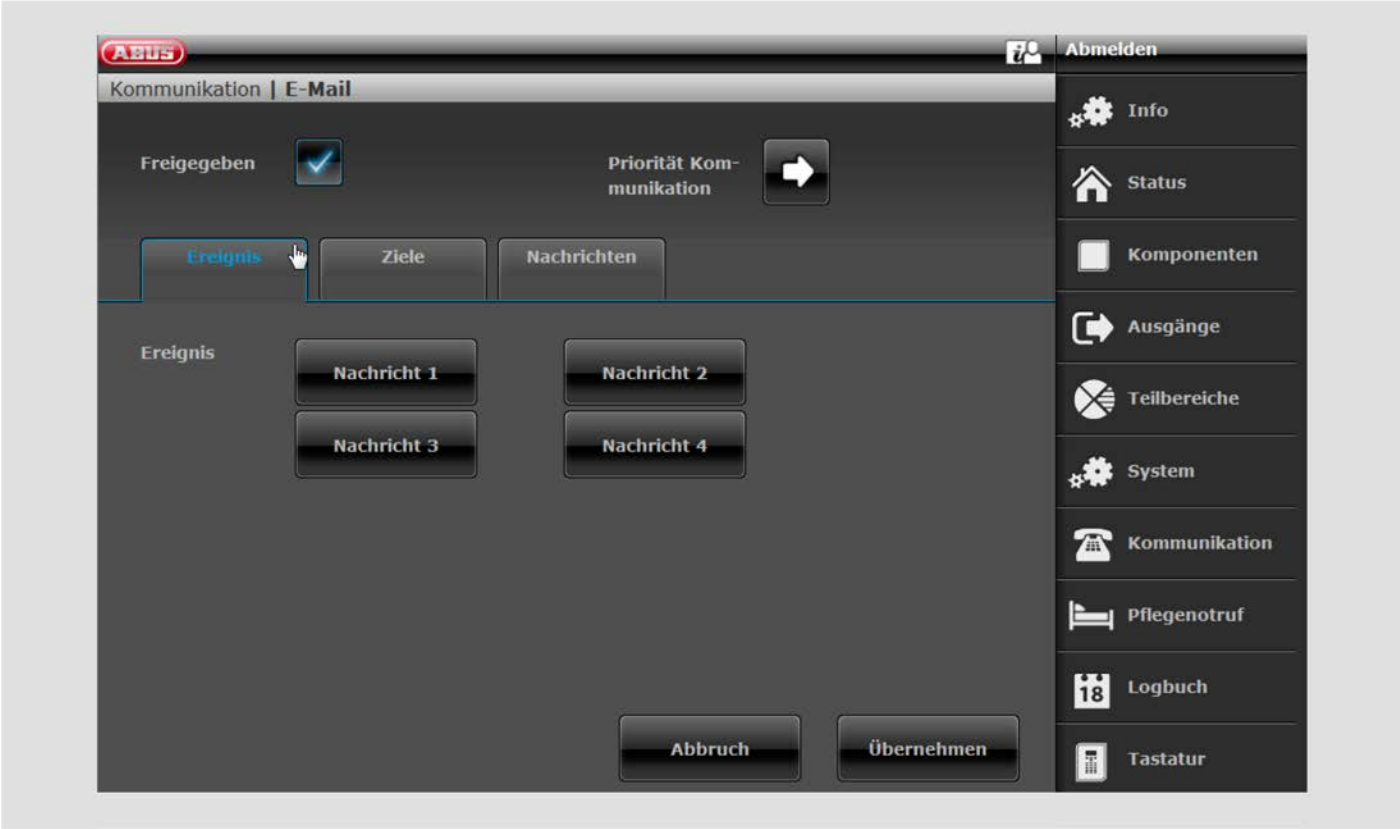
Note
If you do not have an integrated GMS module but want to send SMS messages over the PSTN line, you need to configure some additional data under this menu.

It is possible to send SMS messages with many landline telephone connections.
The connection must be enabled for this, however, and all telecommunications equipment connected between the end of line and first TAE socket and the wireless alarm panel must support the CLIP function.

Name/function	Explanation (checkbox)
Protocol	<p>Select the protocol specified to you by the SMS service centre.</p> <p>Dropdown menu with the following options:</p> <ul style="list-style-type: none">• TAP 8N1• TAP 7E1• UCP 8N1• UCP 7E1• ETSI Protocol 1

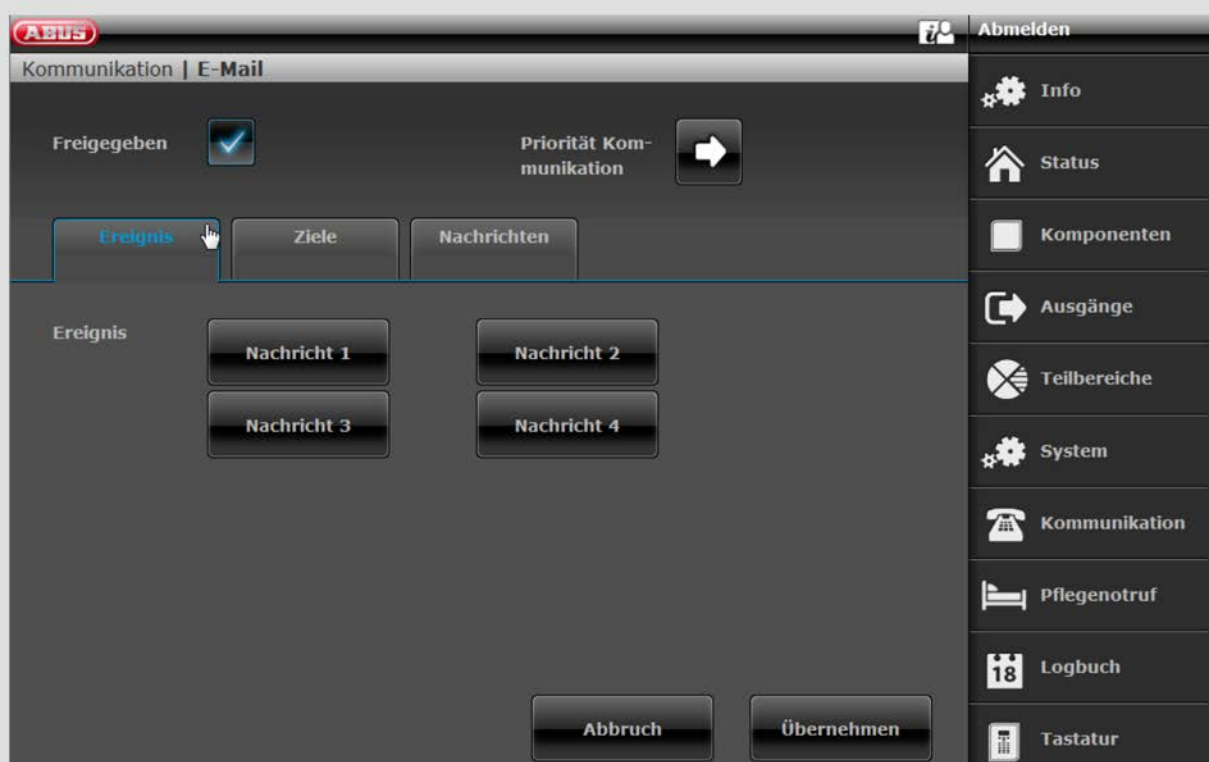
Name/function	Explanation (checkbox)
Service Centre Tel.	<p>Enter the number to dial for the service centre (F-SMSC) given to you. The service centre number and protocol must correspond. Contact your service provider's technical support. When enquiring after the number of the service centre, ask which protocol it supports.</p> <p>Store the service centre number (number of the SMS service centre for SMS messages from the landline). The country-specific numbers can be found in the appendix "SMS notifications".</p> <p>Note To send SMS messages from the GSM network (starting from the GSM module) the number of the SMS service centre for the network operator in question is already stored on the SIM card. You can check the number stored there using a mobile phone if necessary. A selection can be found in the appendix "SMS notifications", second part.</p>
Own Telephone No	<p>Some SMS service centres or protocols require the calling number before they accept a processing request for an SMS message. (This is also used for clear invoicing of SMS messages.) Enter the Secvest landline number here.</p> <p>Only available when one of the following UCP protocols has been selected in the dropdown menu:</p> <ul style="list-style-type: none"> • UCP 8N1 • UCP 7E1

Email



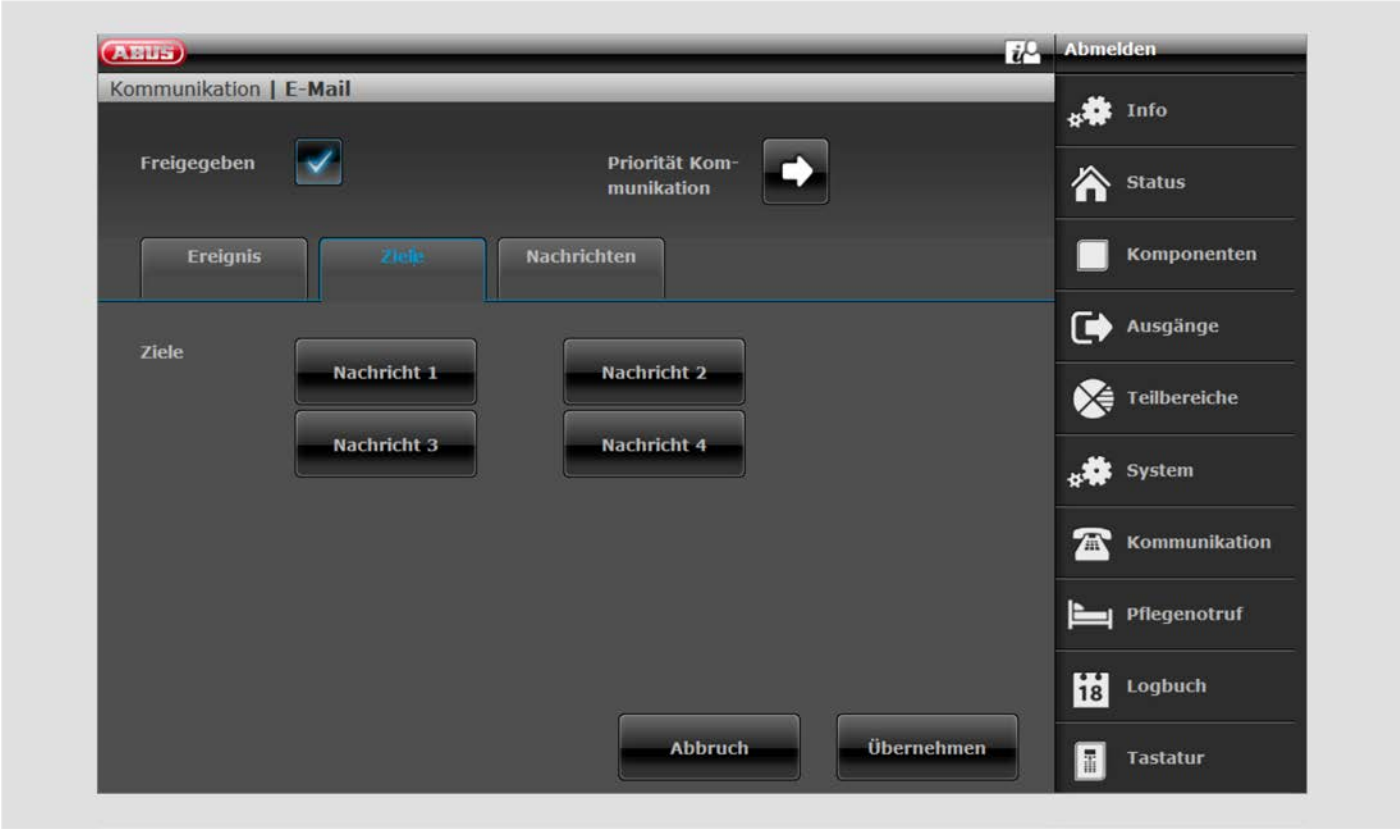
Name/function	Explanation (checkbox)
Enabled	Activated
	The email function is available.
	Deactivated
	The email function is not available.
Telecoms Priority	Set the order in which the communication methods should be used here.
	• Ethernet 1, 2, 3 or No

Email, Triggers



Name/function	Explanation (checkbox)
Message #	<p>After clicking in a selection field, a pop-up window appears, where the desired trigger for message 1 to 4 can be selected:</p> <ul style="list-style-type: none"> • Tamperers • Alarms • Sets/Unsets • System

Email, Destinations



Name/function	Explanation (checkbox)
Message #	After clicking in the selection field, a pop-up window appears, where the desired email address of a recipient can be selected from the contacts in the phone book.

Email, Messages

ABUS Abmelden

Kommunikation | E-Mail

Freigegeben ☒ Priorität Kommunikation

Ereignis Ziele **Nachrichten**

Standortnachr. **Secvest Lab Wand**

Nachricht 1 **Tamper Alarm** Nachricht 2 **Normal Alarm**

Nachricht 3 **System Alarm** Nachricht 4

Abbruch **Übernehmen**

Abmelden

- Info
- Status
- Komponenten
- Ausgänge
- Teilbereiche
- System
- Kommunikation
- Pflegetruf
- Logbuch
- Tastatur

Name/function	Explanation (checkbox)
Home Message	Store a home message (max. 30 characters)
Message #	Store message 1 to 4 (max. 30 characters)

140

Name/function	Explanation (checkbox)
Ethernet Line Fault Delay	Time in seconds until the alarm system responds to a fault in the internet connection.
PSTN Line Fault Delay	Time in seconds until the alarm system responds to a fault in the telephone connection.
GSM Line Fault Delay (only when GSM module is used)	Time in seconds until the alarm system responds to a fault in the GSM connection.
GSM Omit Digit (only when GSM module is used)	<p>Activated</p> <p>If activated, the first digit of the saved telephone number in the phone book is not selected with the rest of the number for a GSM connection.</p> <ul style="list-style-type: none"> • If you want to make calls from a telephone of a private branch exchange into the public telephone network, you must first dial what is known as the exchange access code (code for an outside line) before you dial the telephone number. • In this case the exchange access code must be entered as the first digit in the phone book on the alarm panel. • This is followed by the actual destination telephone number. • The exchange access code is available from the administrator of the private branch exchange or in the instructions of the private branch exchange. • It is usually the number "0"; in the UK it is usually the number "9". • Format of the telephone number: "0 0123 4567890". • The alarm panel can therefore also be connected to an analogue extension of a private branch exchange. • This extension does not necessarily have to be set up for automatic outside line dialling. <p>Deactivated</p> <p>On a private branch exchange, if you are using an extension that is programmed for automatic outside dialling, or if you are using a regular analogue telephone connection, select "Deactivated".</p> <p>The setting "GSM Omit Digit=Activated" affects numbers to dial for:</p> <ul style="list-style-type: none"> • ARC reporting • Social Care • Speech Dialler <p>SMS messages are normally sent only via GSM. The normal destination numbers are saved in the phone book:</p> <ul style="list-style-type: none"> • Format of the telephone number: "0123 4567890". • With a private branch exchange, the alarm panel is connected to an analogue extension without automatic outside line dialling. • If you want to implement SMS dispatch that starts on the analogue connection of the alarm system, then under • Installer Mode → Communications → SMS → PSTN SMS → Service Centre Tel. • Configure the exchange access code before the actual service centre telephone number. • Format of the telephone number: "0 0123 4567890".

Configuration

Name/function	Explanation (checkbox)
Call-in control	<p>Activated</p> <p>When this option is activated, the user can call the alarm system remotely. After the user has sent an access code to the wireless alarm panel in order to identify themselves, they can send commands using the telephone keypad.</p> <p>Deactivated</p> <p>When this option is deactivated, the user can no longer call the alarm system remotely.</p>
Rings to Answer (only when "Call-in control" is activated)	<p>Select when the wireless alarm panel answers a call.</p> <ul style="list-style-type: none">• 3 rings• 5 rings• 7 rings• 10 rings• 15 rings• 255 rings <p>Note</p> <p>If the value is set to 255, the alarm panel never answers the call.</p>
Answer on 1 ring (only when "Call-in control" is activated)	<p>Activated</p> <p>If the function is activated, the dial-in for remote configuration runs in stages. The telephone dials the alarm system, rings twice and establishes the connection. The alarm panel is activated by this call.</p> <p>The wireless alarm panel answers the next call immediately, provided this call occurs within 10 to 90 seconds. The "Rings to Answer" function is overridden in this case.</p> <p>Deactivated</p> <p>If this function is deactivated, the "Rings to Answer" function takes over from the first call.</p>

Contacts

Kommunikationen | Kontakte

Empfänger 1	Empfänger A	Empfänger 2	Empfänger B
Empfänger 3	Empfänger C	Empfänger 4	Empfänger D
Empfänger 5	Empfänger E	Empfänger 6	Empfänger F
Empfänger 7	Empfänger G	Empfänger 8	Empfänger H
Empfänger 9	Empfänger I	Empfänger 10	Empfänger J
Empfänger 11	Empfänger K	Empfänger 12	Empfänger L

Abbruch

Abmelden

- INFO
- Status
- Komponenten
- Ausgänge
- Teilbereiche
- System
- Kommunikationen
- Pflegenotruf
- Logbuch
- Tastatur

Up to 12 recipients can be defined here, to whom messages are sent.

Name: Empfänger A

Telefon Nr. 1

Telefon Nr. 2

E-Mail

IP Adresse

SIP Ben. ID

Abbruch Übernehmen

Social Care

ABUS

Logbuch | Pflegenotruf

Start Überwachung

8:00

Ende Überwachung

20:00

Überwachungs-Intervall

4

Lautstärke Sprache

3

Abbruch

Übernehmen

Abmelden

Info

Status

Komponenten

Ausgänge

Teilbereiche

System

Kommunikation

Pflegenotruf

18 Logbuch

Tastatur

Name/function	Explanation (checkbox)
Start Monitoring Hr	Start time of social care monitoring (hh:mm).
End Monitoring Hr	End time of social care monitoring (hh:mm).
Monitoring Interval	Interval in hours.
Language Volume	Volume of voice announcement.

Test (only available on alarm panel)

Select the corresponding function.

their features can be found in the following table.

An overview of the different functions and

Function	Meaning
Walk Test	<p>Chime</p> <ul style="list-style-type: none"> • On An info tone sounds when a detector is operated. • Off No info tone sounds. <p>System</p> <p>All detectors belonging to the system can be tested here. Activate all detectors in the building one after the other. If a detector is triggered the alarm panel emits two signal tones. It also indicates on the display whether a tamper contact (S) and/or alarm (A) was triggered. The top of the display shows the number of zones still to be tested (alarm and tamper). When all detectors have been tested the system writes "All Zones tested".</p> <p>Partitions</p> <ul style="list-style-type: none"> • Detectors from a specific partition can be tested here. • Once the partitions are selected only the detectors in the selected partitions are displayed. <p>Zones</p> <ul style="list-style-type: none"> • Selected detectors can be tested here. • A list of all detectors appears. Select the detectors to be tested with Yes.
Keypad	<p>Press all buttons on the keypad one after the other.</p> <p>The corresponding character or button function is shown on the display in response.</p> <p>Press the dual keys (fire alarm, hold up alarm, medical emergency or social care alarm) at the same time to test them.</p> <p>The function of the key combination is shown on the display in response.</p>
Sirens & Sounders	<p>Int.Sirens</p> <ul style="list-style-type: none"> • The sounders on the alarm panel, info module, indoor siren and wireless control device are actuated. <p>Ext. Radio Sirens</p> <ul style="list-style-type: none"> • The sounders for the wireless external sirens are actuated. <p>Sounder Module</p> <ul style="list-style-type: none"> • The sounders for the external sirens are actuated. External siren in connection with the wireless accessory module (WAM) as a "Sounder Module". <p>Loudspeakers</p> <ul style="list-style-type: none"> • Select "Play/Stop" to hear all existing messages in the system one after the other.

Function	Meaning
Control Devices	<p>Press the function buttons on the wireless control device one after the other. Wait 2 to 3 seconds between each button so that the control device can send each message. A corresponding letter appears on the display in response: A = "arm" button (closed lock) C = "internal arm" button (*) D= "query status" button (?) B = "disarm" button (open lock)</p> <p>To test the number buttons, press 4 or 6 numerical buttons (corresponding to the set code length) and then a function button: Example:</p> <ul style="list-style-type: none">• Press : 1234?• Displayed : 1234D <p>Press the dual keys (fire alarm, hold up alarm, medical emergency or social care alarm) at the same time to test them. On the display:</p> <p>F = dual keys fire alarm P = dual keys hold up M = dual keys medical emergency H = dual keys social care alarm</p> <p>The lower "*" and "#" button on the control device cannot be tested.</p>
Door Locks	<p>Select the door lock to be tested. Operate the corresponding door lock. After unlocking, "Unlocked" appears on the display. After locking, "Locked" appears on the display.</p> <ul style="list-style-type: none">• Secvest key: press the button and then lock.• Additional door lock: do not press the button. Then lock. <p>Note</p> <p>You can check here whether DIP switch 3 in the Secvest key is correctly set according to the door stop.</p> <p>The received signal strength is also displayed.</p> <p>The meaning of the number before and inside the brackets can be found in the signal strength explanation on the following page.</p>

Function	Meaning
Signal Strengths	<p>This option can be used to check the received signal strengths of all wireless components of the system.</p> <p>The number before the brackets is the signal strength of the last received signal.</p> <p>The number inside the brackets is the smallest signal strength received since the last reset.</p> <p>The alarm panel records the received signal strengths, even if you do not see them in this menu.</p> <p>If you use a WAM as a repeater to strengthen weak signals from wireless components, you will barely notice a change between the corresponding components. For this reason, use the display of the signal strength for the corresponding WAM in order to gain information about the signal strength of the repeated signals from the wireless components. Press the # button to delete the recorded signal strengths for the selected component.</p> <p>Detectors</p> <ul style="list-style-type: none"> • The display shows the signal strength of each taught-in detector. • The zone names are displayed. To view the zone numbers, press the right menu key. <p>Control Devices</p> <ul style="list-style-type: none"> • The display shows the signal strength of each taught-in control device. <p>External Sirens</p> <ul style="list-style-type: none"> • The display shows the signal strength of each taught-in wireless external siren. <p>WAM</p> <ul style="list-style-type: none"> • The display shows the signal strength of each taught-in WAM. <p>Door Locks</p> <ul style="list-style-type: none"> • The display shows the signal strength of each taught-in door lock.
Outputs	<p>Radio Outputs</p> <ul style="list-style-type: none"> • Use this option to check all configured radio outputs. <p>Wired Outputs</p> <ul style="list-style-type: none"> • Use this option to check all configured wired outputs. <p>After exiting the menu, all outputs switch back to their basic configured state.</p>
Prox Tag	<p>Move the chip key across the reader area at the bottom of the alarm panel (where the ABUS logo is).</p> <p>The following information appears on the display:</p> <ul style="list-style-type: none"> • which user is assigned to this chip key or • that the chip key is not recognised by the alarm panel.

Function	Meaning
Remotes	<p>Press a button on the remote control.</p> <p>The following information appears on the display:</p> <ul style="list-style-type: none"> • the consecutive number of the remote control • a letter or character corresponding to the pressed button A = "arm" button (closed lock) * = "internally arm" button or button for activating a "User Defined" output (*) ? = "query status" button (?) D = "disarm" button (open lock) • which user is assigned to this remote control • the function of the pressed button <ul style="list-style-type: none"> - F. Set All - Prt Set All or Output On (Off or Toggle) xyz - Query Status - Unset All • the received signal strength (RSSI) <p>Example Remote 001,D>User 002 Unset All RSSI: 9</p>
Pendants	<p>Press the button on a pendant.</p> <p>The following information appears on the display:</p> <ul style="list-style-type: none"> • which user is assigned to this pendant • the function of this pendant HUA = hold up alarm Medical = medical emergency Soc. care alm = social care alarm • the received signal strength (RSSI) <p>Example User: User 002 Func: Medical RSSI: 9</p>

Function	Meaning
ARC reporting	<p>ARC Reporting must be activated. Installer Mode->Communications->ARC Reporting ->Call Mode ->Single (or Alternate) A list of the available connected transmission methods can be seen.</p> <p>Ethernet</p> <ul style="list-style-type: none"> • When this is selected, the 2 possible configured recipients (IP Recipient 1, IP Recipient 2) are displayed with their contact names. • Scroll to the desired contact. Press the "Select" button. • The alarm panel sends a test call to this recipient. • The event (or trigger) "Test" is sent according to the set protocol. <p>PSTN</p> <ul style="list-style-type: none"> • When this is selected, the 2 possible configured recipients (Tel Recipient 1, Tel Recipient 2) are displayed with their contact names. • Scroll to the desired contact. Press the "Select" button. • The alarm panel sends a test call to this recipient. • The event (or trigger) "Test" is sent according to the set protocol. <p>GSM</p> <ul style="list-style-type: none"> • When this is selected, the 2 possible configured recipients (Tel Recipient 1, Tel Recipient 2) are displayed with their contact names. • Scroll to the desired contact. Press the "Select" button. • The alarm panel sends a test call to this recipient. • The event (or trigger) "Test" is sent according to the set protocol. <p>During the test call a series of progress messages appear on the display. If the test call was not successful, the display shows a brief message with the cause of the error.</p>
Speech Dialler	<p>Speech Dialler must be activated. Installer Mode->Communications->Speech Dialler->Call Mode->Enabled A list of the available connected transmission methods can be seen.</p> <p>Ethernet</p> <ul style="list-style-type: none"> • When this is selected, enter a valid SIP User ID. • e.g. +498207123456789@sipgate.de • Press the "OK" button. • The alarm panel establishes a connection. If the call is answered by this recipient, the recipient hears the "Home Message" and "Message 1" to "Message 4". <p>PSTN</p> <ul style="list-style-type: none"> • When this is selected, enter a number to dial. • Press the "OK" button. • The alarm panel establishes a connection. If the call is answered by this recipient, the recipient hears the "Home Message" and "Message 1" to "Message 4". <p>GSM</p> <ul style="list-style-type: none"> • When this is selected, enter a number to dial. • Press the "OK" button. • The alarm panel establishes a connection. If the call is answered by this recipient, the recipient hears the "Home Message" and "Message 1" to "Message 4".

Function	Meaning
Speech Dialler, cont.	<p>If "Call Acknowledge" is activated:</p> <ul style="list-style-type: none">• The recipient can acknowledge and end the call with 5 or 9 if the following is set: Installer Mode->Communications->Speech Dialler->Call Acknowledge->Enabled.• During the test call a series of progress messages appear on the display.• If the test call was not successful, the display shows a brief message with the cause of the error.
SMS	<p>SMS must be activated. Installer Mode->Communications->SMS->Call Mode->Enabled</p> <p>A list of the available connected transmission methods can be seen.</p> <p>PSTN</p> <ul style="list-style-type: none">• When this is selected, enter a number to dial.• Press the "OK" button.• The alarm panel sends an SMS to this number. <p>GSM</p> <ul style="list-style-type: none">• When this is selected, enter a number to dial.• Press the "OK" button.• The alarm panel sends an SMS to this number.• The recipient receives an SMS in the following form: <Home Message>: 10:56 21/01/2015 SMS Test Call• During the test call a series of progress messages appear on the display.• If the test call was not successful, the display shows a brief message with the cause of the error.
Email	<p>Email must be activated. Installer Mode->Communications->Email->Call Mode->Enabled</p> <ul style="list-style-type: none">• If this is selected, enter a valid email address.• Press the "OK" button.• The alarm panel sends an email to this address.• The recipient receives an email in the following form: Subject: <Home Message>: Email Test Call Text: <Home Message>: 11:09 21/01/2015 Email Test Call <ul style="list-style-type: none">• During the test call a series of progress messages appear on the display.• If the test call was not successful, the display shows a brief message with the cause of the error.

Function	Meaning
Zone Resistances	<p>The current resistances for the wired zones are displayed here.</p> <p>The zone names are displayed. To view the zone numbers, press the right menu key.</p> <p>Test all variants according to the type of wiring to determine whether they meet the requirements:</p> <ul style="list-style-type: none"> • Alarm contact open/closed • Tamper contact open/closed • Short circuits • Open (isolated circuits) <p>0k00 means 0 ohms or NC</p> <p>For wiring type "4-wire CC" the display switches between the resistance of the alarm loop (A) and the resistance of the tamper loop (S).</p> <p>Example for a "2-wire FSL 2K2/4K7" zone</p> <ul style="list-style-type: none"> • Alarm contact closed (standby) 2k18 • Alarm contact open 6k89 • Alarm contact open and series resistor bridged 4k68 • Short circuit in line to detector 0k00 • Line disconnection NO
Panel PSU	<p>Here you can find information about the voltage values of the power supply:</p> <p>Ext. DC Voltage In</p> <ul style="list-style-type: none"> • The voltage value of the external DC power source <p>Panel Battery 1</p> <ul style="list-style-type: none"> • The voltage value of the first battery <p>Panel Battery 2</p> <ul style="list-style-type: none"> • The voltage value of the second battery <p>Aux. Voltage Out</p> <ul style="list-style-type: none"> • The voltage value at the terminal clamp 0 V/12 V AUX <p>Example (battery 2 is not connected in this example)</p> <ul style="list-style-type: none"> • Ext. DC Voltage In 14.1 volts • Panel Battery 1 8.3 volts • Panel Battery 2 0.1 volt • Aux. Voltage Out 13.9 volts

View Log

The screenshot displays the ABUS Logbuch (Log Book) interface. The main area shows a list of log entries with the following columns: Datum (Date), Zeit (Time), and a description. The right sidebar contains navigation options: Abmelden, INFO, Status, Komponenten, Ausgänge, Teilbereiche, System, Kommunikationen, Pflegenotruf, Logbuch (selected), and Tastatur. The bottom of the interface features a numeric keypad with buttons for navigation and selection.

Datum	Zeit	Ben 000 Log in(9999)
18/11/2014	17:33:05	Ben000 Log in (Web)(9999)
18/11/2014	15:38:15	Ext DC ok TB 1
18/11/2014	15:38:15	Zentrale Ext DC ok
18/11/2014	15:35:49	Ext DC Störung TB 1
18/11/2014	15:35:41	Zentrale Ext DC Störung
18/11/2014	15:22:59	Ben 001 TB 1 deakt(Alex)
18/11/2014	15:22:56	Ben 001 TB 1 akt(Alex)
18/11/2014	15:21:33	Ben001 Log in (Web)(Alex)
18/11/2014	15:21:18	Ben 000 Log out(9999)

You can view the log book in this menu.

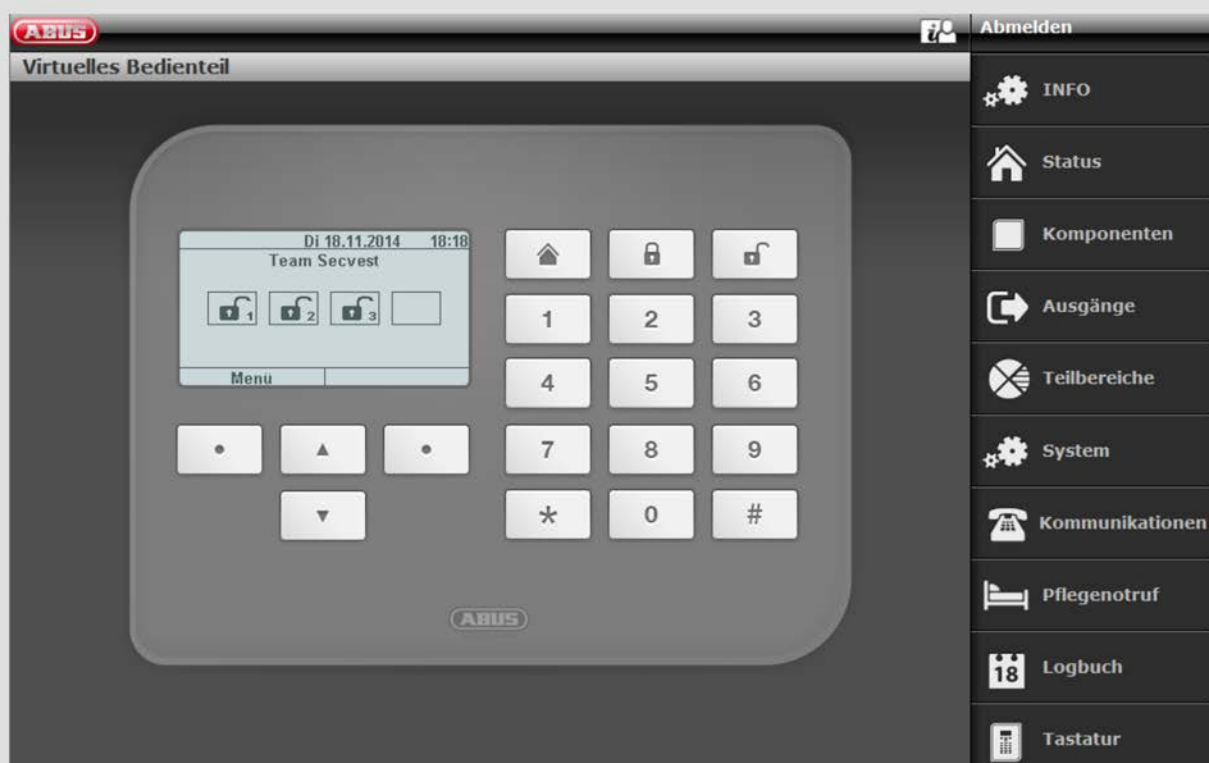
The log book contains all of the relevant data for the alarm panel including the date and time.

The memory can hold up to 600 entries.

If the memory is full, the oldest entry is deleted and overwritten with the new entry ("first in first out" principle).

The following provides an overview of the possible log entries.

Virtual keypad



The virtual keypad has all the functionality of the keypad and display of the alarm panel.

On the alarm panel you press the corresponding buttons.

On the virtual keypad, you click the corresponding buttons using the mouse.

The displays on the virtual keypad are the same as those on the alarm panel.

Note the following:

If you are logged in as an installer on the web server, you open the virtual keypad in installer mode after entering an installer code.

If you are logged in as a user/administrator on the web server, you open the virtual keypad in the user menu after entering a user code.

Appendix	
Technical data	
General	
Material	ABS
Protection class	IP34
Environmental class	II (EN 50131-1 + A1:2009)
Operating temperature	0°C to 40°C
Max. humidity	Average relative humidity approx. 75% – non-condensing
Dimensions (W x H x D)	205 x 285 x 48 mm
Weight	1.453 kg
Power supply	
Operating voltage/frequency	110 V/230 V AC, 50/60 Hz, (85-265 V AC, 50/60 Hz) 13.8 V DC
Power consumption	6.9 W 6.9 W x 24 x 365 = 60 kWh per year 300 mA @ 13.8 V
Fuse	T1A (AC input)
Backup power supply	
Battery	Polymer lithium ion, 7.4 V
Capacity	2500 mAh
Minimum running time in emergency power mode	12 hours (24 hours with optional second battery)
Wireless signal transmission	
Frequency	868.6625 MHz
	In accordance with: <ul style="list-style-type: none"> • EN 300 220-2 • EN 50131-5-3 Grade 2
	Frequency band reserved for applications in the security sector
Modulation	FM
Bandwidth	Narrow band
Transmission power	10 mW
Antenna	Integrated Duplex antenna technology
Range	Indoors: approx. 30 metres (depending on the site conditions) Outdoors: approx. 100 metres
Special features	Individual identification

Safety	
Wireless components	16,777,214 ($2^{24} - 2$) different IDs per component type
Access codes	10,000 code variants with 4-digit codes (0000-9999) 1,000,000 code variants with 6-digit codes (000000-999999) The digits of the code are numbers between 0 and 9.
Proximity chip key	4,294,967,296 (2^{32})
Access lock	Locked for 3 min after 3 incorrect entries in succession
Web encryption	
	HTTPS SSL version 3/TLS 1.2
EMC immunity	In accordance with EN 50130-4
EMC emissions	In accordance with EN 61000-6-3
Electrical safety	In accordance with EN 60950-1
Environmental class	II (EN 50131-1 + A1:2009)
Security grade	2 (EN 50131-1 + A1:2009)
Options of the alarm system	
Users	50
Zones	3 IP zones
	48 wireless zones 4 wired zones for DEOL/FSL or 2-wire CC 2 wired zones for 4-wire CC Various wiring options: <ul style="list-style-type: none"> • 2-wire FSL 2K2/4K7 • 2-wire FSL 1K/1K • 2-wire FSL 2K2/2K2 • 2-wire FSL 4K7/4K7 • 4-wire CC • 2-wire CC
Wireless control devices	Up to 8
Proximity keyfob	Up to 50
Secvest keys/additional door locks	8
IP camera zones	Up to 3 (for defined ABUS camera models)
Remotes	Up to 50

Options of the alarm system	
Outputs	2 relay outputs <ul style="list-style-type: none"> • Potential-free, changeover contact NO / C / NC • Max. load capacity: 500 mA at 24 V AC rms or 30 V DC 2 transistor outputs <ul style="list-style-type: none"> • Open-drain • Max. load capacity: 500 mA at 13.8 V DC
Wireless outputs	32
Sirens	4 x wireless outdoor (external) sirens 1 x wired outdoor (external) siren with 13.8 V up to 700 mA
GSM/GPRS	Optional plug-in module
PSTN	a/b connection
Ethernet	10/100 RJ45
Wireless accessory module WAM	8
PSTN SMS protocols	TAP 8N1 TAP 7E1 UCP 8N1 UCP 7E1 ETSI Protocol 1
Email	Up to 8 email addresses
Alarm receiving centre protocols	ARC Analogue : Fast Format, Contact ID, SIA IP : SIA-IP (DC-09) with Fast Format, Contact ID, SIA Social care : Scancom, Scanfast, Tunstall
VoIP/SIP	Up to 8 receivers via VoIP/SIP
Scheduler	Up to 10 individual schedules for arming/disarming the system
Event log	500+100 entries
Partitions	4
Voice messages	33 pre-recorded voice messages in any language 5 messages recorded by the user 1 memo message
Configuration	Via the integrated web server or directly on the alarm panel

Email error messages

The following table shows the SMTP server response codes:

200	Non standard success response, see RFC876
211	System status, or system help reply
214	Help message
220	<domain> service ready
221	<domain> service closing transmission channel
235	Successful authentication
250	Requested mail action OK, completed
251	User not local, will forward to <forward-path>
252	Cannot VRFY user, but will accept message and attempt delivery
253	Pending message for node started
334	Server challenge
354	Start mail input, end with <CRLF>.<CRLF>
355	Octet offset is the transaction offset
421	<domain> service not available, closing transmission channel
432	A password transition is needed
450	Requested mail action not taken: mailbox unavailable
451	Requested action aborted: error in processing
452	Requested action not taken: insufficient system storage
453	No mail
454	TLS not available due to temporary reason. Encryption required for requested authentication mechanism
455	Server unable to accommodate parameters
458	Unable to queue message for node
459	Node not allowed: <reason>
500	Syntax error, command unrecognized
501	Syntax error in parameters or arguments
502	Command not implemented
503	Bad sequence of commands
504	Command parameter not implemented
510	Check the recipient address
512	<domain> cannot be found. Unknown host
515	Destination mailbox address invalid
517	Problem with senders mail attribute, check properties
521	<domain> does not accept mail (see RFC1846)
522	Recipient has exceeded mailbox limit
523	Server limit exceeded. Message too large
530	Encryption required for authentication mechanism
531	Mail system full
533	Remote server has insufficient disk space to hold email
534	Authentication mechanism is too weak. Message too big
535	Authentication unsuccessful/Bad username or password
538	Encryption required for authentication mechanism
550	Requested action not taken: mailbox unavailable
551	User not local, please try <forward-path>
552	Requested mail action aborted: exceeded storage allocation
553	Requested action not taken: mailbox name not allowed
554	Transaction failed
555	MAIL FROM/RCPT TO parameters not recognised or not implemented

TCP/IP error messages

The following table shows the TCP/IP error messages:

1001	General Error
1002	Invalid socket descriptor
1003	Invalid parameter
1004	It would have blocked
1005	Not enough memory in memory pool
1006	Connection is closed or aborted
1007	Socket is locked in RTX environment
1008	Socket, Host Resolver timeout
1009	Host Name resolving in progress
1010	Host Name not existing

Overview of the SSL-relevant messages

The following table shows SSL-relevant messages that are used in the SSL stack – these may change in a future update:

10064	Failed to get an IP address for the given hostname
10066	Failed to open a socket
10068	The connection to the given server / port failed
10070	Binding of the socket failed
10072	Could not listen on the socket
10074	Could not accept the incoming connection
10076	Reading information from the socket failed
10078	Sending information through the socket failed
10080	Connection was reset by peer
10082	Connection requires a read call
10084	Connection requires a write call
37520	A counter would wrap (eg, too many messages exchanged).
37648	Internal error (eg, unexpected failure in lower-level module)
37776	Unknown identity received (eg, PSK identity)
37904	Public key type mismatch (eg, asked for RSA key exchange and presented EC key)
38032	Session ticket has expired.
38160	Processing of the NewSessionTicket handshake message failed.
38288	Handshake protocol not within min/max boundaries
38416	Processing of the compression / decompression failed
38544	Hardware acceleration function skipped / left alone data
38800	The requested feature is not available
38928	Bad input parameters to function
39056	Verification of the message MAC failed
39184	An invalid SSL record was received
39312	The connection indicated an EOF
39440	An unknown cipher was received
39568	The server has no ciphersuites in common with the client
39696	No RNG was provided to the SSL module
39824	No client certification received from the client, but required by the authentication mode
39952	Our own certificate(s) is/are too large to send in an SSL message
40080	The own certificate is not set, but needed by the server
40208	The own private key or pre-shared key is not set, but needed
40336	No CA Chain is set, but required to operate
40464	An unexpected message was received from our peer

40592	A fatal alert message was received from our peer
40720	Verification of our peer failed
40848	The peer notified us that the connection is going to be closed
40976	Processing of the ClientHello handshake message failed
41104	Processing of the ServerHello handshake message failed
41232	Processing of the Certificate handshake message failed
41360	Processing of the CertificateRequest handshake message failed
41488	Processing of the ServerKeyExchange handshake message failed
41616	Processing of the ServerHelloDone handshake message failed
41744	Processing of the ClientKeyExchange handshake message failed
41872	Processing of the ClientKeyExchange handshake message failed in DHM / ECDH Read Public
42000	Processing of the ClientKeyExchange handshake message failed in DHM / ECDH Calculate Secret
42128	Processing of the CertificateVerify handshake message failed
42256	Processing of the ChangeCipherSpec handshake message failed
42384	Processing of the Finished handshake message failed
42512	Memory allocation failed
42640	Hardware acceleration function returned with error

VoIP error messages

The following table shows the user-relevant error messages:

VOIP_CALL_NO_RESULT	0
VOIP_CALL_FAIL_NO_LINK	1
VOIP_CALL_FAIL_NO_LOCAL_ADDRESS	2
VOIP_CALL_REJECTED	3
VOIP_CALL_TIMEOUT_NO_ANSWER	4
VOIP_CALL_CANCELLED	5
VOIP_CALL_DECLINED	6
VOIP_CALL_FORBIDDEN	7
VOIP_CALL_NOT_FOUND	8
VOIP_CALL_INIT_SIP_URL_ERROR	9
VOIP_CALL_CALLER_ABORT	10
VOIP_CALL_DISCONNECT	11
VOIP_CALL_PASSWORD_ERROR	12
VOIP_CALL_LINK_LOST_ERROR	13

The following table shows the internal error messages:

VOIP_CALL_INIT_PARAM_ERROR	14
VOIP_CALL_PJSIP_APP_ERROR	15
VOIP_CALL_ICE_CREATE_ERROR	16
VOIP_CALL_ICE_PROCEDURE_ERROR	17
VOIP_CALL_ICE_INVITE_CREATION_ERROR	18
VOIP_CALL_ICE_REINVITE_CREATION_ERROR	19
VOIP_CALL_ICE_REINVITE_SEND_ERROR	20
VOIP_CALL_ICE_UPDATE_CREATION_ERROR	21
VOIP_CALL_ICE_UPDATE_SEND_ERROR	22
VOIP_CALL_ICE_SDP_POINTER_ERROR	23
VOIP_CALL_ICE_NEGOTIATION_FAIL_ERROR	24
VOIP_CALL_REGISTRATION_CREATION_ERROR	25
VOIP_CALL_REGISTRATION_INIT_ERROR	26
VOIP_CALL_REGISTRATION_CRED_ERROR	27
VOIP_CALL_REGISTRATION_REG_ERROR	28
VOIP_CALL_REGISTRATION_SEND_ERROR	29
VOIP_CALL_REGISTRATION_SERVER_RESPONSE_TIMEOUT	30
VOIP_CALL_REGISTRATION_RESULT_INTERNAL_ERROR	31
VOIP_CALL_REGISTRATION_SERVER_RESPONSE_ERROR	32
VOIP_CALL_PJSIP_ASSERT_ERROR	33
VOIP_CALL_AUDIO_PLAYBACK_NOT_CONNECTED_ERROR	40

Time zones



The numbers indicate the difference between the local time and UTC (Coordinated Universal Time), otherwise known as GMT (Greenwich Mean Time).

For example, the time in Germany is:

- Winter time: UTC/GMT +1
- Summer time: UTC/GMT +2

A detailed map can be found here:

<http://www.weltzeit.de/zeitzonenkarte.php>

All information subject to change.

Landline notification centre

Germany

F-SMSC operator	Protocol	Service Centre Tel.
Materna	UCP 8N1	09003 266 9002
Telekom		01930105

Additional information can be found here:

Materna

<http://www.sms-im-festnetz.de/sms/>

Telekom

<http://hilfe.telekom.de/hsp/cms/content/HSP/de/12556/Startseite/SMS;jsessionid=1620596013AB81A8BADD3E34609A213F>

<http://hilfe.telekom.de/hsp/cms/content/HSP/de/12538>

GSM network notification centre

In order to send a text message (SMS) to a predefined telephone number if an event occurs, the number of the SMS service centre must be stored on the SIM card.

This section provides an overview of the providers with their mobile phone networks and the related telephone number of the SMS service centre.



Note

For detailed information please contact your mobile phone network provider.

SMS notification

Service provider	Wireless mobile phone network	SMS service centre
Telekom (D1)	Telekom	+491710760000
Vodafone (D2)	Vodafone	+491722270333 (alternativ: +491722270000)
o2	o2	+491760000443
BASE (E-Plus)	E-Plus	+491770610000
mobilcom- debitel	Telekom	+491710760315
	Vodafone	+491722270880
	o2	+491760000462
	E-Plus	+491770602300
1&1	Vodafone	+491722270333 (alternativ: +491722270000)
blau.de	E-Plus	+491770610000
callmobile	Telekom	+491710760000
	Vodafone	+491722270333
congstar	Telekom	+491710760000
FONIC	o2	+491760000443
klarmobil	Telekom	+491710760000
	o2	+491760000466
McSIM	Vodafone	+491722270333 (alternativ: +491722270000)
PHONEX	o2	+491760000443
simyo	E-Plus	+491770610000

* All information subject to change.

To send an email to a predefined email address if an event occurs, the SMTP login data for the email account must be stored in the Secvest.

**Note**

The SMTP functionality is not available free of charge from all freemail providers.

This section provides an overview of the email providers that offer their services free of charge.

- GMX
- web.de
- Yahoo
- T-Online
- Google Mail
- Outlook

Email notification/email setup

To send an email to a predefined email address if an event occurs, the SMTP login data for the email account must be stored in the Secvest.

**Note**

The SMTP functionality is not available free of charge from all freemail providers.

This section provides an overview of the email providers that offer their services free of charge.

- GMX
- web.de
- Yahoo
- T-Online
- Google Mail
- Outlook

Appendix

* All information subject to change.

Arcor

Server name	mail.arcor.de
Server IP port number	25 or 587
Account	<email address> e.g. yourname@arcor.de
User name	<email address> e.g. yourname@arcor.de
Password	<password for email account>
SSL	Disabled

GMX

Server name	mail.gmx.net
Server IP port number	465
Account	<email address> e.g. yourname@gmx.de
User name	<email address> e.g. yourname@gmx.de
Password	<password for email account>
SSL	Enabled

GMX

Server name	mail.gmx.net
Server IP port number	25 or 587
Account	<email address> e.g. yourname@gmx.de
User name	<email address> e.g. yourname@gmx.de
Password	<password for email account>
SSL	Disabled

Googlemail

Server name	smtp.gmail.com
Server IP port number	465
Account	<email address> e.g. yourname@gmail.com
User name	<email address> e.g. yourname@gmail.com
Password	<password for email account>
SSL	Enabled

Googlemail

Server name	smtp.gmail.com
Server IP port number	25 or 587
Account	<email address> e.g. yourname@gmail.com
User name	<email address> e.g. yourname@gmail.com
Password	<password for email account>
SSL	Disabled

T-Online

Server name	securesmtp.t-online.de
Server IP port number	465
Account	<email address> e.g. yourname@t-online.de
User name	<email address> e.g. yourname@t-online.de
Password	<password for email account>
SSL	Enabled

T-Online

Server name	securesmtp.t-online.de
Server IP port number	25 or 587
Account	<email address> e.g. yourname@t-online.de
User name	<email address> e.g. yourname@t-online.de
Password	<password for email account>
SSL	Disabled

Appendix

Web.de

Server name	smtp.web.de
Server IP port number	25 or 587
Account	<email address> e.g. yourname@web.de
User name	<email address> e.g. yourname@web.de
Password	<password for email account>
SSL	Disabled

Yahoo.de

Server name	smtp.mail.yahoo.de
Server IP port number	465
Account	<email address> e.g. yourname@yahoo.de
User name	<email address> e.g. yourname@yahoo.de
Password	<password for email account>
SSL	Enabled

Yahoo.de

Server name	smtp.mail.yahoo.de
Server IP port number	25 or 587
Account	<email address> e.g. yourname@yahoo.de
User name	<email address> e.g. yourname@yahoo.de
Password	<password for email account>
SSL	Disabled

Index

- ABUS Security-Center 7, 174
- Active intrusion protection 15
- Alarm
 - External 16
- Alarm panel 15
- Alarm system 15
- Alarm type 15
- Alarm zone 15
- Antenna 155
- Arm 19
- Arm components 19
- Arming, disarming 15
- Backup power supply 155
- Battery 155
 - Capacity 155
- Bidirectional 2-way wireless 15
- Burglar alarm system 16
- Button
 - Login 30
- Certifications 21
- Chip key 16
 - Proximity keyfob, Prox Tag 16
- Coding of wireless signals 16
- Combination signalling device 18
- Communication options 18
- Communications 34
- Components
 - Connecting 24
- Configuration 18
 - Peripheral devices for the wireless alarm system 7
 - Secvest 7
- Control elements 29
- Control panel
 - Arm button 11
 - Disarm button 11
 - Proximity reader 11
- Customisation 36
- Danger alarm system 17
- Danger detector 15
- DEOL 16
- Device front 11
- Device overview 10
- Devices 18
- Disarm 19
- Display 16
- Double end of line 16
- Email notification 167
- Environmental class 156
- Ethernet 35
- Event log 157
- External siren 15
- False alarm 9
- Flood detector 21
- Frequency 155
- Function test
 - Secvest 7
- Glass breakage detector 15, 17
- GMT 163
- Handover log 7
- Housing tamper switch 24
- Individual identification 16
- Indoor siren 17
- INFO 33
- Info bar 29
- Input field
 - Password 30
 - User name 30
- Installation 17
 - Peripheral devices for the wireless alarm system 7
 - Secvest 7
 - Wireless alarm system 7
- Installing the GSM module 24
- Intended use 8
- Interior protection 17
- Internal alarm 17
- Intruder alarm system 16
- Intuitive operation 17
- Key assignment 12
- Line fuse 155
- Local alarm 18
- Logging in
 - On the Secvest 26
- Logging in/out 7
- Login button 29
- Login screen 26, 30
- MAC address 35
- Magnetic contact 18
- Main menus 29
- Medical emergency 18

- Menu structure 27
- Micro SD card 24
- Minimum running time in emergency power mode 155
- Modulation 155
- Motion detector 15
- Mounting location 10
- Mounting plate
 - Wall mounting 22
- Notification centre 163
- Online help 29
- Operating temperature 155
- Operating voltage 155
- Outputs 157
- Panel 33
- Partition selection 37
- Partitions 20, 157
- Password 26, 30
- Perimeter protection 15
- Perimeter surveillance 18
- Power consumption 155
- Power supply 155
 - Caution 9
- Power supply unit 9, 23
- Protected outdoor area 17
- Protection class 155
- Proximity reader 11
- PSTN 34
- Quick start guide 6
- Quick start guide 7
- Range 155
- Relay outputs 19
- Remote access 16
- Remote configuration 16
- Sabotage 19
- Safety 7
- Safety 156
- Security frequency band 19
- Secvest
 - Arming/disarming 7
 - Mounting location 10
- Seismic sensor 19
- Shock detector 16
- Signal transmission 155
- Silent alarm 20
- Sirens 157
- Smoke alarm device 19
- SMS service centre 163
- Sounder 15, 19
- Speech dialler 20
- Status 20
- Status display 37
- Status feedback 20
- Status query 20
- Submenus 29
- Symbols 8
- Tamper protection 19
- Tampering 19, 20
- Technical damage 20
- Telephone dialler 10, 20
- Terms and definitions 15
- Time zones 162
- Transmission power 155
- User 15
 - Installer 26, 30
 - Logging in/out 7
- User guidance 15
- Users 156
- UTC 163
- Voice messages 157
- Warning
 - Caution 8
 - Important 8
 - Note 8
- Wired alarm zone 16
- Wired detector 16
- Wired detectors 16
- Wired zone 16
- Wireless alarm system 16
- Wireless alarm zone 16, 17
- Wireless control device 17
- Wireless control devices 156
- Wireless detector 17
- Wireless key switch 17
- Wireless mobile phone network 163
- Wireless operation 10
 - R&TTE certification 10
 - wireless licence 10
- Wireless range 17
- Wireless remote control 17
- Wireless window lock 17
- Wireless zone 17
- Zone 21

ABUS wireless alarm system

Secvest

Manufacturer
ABUS Security-Center GmbH & Co. KG
Linker Kreuthweg 5
86444 Affing, Germany