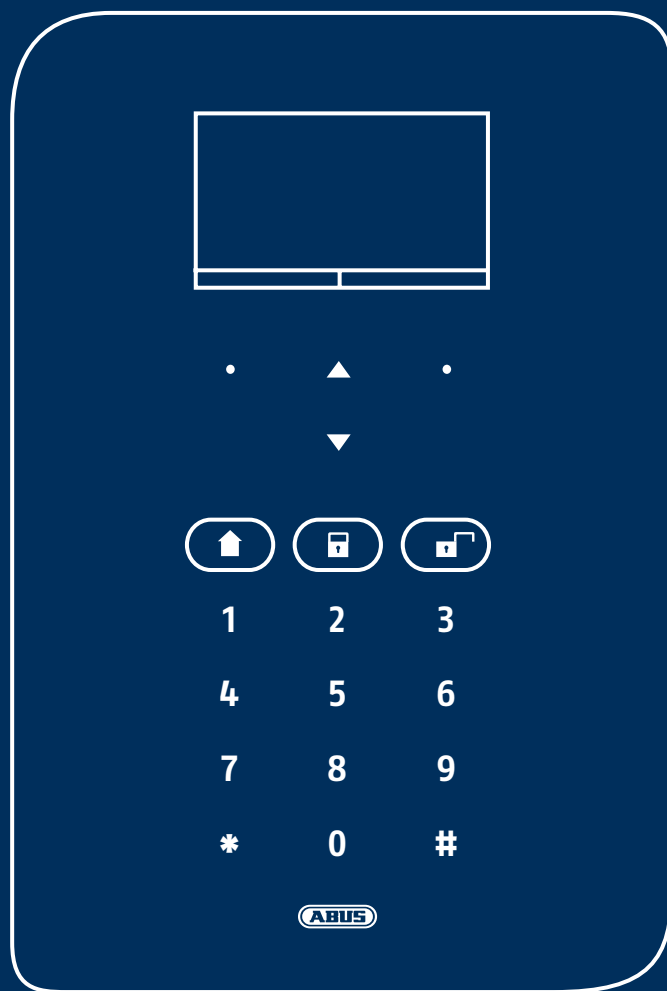
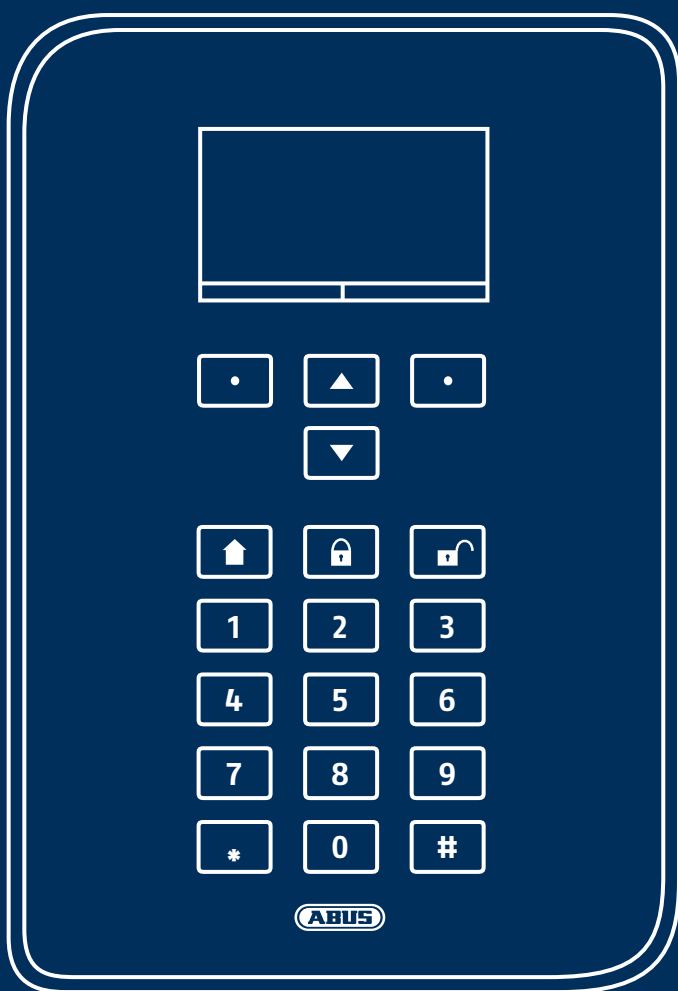


# SECVEST

## 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

This 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 .

## Italiano

Queste istruzioni contengono avvertenze importanti per la messa in funzione e l'utilizzo. La preghiamo pertanto di conservare le presenti istruzioni per eventuali consultazioni future. Le presenti istruzioni sono parte integrante del prodotto, pertanto vanno osservate anche in caso di cessione del prodotto a terzi.

## Limitation of liability

Everything possible has been done to ensure that the content of these instructions is correct. However, neither the author nor ABUS Security-Center GmbH & Co. KG can be held liable for loss or damage caused by incorrect or improper installation and operation or failure to observe the safety instructions and warnings. No liability can be accepted for consequential damage. No part of the product may be changed or modified in any way. If you do not follow these instructions, your warranty claim will be invalid. The content of all external links within the text is not the responsibility of ABUS Security-Center GmbH & Co. KG, but is instead managed by the respective providers. ABUS Security-Center GmbH & Co. KG carefully checked the linked external websites at the time of publication and no potential legal infringements were identified at the time the link was established. We have no influence on subsequent changes. Liability of ABUS Security-Center GmbH & Co. KG is therefore excluded.

Subject to technical modifications.

© ABUS Security-Center GmbH & Co. KG, 01/2020



### Note

#### S/W 3.01.17

This manual relates to software version 3.01.17 and all other previously published software versions. All new features that are only valid from a certain software version are marked accordingly, e.g.  $\geq 2.00.00$ . All other features that are valid up to a certain software version are also marked accordingly, e.g.  $< 2.00.00$ .

## Declaration of conformity

ABUS Security-Center hereby declares that the radio equipment type FUAA50xxx is in compliance with RED Directive 2014/53/EU. The full EU Declaration of Conformity text can be found at:

[www.abus.com](http://www.abus.com) Item search FUAA50xxxx/Downloads.

The Declaration of Conformity can also be obtained from the following address:

ABUS Security-Center GmbH & Co. KG

Linker Kreuthweg 5

86444 Affing

GERMANY

## Warranty



### Note

- ABUS products are designed and manufactured with the greatest care and tested according to the applicable regulations.
- The warranty only covers defects caused by material or manufacturing errors at the time of sale. If there are demonstrable material or manufacturing errors, the alarm panel will be repaired or replaced at the warrantor's discretion.
- In such cases, the warranty ends when the original warranty period of two years expires. All further claims are expressly rejected.
- ABUS will not be held liable for defects and damage caused by external influences (e.g. transport, use of force, operating errors), inappropriate use, normal wear and tear, or failure to observe the instructions in this manual.
- In the event of a warranty claim, the original receipt with the date of purchase and a short written description of the problem must be supplied with the product.
- Should you discover a defect on your alarm panel that was already present at the time of purchase, please contact your dealer directly within the first two years.

<b>Contents</b>	
<b>Limitation of liability</b> .....	<b>2</b>
<b>Declaration of conformity</b> .....	<b>3</b>
<b>Warranty</b> .....	<b>3</b>
<b>Contents</b> .....	<b>4</b>
<b>Quickstart guide</b> .....	<b>8</b>
Target audience .....	8
Installing Secvest .....	8
Configuring Secvest.....	8
Secvest function test.....	8
<b>Safety information</b> .....	<b>9</b>
Explanation of symbols .....	9
Intended use .....	9
General .....	10
Power supply .....	11
Battery warning notes .....	13
Connections .....	15
Wireless operation .....	15
Mounting location of the alarm panel.....	15
Processing priority .....	16
Packaging .....	16
<b>Scope of delivery</b> .....	<b>16</b>
<b>Device overview</b> .....	<b>17</b>
Device front .....	17
International key assignment .....	18
Device rear (mounting plate).....	19
<b>Introduction</b> .....	<b>21</b>
Terms and definitions.....	21
Alarm panel error and tamper monitoring .....	36
Time conditions .....	36
<b>Mounting/Installation</b> .....	<b>37</b>
Connection overview, terminal block .....	37
Fixing the mounting plate to the wall .....	39
Positioning the wireless alarm system (alarm panel) .....	39
Fixing the mounting plate.....	39
Connecting the components .....	40
Installing an optional wireless mobile module .....	40
Installing the micro SD card.....	41
Final steps .....	41
Changing the upper part of the housing, touch front, keypad front .....	41
<b>Commissioning</b> .....	<b>42</b>
Initial commissioning/factory reset.....	42
For a system that is already installed .....	43
Logging into the wireless alarm system .....	43
Logging out from the wireless alarm system .....	44
<b>Configuration</b> .....	<b>45</b>
Notes.....	45
Menu control elements.....	46
Login screen .....	47

Main menu .....	48
INFO .....	50
Alarm panel .....	50
Communication.....	55
PSTN.....	56
Ethernet.....	57
Mobile.....	58
Hybrid module .....	60
Customisation .....	61
Status.....	62
Components .....	63
Teach-in via web interface.....	63
Detectors .....	67
IP zones .....	67
Wireless Zones .....	79
Wired Zones.....	81
HyMo zones .....	82
Wireless control panel .....	85
Add wireless control panel .....	85
External Sirens .....	87
Wireless sirens.....	87
Wired Sirens .....	88
Indoor sounder .....	89
Info module/indoor siren .....	92
WUM (Wireless Universal Module) .....	94
Door locks.....	96
RF repeater .....	98
Hybrid module .....	102
Outputs .....	106
Radio Outputs.....	107
Configuring radio outputs.....	107
Wired Outputs.....	115
Configuring wired outputs .....	116
HyMo outputs .....	117
Configuring HyMo wired outputs.....	118
Combination outputs.....	120
Partitions .....	122
Configure partitions.....	123
Complete arming .....	123
Configure partitions.....	132
Part Set.....	132
Configure partitions.....	141
Deactivated.....	141
Configure partitions.....	145
Panic response:.....	145
System .....	147
General .....	148
Installer details.....	157
User access.....	159
User Reset.....	163
Confirmation .....	164
Hardware .....	167
Security settings .....	170
Panel upgrade .....	187
Checking for an upgrade? .....	190
Backup/restore .....	191

# Contents

---

Report .....	194
Communication .....	196
Network .....	196
Network Setup .....	197
IP Mobile Setup .....	200
Email Setup .....	206
VoIP Dialler Setup .....	208
ARC reporting .....	210
ARC Reporting, Phone Book .....	213
ARC Reporting, Account Numbers .....	215
ARC Reporting, Fast Fmt Channels (for "Fast Format" protocol only) .....	216
ARC Reporting, CID/SIA Triggers (for all protocols EXCEPT "Fast Format") .....	217
Encryption .....	219
ARC Reporting, More .....	225
Emergency call .....	229
Social Care, Phone Book .....	231
Social Care, Account Numbers .....	232
Voice dialler .....	233
Speech Dialler, Triggers .....	236
Speech Dialler, Destinations .....	237
Speech Dialler, Test Call .....	238
SMS .....	240
SMS, Triggers .....	242
SMS, Destinations .....	244
SMS, Destinations, Message X .....	245
SMS, Destinations, Forward .....	246
SMS, Destinations, Message, Telephone Recipients .....	247
SMS, Messages .....	248
SMS, PSTN SMS .....	249
SMS, test call .....	251
Email .....	253
Email, Triggers .....	255
Email, Destinations .....	257
Email, Messages .....	258
Email, test call .....	259
Communication options .....	261
Contacts .....	266
Emergency call .....	272
Test .....	273
Log .....	294
Virtual keypad .....	297
<b>Appendix .....</b>	<b>298</b>
Technical data .....	298
Compatible equipment .....	312
HW default values/factory defaults .....	320
SW default values/factory defaults .....	321
Installer Mode .....	321
User menu .....	337
Start Wizard .....	341
Acoustic signal tones .....	342
Repairs and maintenance .....	344
Maintenance by the installer .....	344
Maintenance by the user .....	344
S/W upgrade .....	345
Software file set for V3.01.17 .....	347
Software upgrade with new files from the SD card .....	348

---

Software upgrade with new files on the PC.....	349
Software upgrade with new files from the FTP server .....	357
S/W upgrade with the Secvest update utility .....	359
ARC/ESCC reporting .....	360
ARC/ESCC reporting protocol formats.....	360
CID/SIA Events.....	364
Email error messages.....	376
TCP/IP error messages .....	377
Overview of the SSL-relevant messages .....	377
VoIP error messages .....	379
GSM CME / CMS Error messages .....	380
CME Error codes .....	380
CMS Error codes .....	382
Log .....	384
Log book entries .....	384
User numbers .....	397
Troubleshooting .....	399
Manual restart (switching off and switching back on).....	399
Carry out a GSM/wireless mobile manual test call, prepaid.....	402
Diagnostic LEDs on the motherboard and GSM/wireless mobile module .....	403
Trace, recording communication sequences.....	405
Router, IAD, Firewall .....	408
Time zones .....	409
Landline notification centre .....	410
GSM network notification centre.....	411
SMS notification.....	411
Email notification/email setup .....	412
IP Mobile Setup / Mobile Data Communication .....	415
Customer service and support.....	416
Decommissioning the alarm panel .....	417
Data protection .....	417
Disposal .....	418
<b>Index.....</b>	<b>419</b>

## Quickstart 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 the chapter Mounting/Installation.

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](http://www.abus.com/ger/products/FUAA50000)

### Configuring Secvest

The configuration of the wireless alarm system is described there.

### 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
- Operating the Secvest and remote control.
- Create a handover log



#### Note

Please observe the general notes for user training.

Provide the user with the user manual and the quick start guide and, where applicable, these installation instructions.



**Safety information**

**Explanation of symbols**

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

Symbol	Signal word	Meaning
	<b>Danger</b>	Indicates a risk of injury or health hazards.
	<b>Danger</b>	Indicates a risk of injury or health hazards caused by electrical voltage.
	<b>Important</b>	Indicates possible damage to the device/accessories.
	<b>Note</b>	Indicates important information.
		The EU Directive WEEE 2012/19/EU governs the proper recovery, treatment and recycling of used electronic devices. This symbol means that, in the interest of environmental protection, the device must be disposed of separately from household or industrial waste at the end of its lifespan, in accordance with applicable local legal guidelines. Used devices can be disposed of at official recycling centres in your country. Obey local regulations when disposing of materials. Further details on returns (also for non-EU countries) can be obtained from your local authority. Separate collection and recycling conserve natural resources and ensure that all the provisions for protecting health and the environment are observed when recycling the product.

Only use the device for the purpose for which it was built and designed. 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.

This product complies with current domestic and European regulations.

Conformity has been certified, and all related certifications are available from the manufacturer on request.

To ensure this condition is maintained and that safe operation is guaranteed, it is your obligation to observe this manual. If you have any questions, please contact your specialist dealer. Further general information and information on product support can be found at [www.abus.com](http://www.abus.com) on the general page or for dealers and installers, in the Partner portal.

 **Danger**  
Set the alarm panel to installer mode before starting any installation or maintenance work. Installer mode prevents alarms from being activated when the cover of the control panel or of another component is opened.

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**

### 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.



#### Danger

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.



#### Danger

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.

Store the instructions in a safe place for future reference.

If you sell or pass on the device to third parties, you must include these instructions with the device.

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



#### Note

#### S/W >=1.01.02

During the initial set-up of the alarm control panel there is **neither a predefined standard installer code nor a predefined standard administrator code**. These need to be individually assigned in the set-up wizard.

After the initial start-up, please change the **default installer name (code = name)** as well as the **default administrator name (code = name)** to secure user names. When adding users, please make sure you are careful about how log-in details are handled.

#### Handling log-in details for your security systems

### Basics:

- User names and codes for logging into security systems should be known only by the legal owners and never given out to unauthorised parties.
- If you have to pass this information on via email, please take care to send the user name and code in two separate emails.
- User names and codes should be changed regularly.

### Standards

- User names must be at least eight characters long.
- They should ideally contain characters from at least three of the following categories: uppercase letters, lowercase letters, special characters, and numbers.
- User names should never contain your own name, the name of a family member, your pet, your best friend or your favourite celebrity, or your hobby or date of birth.
- Avoid using user names and codes that you use on other websites or that could be easily guessed by others.
- Your user name should not be able to be found in a dictionary and should never be a product name.
- It should not be a conventional series of characters, a repeated pattern or a keyboard pattern, such as asdfgh or 1234abcd.
- You should avoid only using numbers at the end of your user name or using one of the more typical special characters (! ? #) at the beginning or end to compensate for an otherwise simple user name.
- User names and codes should be changed at least every 180 days.
- New user names and codes should not be identical to any of the three combinations used before them.
- New user names and codes should differ from user names and codes that have been used before by at least two characters.
- Macros and scripts should not be used to input user names and codes.



#### 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.

- 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.



#### Danger

Alterations or modifications to the device invalidate the guarantee.



#### Danger

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.



#### Note

Interference filter, noise filter, interference suppression filter

We recommend attaching a ferrite to the 230 V power supply line.

e.g. Ferrit Würth 742 711 32S or 742 715 3

This prevents any potential malfunction of the alarm panel should electromagnetic interferences occur that may be permissible in accordance with the EMC Directive, but which are nevertheless very strong.

## Power supply



### **Danger**

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.

**Battery warning notes**

**!!! Please read the following information very carefully!!!**

Strictly observe the following! ABUS Security-Center GmbH & Co. KG is not liable for accidents caused by handling outside of these safety precautions. Please read the user guide and handling safety instructions carefully before using the battery.

Incorrect handling of rechargeable lithium ion cells may result in leakage, high temperature, smoke, explosion or fire, and capacity may be reduced.



**Caution  
portant**



**Caution**



**Im-**

It is strictly prohibited to:

- heat the battery or throw it into a fire.
- throw the battery into liquids such as water, petrol or drinks and make it wet.
- drop the battery
- use rechargeable batteries near a fire or in a car where the temperature may exceed 60°C. The battery should also not be charged or discharged under such conditions.
- place the batteries together with metal objects, such as necklaces, hairpins, coins or screws, in pockets or bags

Do not store or transport the batteries with such objects.

- short circuit the (+) and (-) connections with other metals.
- pierce batteries with a sharp object such as a needle.
- disassemble or modify the battery
- weld or solder directly onto the battery
- place the battery in a microwave oven, dryer or high pressure container.
- use rechargeable batteries together with dry batteries or other primary batteries
- use new and old batteries together, use batteries from different batches, or use batteries of a different type or make
- reverse the polarity

Keep batteries out of the reach of children so that they are not accidentally swallowed.

Where younger children may be using the battery, their parent or guardian should explain how to use it properly.

Only charge the battery with a special charger in accordance with the product specification. Only charge the battery using the CC/CV method.

Finish charging the battery if charging is not completed within the specified time.

Stop using the cell if abnormal heat, odour, discolouration, deformation or abnormal condition is detected during use, charging or storage.

Do not place the battery in a device with (+) and (-) the wrong way round

If the battery is connected incorrectly, the battery will not charge. At the same time, the charge-discharge properties and the safety characteristics will be reduced. This can lead to product heating and leakage.

Do not use a battery with significant buckling or deformation.

Keep the battery away from fire immediately should leakage or an unpleasant odour be detected.

Should liquid get on your skin or clothing, wash it off immediately with fresh water.

If liquid leaking from the battery gets into your eyes, do not rub them. Wash thoroughly with clean cooking oil and seek medical attention immediately.

Batteries have life cycles. If the time for which the battery operates devices becomes much shorter than usual, the lifespan of the battery is at an end. Replace the battery with a new one of the same type. Replace the battery with another battery of the same type.

If the battery will not be used for an extended period of time, remove it from the device and store it in a location with low humidity and low temperature.

While the battery is being charged, used, or stored, keep it away from objects or materials with static charge.

If the battery terminals are dirty, wipe them with a dry cloth before using the battery.

Store the cells in the storage temperature range according to the specifications. After complete discharge, we recommend charging to 7.4 to 8.0 V without using it for a longer period of time.

Do **not** exceed the following temperature ranges:

	from	to
Charging temperature range	0 °C	45 °C

## Safety information

---

Discharging temperature range	-20 °C	60 °C
Storage for less than one month	-20 °C	60 °C
Storage for less than three months	-20 °C	45 °C
Storage for less than one year	-20 °C	25 °C

Keep the battery in a 50% state of charge during prolonged storage.

We recommend recharging the battery every 3 months after receipt of the battery up to 50% of the total capacity and keeping the voltage between 7.4 and 8.0 V. Store the battery in a cool, dry place.

## Connections



### Note

This device uses Safety Extra Low Voltage (SELV). The circuits of the zones, the circuits of the switch outputs and the 12 V power supply of the ABUS alarm control panels also operate in this voltage range.

SELV is a low electrical current that offers special protection against electric shocks based on its low level and insulation compared to higher voltage circuits.

The PSTN module contains a mix of connections related to alarm systems, along with telecommunications connections. The typical alarm system connections are designed for Safety Extra Low Voltage (SELV). The telecommunication connections are designed for the voltages of the telecommunications network (Telecommunications Network Voltage, TNV).



### Important

It is extremely important that the two types of connections are kept separate. Always use a separate cable. Connect the respective connections with appropriate external connections (such as alarm system connections) or with appropriate telephone connections. TNV circuits should only be connected by a qualified person in accordance with local regulations.

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 convenient height (between 1.5 and 2 m).

## 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).

The wireless devices in this system have been tested by an independently accredited laboratory for RED Directive 2014/53/EU or 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.

## Scope of delivery

---



### 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 the 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).

## Processing priority



### Note

If several detectors are activated at the same time, the alarm control panel always processes panic zones (panic transmitters) and normal alarms (burglar alarms) first, followed by fire zones (smoke alarm devices) and then followed by all other zone types (alarm types)

The alarm control panel always processes alarms ahead of warnings (fault messages).

## Packaging



### Danger

Keep packaging material and small parts away from children.

There is a risk of suffocation!

Remove all packaging material before using the device.

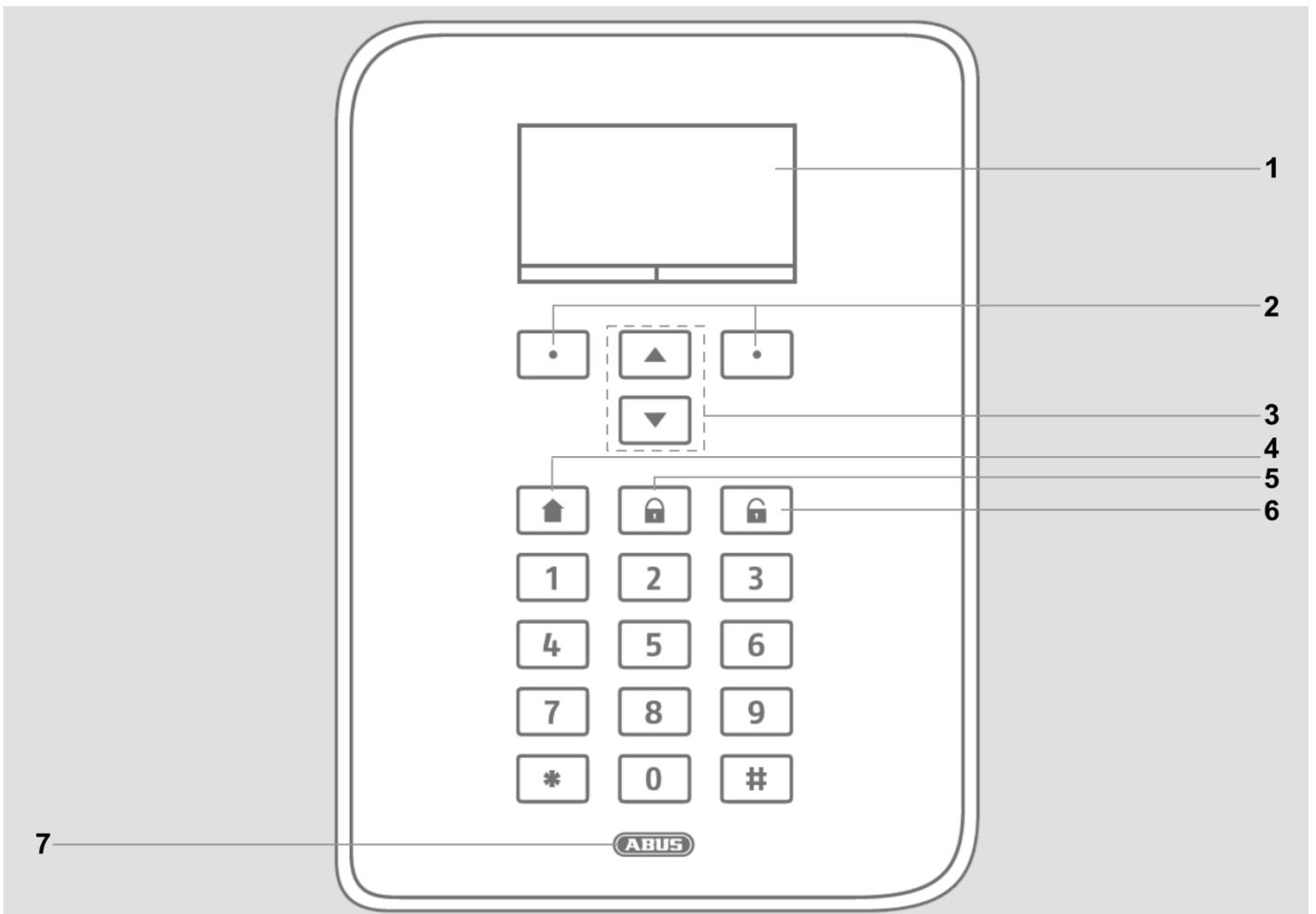
## Scope of delivery

- 1x Secvest wireless alarm panel
- 1x battery
- Quick guide and safety instructions
- Installation material



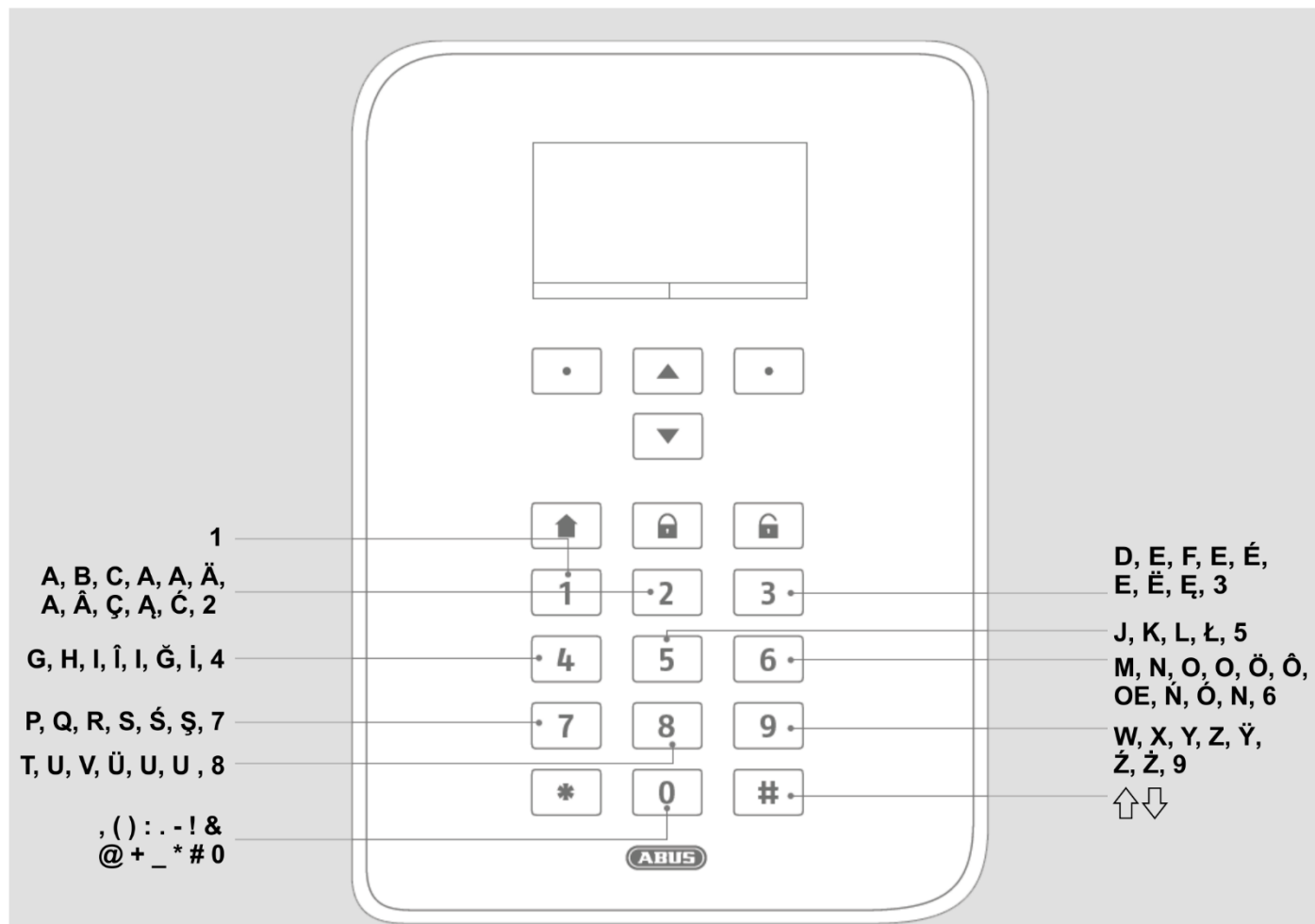
Device overview

Device front

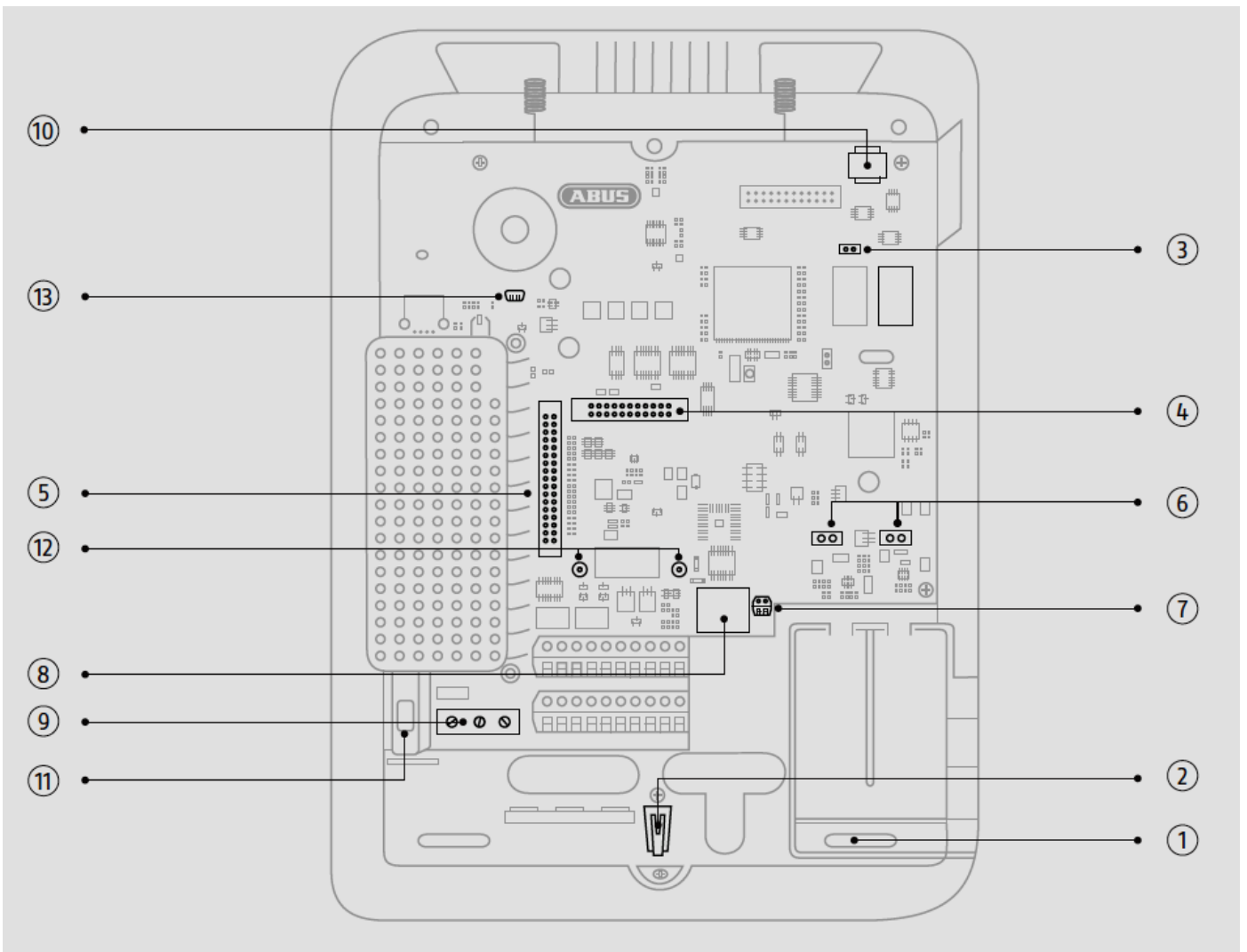


No.	Name/function	No.	Name/function
1	<b>Status display</b> Display of status and menus	5	<b>Arming button</b> Monitoring of all available areas is activated (device armed).
2	<b>Confirmation buttons</b> Used to navigate to a higher/lower menu level or to select options or to exit a menu	6	<b>Disarm button</b> Monitoring is deactivated (device disarmed).
3	<b>Navigation buttons</b> Used to navigate up/down	7	<b>Proximity reader</b> Reader for the proximity keyfob. Hold the keyfob in front of the ABUS logo.
4	<b>Internal arm button</b> 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, see note below	10	Micro SD card holder
4	Connection for optional mobile wireless module	11	Fuse holder for mains fuse
5	Connection for ribbon cable	12	Holes for plastic holder for optional mobile wireless module
6	Connections for battery pack	13	USB mini-B
7	Analogue telephone connection		



**Note**

**Code reset PINs**

If user 1 and/or installer codes are no longer known, all user settings can be deleted.

All users, all proximity tags, all remote controls and all emergency buttons will be deleted. After the reset you will be prompted to enter a new installer code and a new administrator code.

1. If possible, go to installation mode.

Note:

## Device overview

---

If you cannot go into installation mode, the alarm panel will sound a tampering alarm when you open the housing.

2. Open the housing. Disconnect the entire power supply (mains voltage and batteries).

Note:

This procedure will not work if the tamper switch on the cover is closed.

3. Identify the reset code PIN on the motherboard (see illustration above).
4. Shortly close both of the reset code PINs. Use a screwdriver or jumper to do so. Leave the short circuit until step 6.
5. Reconnect the mains voltage. After a short pause, the system will start. The alarm panel will now delete all user information and will start with the reallocation of your new installer code and administrator code (like in the start wizard).
6. Remove the short circuit on the reset code PINs.
7. Reconnect the battery.
8. Close the alarm panel cover and therefore also the tamper switch.

---

**Introduction****Terms and definitions****2G**

Mobile wireless second generation standard, see GSM

**3G**

Mobile wireless third generation standard, see UMTS

**4G**

Mobile wireless fourth generation standard, see LTE

**AES**

Alarm receiving centre, for details see EN 50518-1/2/3, EN 50136 and VdS 2471, see also ESCC

**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.

**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.

**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.

**Sounder**

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

**Alarm sensor**

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

**Alarm panel**

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

**Alarm zone**

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

**APN**

Access Point Name

also "access point", is the name of the gateway between a backbone of a mobile wireless network (e.g. GPRS, 3G or 4G) and an external packet-based data network, usually the public internet.

### **ATS**

Alarm transmission system

### **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.

### **Outdoor 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 detectors**

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

### **Bidirectional 2-way wireless (2WAY)**

Unidirectional: arm components (e.g. simple 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.

**CC/CV battery charging method**

The IU charging method, also known as CCCV for constant current constant voltage, combines the constant current charging method with the constant voltage charging method. In the first phase of charging, a constant current that is limited by the charger is used for charging. Compared to the standard constant voltage charging method, this limits the otherwise high initial charging current. When the battery's selected cut-off voltage is reached, the system switches from current to voltage regulation and continues charging at a constant voltage during the second charging phase, with the charging current automatically decreasing as the level of the battery's charge increases. As a criteria for terminating the charge, it is possible to define a minimum charge current for lithium-ion batteries.

**Chip key/proximity keyfob**

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/ESCC.

**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, wired detectors**

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).

### **GDPR**

General Data Protection Regulation

### **DTMF**

Dual Tone Multi-Frequency

Dual tone multi-frequency

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

Is used with monitoring station protocols FF, CID, Scancom and Scanfast.

### **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 standards series for alarm systems, "Intrusion and hold up systems"

### **Shock detector**

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

### **Ethernet/LAN**

Ethernet is a technology for local data networks (LAN), that specifies software (protocols etc.) and hardware (cable, distributor, network cards etc.) for wired data networks.

### **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.



**Fast Format, FF**

Protocol for transmitting data to an ARC/ESCC. DTMF-based

**Remote access/remote configuration**

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

**FSK**

Frequency Shift Keying, is used with SIA monitoring station protocol.

**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 panel**

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 switches**

For convenient arming/disarming of the alarm panel without entering a code (using a key).

**Wireless range**

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

**Glass breakage detectors**

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

**GMT**

**Greenwich Mean Time** is the mean solar time on the prime meridian. The expression Greenwich Mean Time (GMT) is still used today to refer to "Western European Time" (WET, UTC+0). The designation "GMT", sometimes used in time stamps in internet protocols, always refers to UTC. The majority of electronic devices with time and date also continue to use the term GMT. When setting the correct time zone for the user location, the input/selection is often made by entering the number of hours by which the local time is ahead of (+) or behind (-) the standard time (GMT or UTC).

Example, Germany:

Winter time: UTC/GMT +1

Summer time: UTC/GMT +2

**GPRS**

General Packet Radio Service, **shortened to GPRS, is the term used to refer to the packet-based services for transferring data in GSM networks.**

**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).

Strictly speaking this is the technologies of the second generation.

However, it is also used as a generic term for all the generations, 2G=GSM, 3G=UMTS, 4G=LTE.

**GSM CME CMS Error Codes**

CME Error codes

GSM Equipment related codes

CMS Error codes

GSM Network related codes

**GUI**

Graphical use interface, the display on the alarm panel used to program and operate the alarm panel via menu keys

### **H/M**

Hybrid Module, HyMo, wireless additional module for the Secvest with wired zones and wired outputs.

### **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.

### **HyMo**

Hybrid Module, H/M, wireless additional module for the Secvest with wired zones and wired outputs.

### **IAD**

An **Integrated Access Device** (or router) is a device used for the network connection of NGN ports by the participant.

### **ICMP**

The **Internet Control Message Protocol** is used in computer networks to exchange information and error messages via the Internet protocol.

#### **ICMP Ping.**

Ping sends an "Echo request" package (Ping) to the target address of the host to be checked. If the recipient supports the protocol, they must send a response according to the protocol specification: ICMP "Echo reply" (Pong). If the target computer is not accessible, the corresponding router will respond: "Network unreachable" or "Host unreachable".

### **IMEI**

International Mobile Station Equipment Identity (IMEI), a unique 15-digit serial number that can be used to uniquely identify each wireless mobile end device.

### **IMSI**

International Mobile Subscriber Identity (IMSI), used in 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 sounder**

Signal generator for indoor use, visual/acoustic sounder (in addition to outdoor sirens)

### **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.

### **IP mobile**

Synonym for 4G (LTE) and 2G (GPRS) IP-based transmission

### **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 sounder

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

### Communication options

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

### Components

See system components

### LAN / Ethernet

see Ethernet/LAN

### Receiving centre

See ARC

### Level 1-4

See access level 1-4

### 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).

### LTE

**Long Term Evolution (LTE for short, also 3.9G)** is the name given to the third generation wireless mobile standard. An extension is called *LTE-Advanced*, or 4G, it is backwards compatible with LTE in the Next Generation Mobile Networks (NGMN) project. For marketing reasons, LTE is already advertised as 4G and LTE-Advanced as 4G+, which, technically speaking, is not correct.

With up to 300 megabits per second, depending on the reception status, significantly higher download speeds are possible than with older standards.

For this, LTE wireless mobile providers exclusively use the UHF frequency band (also known as the decimetre waveband) for their frequency range. Within this, several frequencies are used, varying regionally in the central to upper UHF range from approx. 700 to 2600 Megahertz.

The basic schema of the Universal Mobile Telecommunications Systems (UMTS, 3G) is retained for LTE (3.9G). This allows for quick, cost-efficient retrofitting of the UMTS technology infrastructures, e.g. to LTE-Advanced (4G).

**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.

**Mobile**

Synonym for the following transmissions in the wireless mobile network:

- Voice calls with a telephone number, e.g. +49 173 1234567
- ARC reporting classic DTMF or FSK based, such as FF, CID, SIA, Scancom, Scanfast, Tunstall
- SMS transmission

**N/A**

Only enabled, a user or zone type that can be used only to activate the system.

**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).

**NTP**

Network Time Protocol

The Network Time Protocol (NTP) is a standard for synchronizing clocks in computer systems via packet-based communication networks. NTP uses the UDP connection free transport protocol, which was specially developed to facilitate reliable time setting across networks with variable packet run times.

Generally, references to NTP refer to both the protocol and its software reference implementation. The SNTP (Simple Network Time Protocol) represents a simpler form of the NTP.

### **O/C**

Open Circuit

### **Opening detector**

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.

### **Programming**

Detailed settings for the alarm panel according to the user's requirements (e.g. zones/partitions 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.)

**Rolling Code (RC)**

Rolling code is a technology which provides optimum protection against code scanning and code grabbing in order to prevent unauthorised access.

**Router**

See IAD

**RSSI**

The **Received Signal Strength Indicator** is an indicator of the signal strength of wireless communication applications.

**S/C**

Short Circuit

**Tampering, tampering protection, sabotage**

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).

**Arming, disarming**

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).

**SD card, micro SD card**

Micro SD storage card for saving:

- Application software in the INSTALL folder

- Language files in the INSTALL folder

- Images from the TVIP41550 in the IMG\_X folder

- Configuration of the alarm panel when backing up via the GUI in the CONFIG folder

- Traces in the TRACE folder

A circular buffer function is integrated for images, etc.

The alarm panel checks whether the storage is full or not every minute.

If the SD card is full, the oldest recordings will be automatically deleted. However, you will still receive the error message "SD card full". In order to confirm this error message, data must be manually deleted from the SD card.



**Danger**  
**Data protection**

Follow the SD card instructions in the "De-commissioning the alarm panel" chapter.

### 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.

### SELV

Safety Extra Low Voltage.

### Server

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

### SHA

SHA-2 (secure hash algorithm) is the general term for the four cryptological hash functions, SHA-224, **SHA-256**, SHA-384 and SHA-512, which were standardised in 2001 by the American NIST as a successor to SHA-1.

### SIA

Protocol for transmitting data to an ARC/ESCC.

### SIA-IP (DC-09)

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

### SG

Sounder, sound generator, siren

### 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").

### SNTP

Simple Network Time Protocol

The Network Time Protocol (NTP) is a standard for synchronizing clocks in computer systems via packet-based communication networks. NTP uses the UDP connection free transport protocol, which was specially developed to facilitate reliable time setting across networks with variable packet run times.

Generally, references to NTP refer to both the protocol and its software reference implementation. The SNTP (Simple Network Time Protocol) represents a simpler form of the NTP.

### Voice 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 (arming device, 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 a monitoring station 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.

### **Sabotage**

See "Tampering"

### **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 partitions (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.

### **TNV**

Telecommunications Network Voltage

### **Tunstall**

A social care alarm protocol

### **Overlapping signal**

See jamming.

### **TE**

Transmission equipment according to EN 50136

### **UCP**

Universal Computer Protocol

### **UMTS**

The **Universal Mobile Telecommunications System (UMTS)** is a wireless mobile standard of the third generation (3G), with significantly higher data transfer speeds possible (up to 42 Mbit/s with HSPA+, otherwise max. 384 kbit/s) than with the wireless mobile standard of the second generation (2G), the **GSM** standard (up to 220 kbit/s with EDGE, otherwise max. 55 kbit/s with GPRS).

### **UTC**

**Universal Time Coordinated** is the currently applicable world reference time (also known as GMT).

### **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)

**WAN**

A wide area network is a computer network which, in contrast to a LAN, stretches over a very wide geographical area. It is a popular science synonym for Internet.

**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.

**WBI**

Web interface, means access to the web server of the alarm panel via a web browser

**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.

**Access level 1–4**

Access level 1-4, also known as level 1-4, In accordance with  
EN50131-1 Section 8.3.1  
EN50131-3 Section 8.3.1  
EN50136-2 Section 5.2  
EN50136-3 Section 6.2

Access level 1

Access for all

Access level 2

User access, e.g. via a controller

Access level 3

User access, e.g. via personnel from a security company

Access level 4

User access, e.g. via the device manufacturer

**Note:**

In the event of changing operating software, access level 4 is applied, without activating a tampering device on the alarm control panel or the additional operating device.

**Force Set**

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

## Alarm panel error and tamper monitoring

The alarm panel continually monitors error and tamper states. The following is monitored:

- Tamper contact:  
The alarm panel's tamper contact is continually monitored.
- Supervision  
The alarm panel continually monitors supervision messages from the components to the alarm panel.
- Signal jamming:  
The alarm panel monitors attempts to jam the wireless signal and monitors attempts to jam the wireless signal of selected components. If jamming is detected there, the message "Signal jamming" is sent to the alarm panel.
- Zone connections
- Communication connections
- Supply voltage:  
The alarm panel monitors the supply voltage under load conditions and registers faults.
- Load on the voltage outputs.

## Time conditions

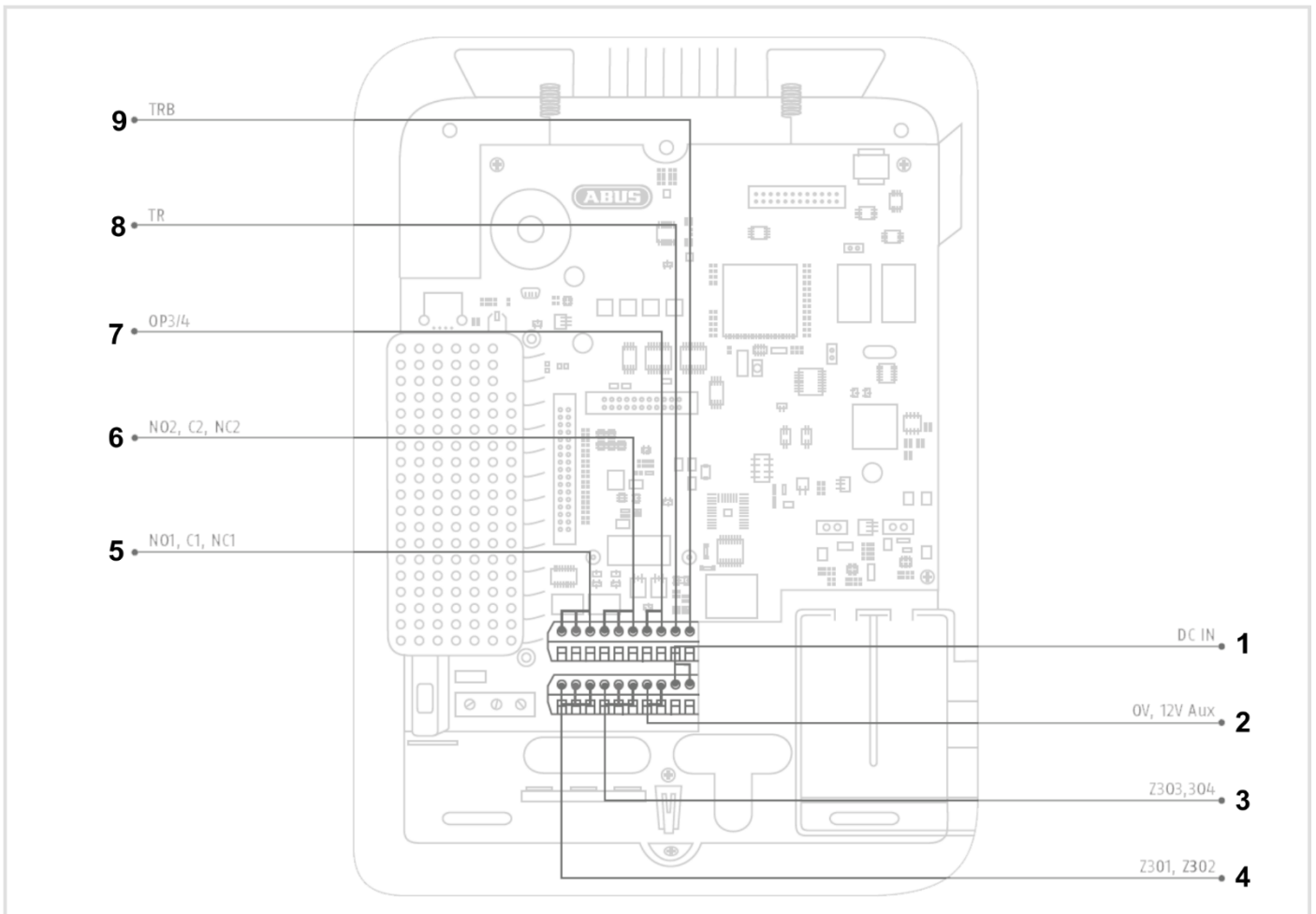
The alarm panel was designed so that changes to the zone statuses are detected if they last at least 400 ms (EN50131-1 Chapter 8.9.1 and EN50131-3 Chapter 8.9 and Annex B).




Breaking and entering, intrusion and tampering signals must last at least 400 ms.

The alarm panel was designed so that changes to the fault status (fault signals) are detected if they last at least 10 s (EN50131-1 Chapter 8.9.1 and EN50131-3 Chapter 8.9 and Annex B).

Mounting/Installation


Connection overview, terminal block



No.	Name/function	No.	Name/function
1	<b>DC IN 13.8 V +:</b> Connection for voltage supply 13.8 V	6	<b>N02, C2, NC2 – relay output 2:</b> potential-free relay contact, 30 V DC, 24 V AC rms, 500 mA
2	<b>0 V, 12 V aux:</b> voltage output 13.8 V  <b>Note</b> This output is <b>not</b> buffered by the battery in case of power failure. The output voltage during a power failure is directly 0 V.	7	<b>OP3/4 – transistor outputs:</b> for a wired siren, strobe and audio alarm signalling device Open drain transistor output 500 mA 13.8 V DC  <b>Note</b> These outputs will drop to 0 V during power failures.
3	<b>Z303, Z304:</b> Wired zones 303 and 304	8	<b>TR – tamper return:</b> Tamper input for the tamper output of a wired sounder  <b>Note</b> In the default settings, a jumper is connected to 0 V. This means there is no fault indication (tamper) if no wired sounder is connected.

## Mounting/Installation

---

<b>4</b>	<b>Z301, Z302:</b> wired zones 301 and 302	<b>9</b>	<b>TRB – trouble:</b> Fault indication input for the fault output of a wired sounder  <b>Note</b> In the default settings, a jumper is connected to 0 V. This means there is no fault indication (fault) if no wired sounder is connected.
<b>5</b>	<b>NO1, C1, NC1 – relay output 1:</b> 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 convenient 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



**Danger**

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.



**Note**

We recommend attaching a ferrite to the 230 V power supply line.

e.g. Ferrit Würth 742 711 32S or 742 715 3

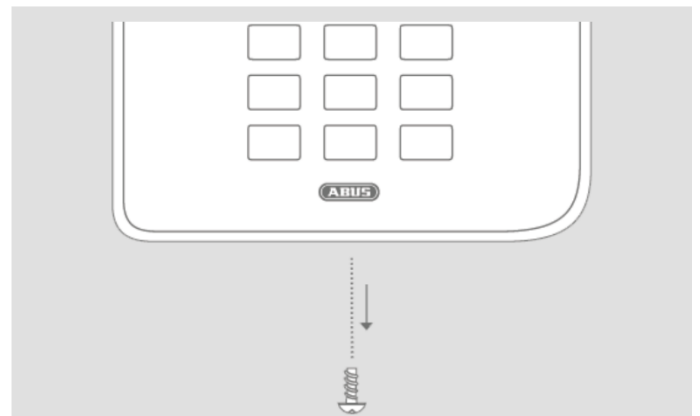
This prevents any potential malfunction of the alarm panel should electromagnetic interferences occur that may be permissible in accordance with the EMC Directive, but which are nevertheless very strong.



**Danger**

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.

### Important note:

Place cables in such a way that none are crushed.



### Important note:

In the default settings, a jumper is connected between the TR (tamper return) connection and 0 V as well as the TRB (trouble) connection and 0 V. This means there is no fault indication (tamper/fault) if no wired sounder is connected.

## 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 costs incurred by potential dispatches of rescue services, such as the fire service or police, must be borne by the operator of the system. 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.



### Important note:

**Please note that bare wire ends must not come into contact with conducting surfaces or contacts on the PCBs.**

**Therefore, insulate all unused stripped wire ends as required.**

## Installing an optional wireless mobile module

If available:

Plug the wireless mobile module 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 respective wireless mobile module.)



### Important note:

When connecting components with a separate external power supply, equipotential bonding connections must be used for all earthing, 0-volt or minus terminals. This provides defined signal levels on the connecting wires between the components.



### Important note:

In a security system, tamper monitoring is also important and/or necessary for the wiring between the components.





### 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.



The control panel software automatically detects what type of upper part the housing has: touch front or key front.

When switching on, the software checks which front is installed.

That means that the user interface and several functions change in order to support either the Secvest touch front or the Secvest keypad front.

If the software identifies a touch front, it will change to the Secvest touch operation. Otherwise, the software supports Secvest key operation.

**Note:**

**For details, see the user guide section 10.5.1 “Functions”**

3. Connect the connecting cable connector of the battery (or batteries) into the connector (BATT1 CON 8, BATT2 CON 9) on the PCB.



**Once the battery is connected, the system will start.**

Turn on the main power supply.

Either plug the external power supply unit into the socket or turn on the circuit that provides the Secvest with 230V.

**Tip:**

By removing and reinserting the 230V main fuse within the Secvest, you can initiate an on/off of the 230V power supply.

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.

### Changing the upper part of the housing, touch front, keypad front



**Proceed in the following order:**

- **Upgrade** the alarm panel software to the newest version (Secvest touch support, S/W  $\geq$  2.01.08).
- **Disconnect** the alarm panel completely from the power supply, battery (or batteries) and external power supply.
- **Exchange** the front.
- **Connect** the alarm panel completely to the power supply, battery (or batteries) and external power supply once again.

Otherwise, failures in the touch sensitivity of the touch keys and the proximity functionality may occur.

## Commissioning

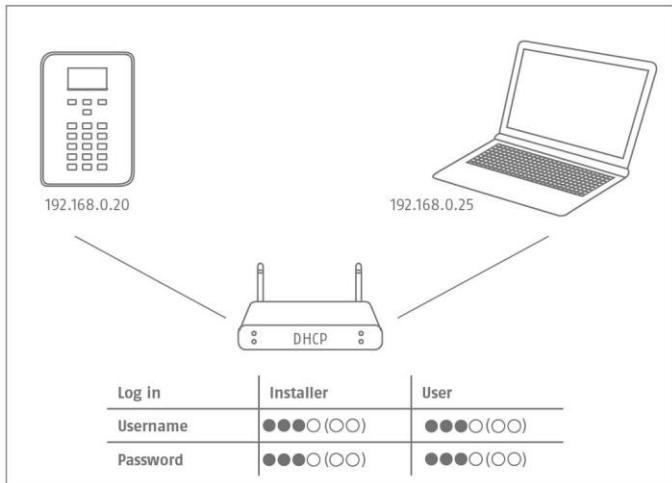
### Initial commissioning/factory reset



#### 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:
  - your desired menu language
  - the desired software version for the alarm panel
  - your country, for country-specific settings
  - the current date
  - the current time
  - whether switching between daylight savings/standard time is to be carried out manually or automatically.
  - A/C error message for 230 V power supply. You will then receive error messages in the event of such faults.
  - External D/C power supply error message for 13.8 V DC power supply. You will then receive error messages in the event of such faults.
  - Battery 2 if it will also be used.
  - the type of wired zone (e.g. 2-wire FSL 2k2/4k7).
  - whether access via the web server is/is not permitted. Set to "permitted" as standard
  - whether the system should obtain the IP address automatically or if you wish to enter the IP address manually
    - Automatic DHCP on

- Manual DHCP off, the following menus appear where you can enter the address:
  - IP address
  - IP Subnet mask
  - Gateway IP address
  - Initial IP address of the DNS server
- Internal HTTP port

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

Make a note of the IP address.

- ARC/ESCC reporting, whether reports are to be sent to monitoring station
- the length of the access code, 4 or 6 characters
- the installer code (S/W >=1.01.00)
- the administrator code (S/W >=1.01.02)

5. The overview then displays:

- the temporary login data for the installer and administrator.

6. The following message will be displayed "Please check whether new software is available."

The verification will take place in Installer Mode.

You can also check this in the Level4 user menu, and then immediately perform a software upgrade.

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](http://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.

## Commissioning

A window appears with the following message:  
SSL certificate will be created, this can take several minutes.  
Network functions are not available during this time.



### Note

This message will display: Network initialisation, please wait...

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 as an installer.

### 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.

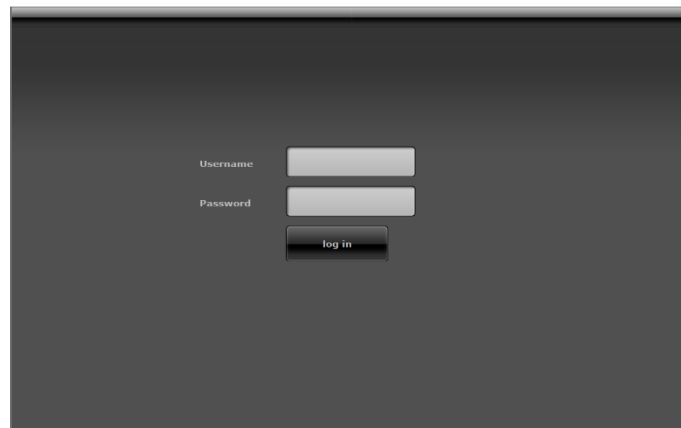


### Note

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.

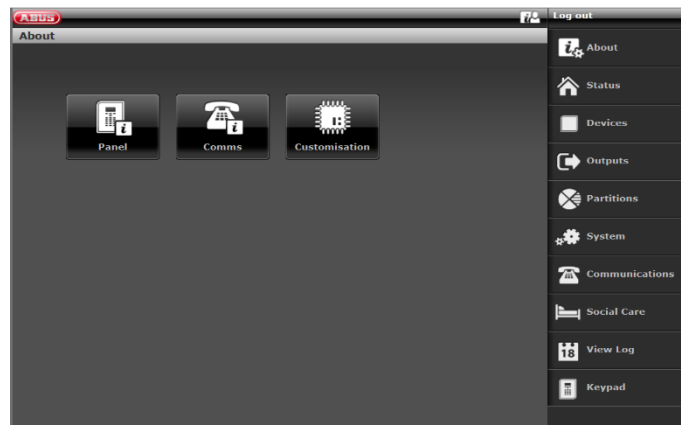


4. Log in as an **Installer** with the user name and the installer password.

### Note for S/W <1.01.00

The default installer password is 9999(99)

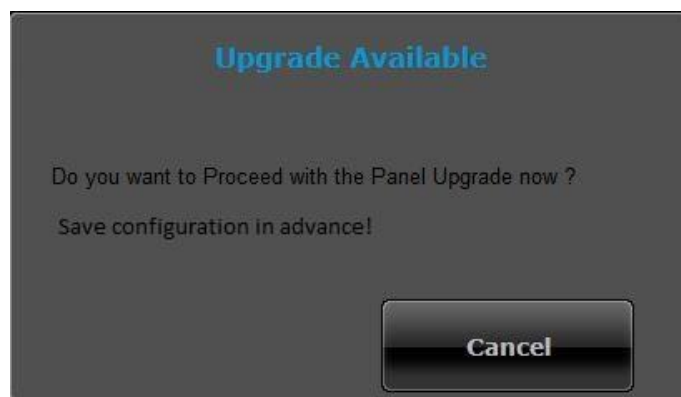
5. Click on the **Login** button or press the **enter key** on the keyboard.
6. The main menu appears:



S/W >=3.00.03

After logging in, the software automatically asks the ABUS FTP server: "Is new software available?"

If the FTP server replies to this question with a "Yes", the following pop-up menu appears.



Click the **Cancel** button.

## Commissioning

---

You will find further details in the "Software upgrade" chapter in the appendix.



### Note

A software upgrade via the web server may only be performed by a Level4 type user.

## Logging out from the wireless alarm system

Click the **Log out** button.

If you are working directly in the alarm control panel, click the **"Exit"** menu key.



### Important!

#### Saving the settings:

S/W <2.00.00

When you make these changes in the Installer Mode, the Secvest stores these changes in temporary storage until you leave the Installer Mode.

When you leave the Installer Mode, the alarm control panel writes these changes to permanent storage.

If you power off the alarm control panel completely **BEFORE** leaving the Installer Mode, the alarm control panel will lose all your changes.

Please note that this does not apply if you restore the factory defaults; this change is implemented immediately.

S/W >=2.00.00

When you make these changes in the installer mode, they will be saved directly in the Secvest's permanent storage following confirmation.

They will be preserved, even in the event of power failure before you exit installer mode.



### Important!

#### Automatic log out function:

Based on the Secvest's automatic log out function, this is now also possible on the web interface and Secvest app.

- Installer or level 4 user is logged into the web interface. The automatic log out occurs after **1 hour** of inactivity.
- iOS/Android app: Once opened, the app closes after 4:15 minutes have passed without an input in accordance with the VdS 3169 standard,
  - providing "Remember PIN" is set to no.

- Normal user or administrator is logged in. The automatic log out occurs after **1 minute** of inactivity.



### Important!

#### Time schedules active/inactive, week planner

Please inquire with the alarm panel user about a possible programmed time schedule in the user menu.

If the alarm panel is in installer mode, planned events are moved. They are NOT annulled.

Pending events are carried out when installer mode is finished.

This means that after leaving installer mode, the alarm panel switches to the state desired and programmed by the user for this time period.

## Configuration

### Notes

Please consult the user guide for details on activating and deactivating the system, and on the behaviour of the alarm control panel and the display (user interface).

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.

S/W < 2.00.00

(Wireless) components are set up/taught in directly on the wireless alarm panel.

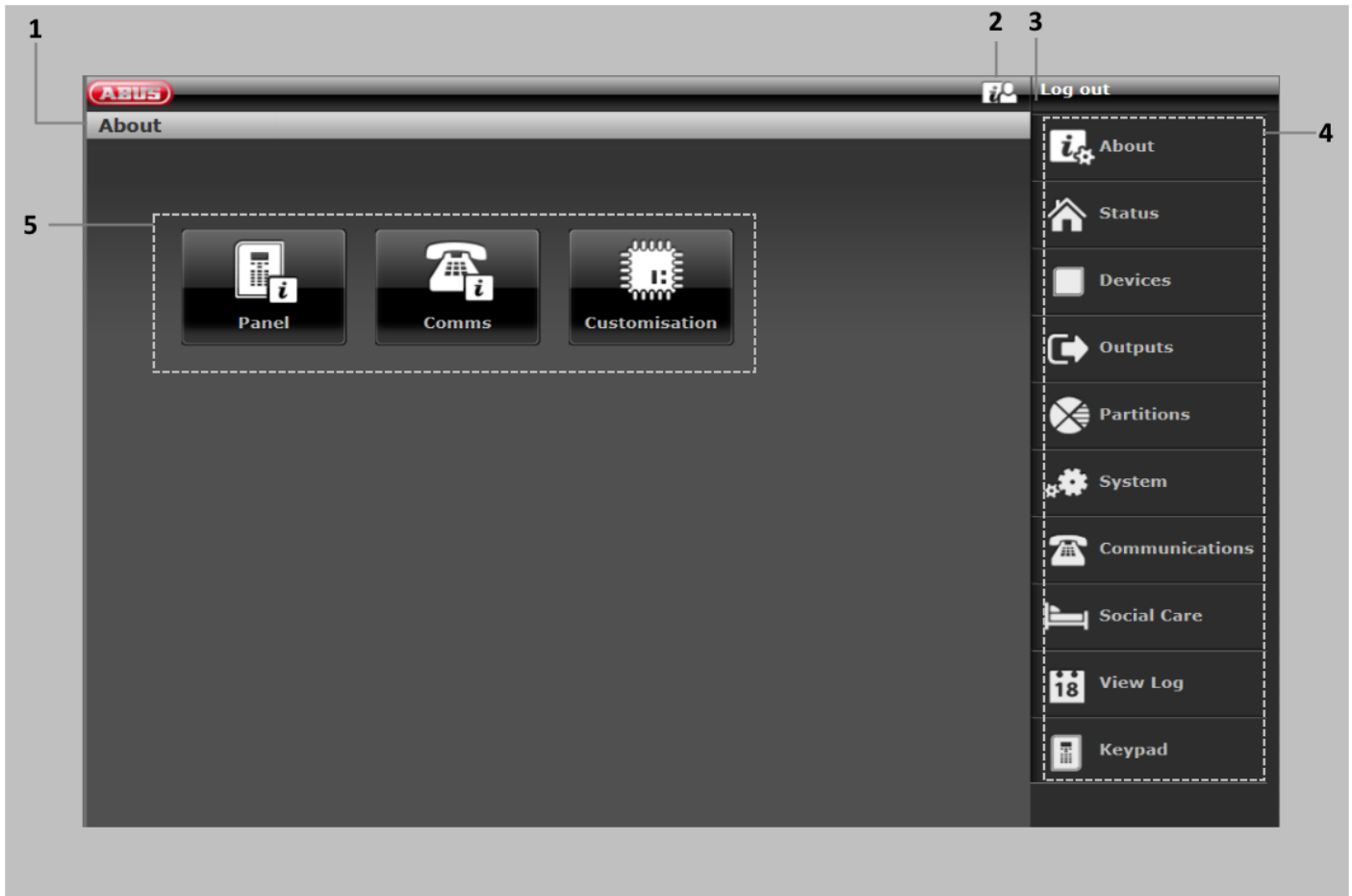
S/W >= 2.00.00

(Wireless) components can be set up/taught in directly on the wireless alarm panel or via the web server.

Please also see the "Standard values/factory defaults" in the appendix.

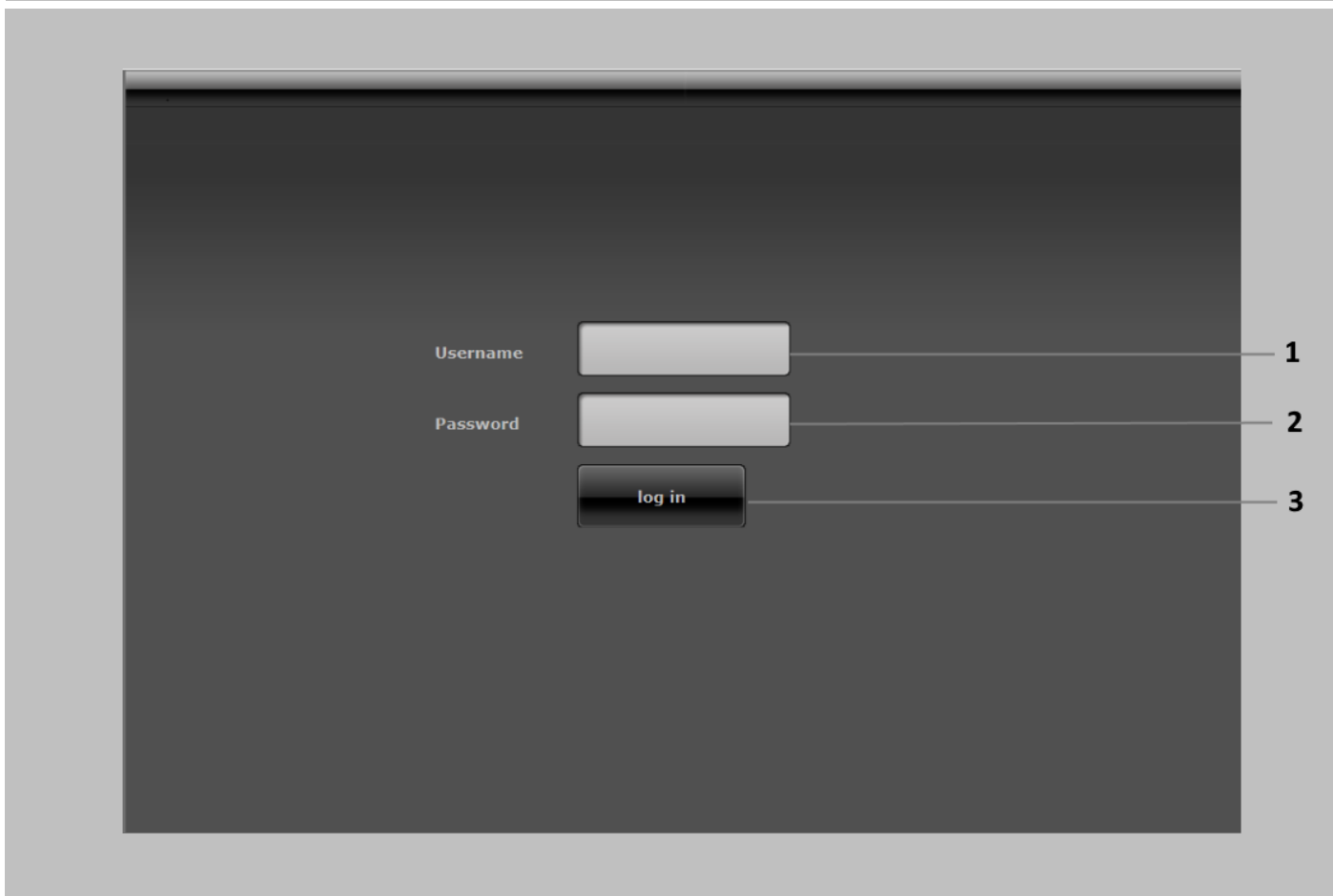
This section provides reference information about the options that are available in Installer Mode.

## Menu control elements




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

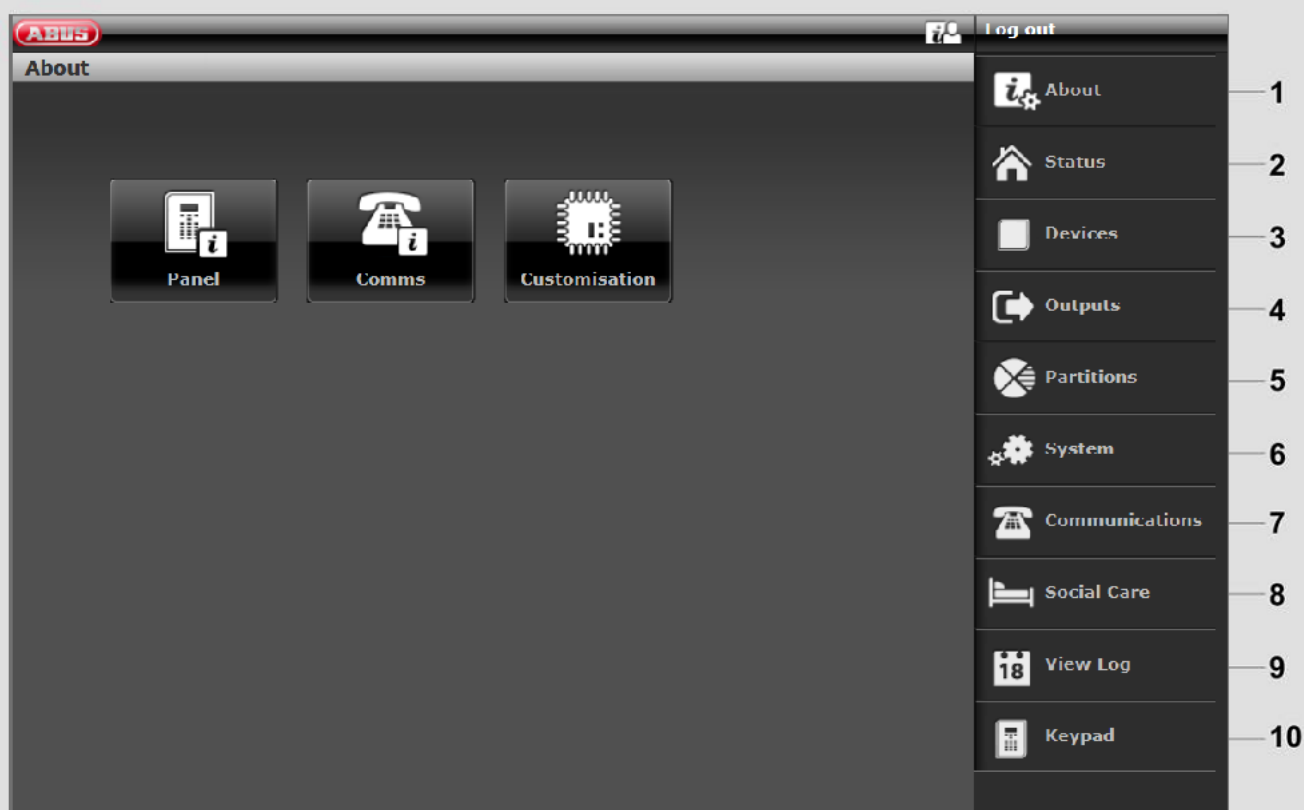
Login screen



No.	Name/function	No.	Name/function
1	<b>Input field for the user name</b> <ul style="list-style-type: none"> <li>• Enter the Installer names.</li> <li>• The entry is case-sensitive.</li> </ul>	3	<b>Login button</b>
2	<b>Input field for the password</b> <ul style="list-style-type: none"> <li>• Enter the Installer password.</li> <li>• <b>Note for S/W &lt;1.01.00</b> The default installer password is 9999(99).</li> <li>• The entry is case-sensitive.</li> </ul>		

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

## Main menu



No.	Name/function	Page	No.	Name/function	Page
1	<b>INFO</b> General information about: <ul style="list-style-type: none"> <li>the alarm panel (software and hardware version)</li> <li>communications</li> <li>the hybrid module</li> <li>customisation</li> </ul>	50	4	<b>Outputs</b> Overview/configuration of the outputs: <ul style="list-style-type: none"> <li>Wireless outputs</li> <li>Wired outputs</li> <li>HyMo outputs</li> <li>Combination outputs</li> </ul>	106
2	<b>Status</b> Information about the status of the alarm system partitions	62	5	<b>Partitions</b> Overview/configuration of the partitions	122
3	<b>Components</b> Overview/configuration of the components: <ul style="list-style-type: none"> <li>IP zones</li> <li>Wireless Zones</li> <li>Wired Zones</li> <li>HyMo zones</li> <li>Wireless control panel</li> <li>External sirens, wireless sirens, wired sirens</li> <li>Info module/indoor siren</li> <li>WAM</li> <li>Door locks</li> <li>RF repeater</li> <li>Hybrid module</li> <li>Indoor sounder</li> </ul>	63	6	<b>System</b> Overview/configuration of the alarm system: <ul style="list-style-type: none"> <li>General</li> <li>Installer details</li> <li>User access</li> <li>User reset</li> <li>Confirmation</li> <li>Hardware</li> <li>Safety settings</li> <li>Backup/restore</li> <li>Alarm panel upgrade S/W &lt;1.01.00</li> <li>Report</li> </ul>	147



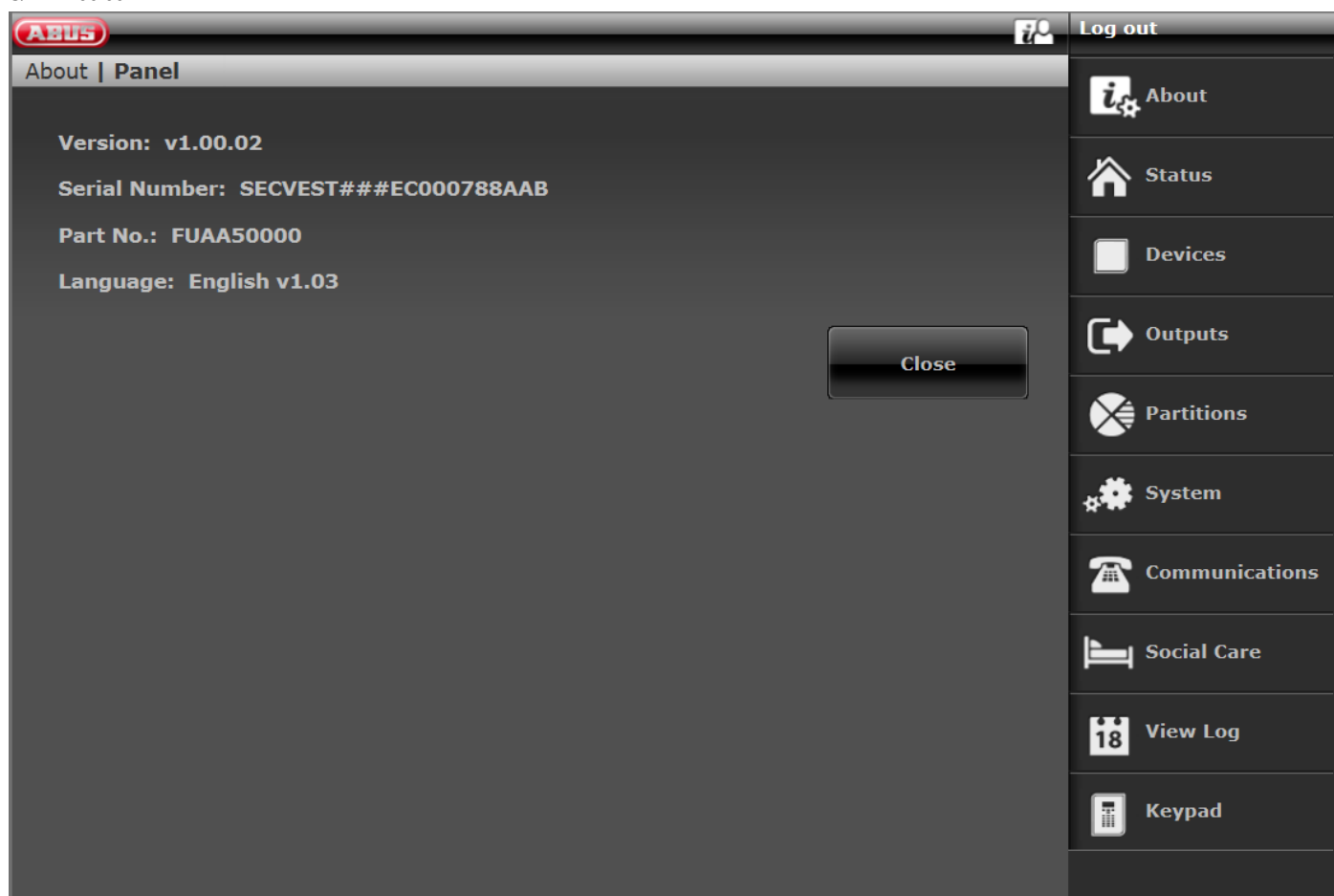
No.	Name/function	Page	No.	Name/function	Page
<b>7</b>	<b>Communication</b> Overview/configuration of the communication interfaces and transmission methods <ul style="list-style-type: none"> <li>• Network</li> <li>• ARC reporting</li> <li>• Emergency call</li> <li>• Voice dialler</li> <li>• SMS</li> <li>• Email</li> <li>• Communication options</li> <li>• Contacts</li> </ul>	196	<b>9</b>	<b>Log</b> Overview of faults, events and processes on all components of the alarm system	294
<b>8</b>	<b>Emergency call</b> Overview/configuration of the nursing emergency call	229	<b>10</b>	<b>Virtual keypad</b> 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.	
<b>X</b>	<b>Test</b> Overview/Implementation of all possible test functions				

## INFO



## Alarm panel

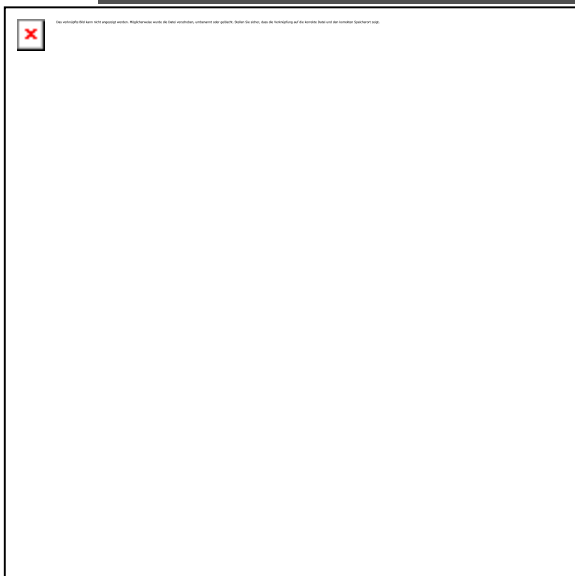
S/W <2.00.00



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	Version number for the configured language

S/W >= 2.01.08

The screenshot shows the ABUS configuration interface. At the top left is the ABUS logo. The main area displays system information: Version: v3.00.05, Language: English v1.25, Serial Number: SECVEST###GC028819AAB, Part No.: FUAAS0000, RF Device Exclusivity: No, Panel time: 19:16, Date: 26/02/2018, Zones: Available: 58, Used: IP: 0, Radio: 4, Wired: 0, Radio Sirens: 0, Indoor Sounders: 1, RF Repeaters: 0, Control Devices: 0, WAMs: 0, Door Locks: 0, Partitions: 2, Outputs: Available: 36, Used: Radio: 0, Wired: 1, Panel lid open: No, Bell Tamper: No, RF Jamming: No, Panel A/C Fail: Yes, External DC Fail: No, Ext. DC Voltage In: 14.3V, Battery 1 State: 8.2V, Battery 2 State: Disabled, Auxiliary: 14.1V. A 'Close' button is at the bottom right. On the right is a sidebar menu with options: About, Status, Devices, Outputs, Partitions, System, Communications, Social Care, Test, View Log, and Keypad. A 'Log out' button is at the top right of the sidebar.



Name/function	Explanation
<b>Version, language</b>	Version number of the software currently installed on the alarm system Version number for the configured language
<b>Serial Number</b>	Serial number of the alarm system
<b>Part No.:</b>	Article number of the alarm system
<b>RF Device Exclusivity</b>	Yes only new wireless components that have been on the market since 2015 can be added, e.g. FUMK500XX No all wireless components can be added, e.g. detectors from existing installations such as FU8320.
<b>Alarm panel time, date</b>	Currently set time and date on the control panel

## Configuration

---

<b>Date &amp; time</b>	Synchronises date and time of the alarm panel with the date and time from the PC via mouse click
<b>Zones</b>	Overview of available and configured zones IP zones (IP), wireless zones (WIRELESS), wired zones of the alarm panel (WIRED), HyMo zones (H/M)
<b>Wireless sirens</b>	Number of components in use
<b>Indoor sounder</b>	Number of components in use
<b>RF repeater</b>	Number of components in use
<b>Wireless control panel</b>	Number of components in use
<b>WAM</b>	Number of components in use
<b>Door locks</b>	Number of components in use
<b>Hybrid module</b>	Number of components in use
<b>Partitions</b>	Number of partitions in use
<b>Outputs</b>	Overview of available and configured outputs Wireless outputs (WIRELESS), wired outputs of the alarm panel (WIRED), HyMo outputs (H/M)
<b>Housing Tamper</b>	Specifies whether the tamper contact on the front of the housing or the wall tamper contact has been triggered
<b>Sounder Tamper</b>	Specifies whether the tamper contact on the wired, connected siren has been triggered (TR input on the alarm panel)
<b>RF Jamming</b>	Specifies whether the alarm panel has detected RF jamming
<b>Alarm panel A/C fault</b>	Displays whether the alarm panel is connected to 230 V or if a fault is present
<b>External DC fault</b>	Displays whether the alarm panel is connected to 13.8 V external DC power supply or if a fault is present.
<b>Ext. DC In - U</b>	Specifies the voltage of the external DC power supply
<b>Battery status</b>	Status of each battery (with voltage if required)
<b>Auxiliary</b>	Output voltage to the power supply output terminal

S/W >=3.00.05

**ABUS**
Log out

About | Panel

Version: v3.00.05 Language: English v1.25

Serial Number: SECVEST###GC028819AAB Part No.: FUAAS0000

RF Device Exclusivity: No

Panel time: 19:16 Date: 26/02/2018 [Set Date & Time](#)

Zones: Available: 58 Used: IP: 0 Radio: 4 Wired: 0

Radio Sirens: 0 Indoor Sounders: 1 RF Repeaters: 0

Control Devices: 0 WAMs: 0 Door Locks: 0

Partitions: 2

Outputs: Available: 36 Used: Radio: 0 Wired: 1

Panel lid open: No Bell Tamper: No RF Jamming: No












Panel A/C Fail: Yes External DC Fail No

Ext. DC Voltage In: 14.3V

Battery 1 State: 8.2V Battery 2 State: Disabled

Auxiliary: 14.1V

Close

-  About
-  Status
-  Devices
-  Outputs
-  Partitions
-  System
-  Communications
-  Social Care
-  Test
-  View Log
-  Keypad

# Configuration












S/W >= 3.01.14

**ABUS** Abmelden

Info | Zentrale

Version: v3.01.14 Sprache: Deutsch v1.40  
Serien Nr.: SECVEST###GC028819AAB Part No.: FUA50000  
RF Device Exclusivity: Nein  
Uhrzeit Zentrale: 11:04 Datum: 23/04/2019 Datum & Uhrzeit  
Zonen: Verfügbar: 73 Verwendet: IP: 2 FUNK: 10 VERDRAHTET: 1 H/M: 13  
Funk Sirenen: 1 Innen-SG: 4 RF Repeater: 1  
Funk Bedienteil: 1 UVM: 0 Türschlösser: 1 Hybrid Module: 2  
Teilbereiche: 4  
Ausgänge: Verfügbar: 44 Verwendet: FUNK: 2 VERDRAHTET: 3 H/M: 8  
Gehäuse Sabo: Nein SG Sabo: Nein RF Jammung: Nein  
AC Störung Zentrale: Ja Externe DC Störung Nein  
Ext. DC In - U: 14.2V  
Akku 1 Status: 8.1V Akku 2 Status: 8.1V  
Auxiliar: 14.0V

Schließen

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

Communication

The screenshot displays the 'Communication' configuration page in the ABUS system. The main content area features three prominent buttons for 'PSTN', 'Ethernet', and 'Mobile'. The right sidebar provides navigation options, including 'Log out' and various system settings like 'About', 'Status', 'Devices', 'Outputs', 'Partitions', 'System', 'Communications', 'Social Care', 'Test', 'View Log', and 'Keypad'. The top navigation bar includes the 'About | Comms' breadcrumb and the 'Log out' button.

The screenshot shows a web interface for PSTN configuration. At the top left, there is a red 'ABUS' logo. Below it, a breadcrumb trail reads 'About | Comms | PSTN'. The main content area displays 'PSTN Link Status: Fail' with a 'Close' button. On the right, a vertical navigation menu includes 'Log out' and several menu items: 'About', 'Status', 'Devices', 'Outputs', 'Partitions', 'System', 'Communications', 'Social Care', 'View Log', and 'Keypad'.

Name/function	Explanation
<b>PSTN Link Status</b>	PSTN link status query. 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
<b>MAC address</b>	The hardware address of the network adapter for the Secvest is given here. A MAC address is globally unique.
<b>IP address</b>	If the Secvest is located on a network the IP address is shown here, e.g. 192.168.178.23. If (DHCP) 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.
<b>IP Subnet Mask</b>	The subnet mask is displayed here. In a private network this is normally 255.255.255.0.
<b>Gateway IP address</b>	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.
<b>DNS primary IP address</b>	This is the IP address of the Domain Name System (DNS).
<b>IP Link Status (GUI only)</b>	Ethernet status query. The Secvest checks the connected LAN cable and its own Ethernet connection. The message "OK" appears. If something is not connected, not enabled or is disrupted, the error message "Fault" appears.

## Mobile

**ABUS**
Log out

About | Comms | **SIERRA HL7692**

Network: Reg. Home

Subscriber Number: +4915161721569

Signal Strength: : SS: 3

IMEI: 355465070121286


IMSI: Please wait...

Version: Please wait...

Close

- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- Test
- View Log
- Keypad

Name/function	Explanation														
	<p><b>Note</b></p> <p>These menus only appear when a wireless mobile module with an active SIM card is installed in the alarm panel</p>														
<b>SIERRA HL7692</b>	Manufacturer and type of the fitted wireless mobile module														
<b>Network</b> <b>Signal strength</b>	<p>Displays whether and how the SIM card is connected within the wireless mobile network.</p> <p>Example: Reg. Home RSSI: 4 (G)</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr> <td style="width: 20%;">'Not Reg.'</td> <td>Not registered; the module is not looking for a wireless mobile network.</td> </tr> <tr> <td>'Reg. Home'</td> <td>Registered; home network ('Reg. Home' is replaced with the provider name as soon as this becomes available).</td> </tr> <tr> <td>'Searching...'</td> <td>Not registered; the module is looking for a wireless mobile network.</td> </tr> <tr> <td>"Reg. Denied"</td> <td>Registration denied</td> </tr> <tr> <td>"Reg. Unknown"</td> <td>Unknown</td> </tr> <tr> <td>'Reg. Roam'</td> <td>Registered; roaming network ('Reg. Roam') is replaced with '*' roaming provider name as soon as this becomes available).</td> </tr> <tr> <td>RSSI</td> <td>Indicates the strength of the wireless mobile reception, similar to the bar display in a smartphone. The numbers range from 0 (very low) to 9 (very high).</td> </tr> </tbody> </table>	'Not Reg.'	Not registered; the module is not looking for a wireless mobile network.	'Reg. Home'	Registered; home network ('Reg. Home' is replaced with the provider name as soon as this becomes available).	'Searching...'	Not registered; the module is looking for a wireless mobile network.	"Reg. Denied"	Registration denied	"Reg. Unknown"	Unknown	'Reg. Roam'	Registered; roaming network ('Reg. Roam') is replaced with '*' roaming provider name as soon as this becomes available).	RSSI	Indicates the strength of the wireless mobile reception, similar to the bar display in a smartphone. The numbers range from 0 (very low) to 9 (very high).
'Not Reg.'	Not registered; the module is not looking for a wireless mobile network.														
'Reg. Home'	Registered; home network ('Reg. Home' is replaced with the provider name as soon as this becomes available).														
'Searching...'	Not registered; the module is looking for a wireless mobile network.														
"Reg. Denied"	Registration denied														
"Reg. Unknown"	Unknown														
'Reg. Roam'	Registered; roaming network ('Reg. Roam') is replaced with '*' roaming provider name as soon as this becomes available).														
RSSI	Indicates the strength of the wireless mobile reception, similar to the bar display in a smartphone. The numbers range from 0 (very low) to 9 (very high).														

	<p>The value inside the brackets indicates the availability of the data connection.</p> <p>Availability of the data connection:</p> <table border="1"> <tr> <td>“Without”</td> <td>2G network only available, voice, no data possible</td> </tr> <tr> <td>(G)</td> <td>GPRS network available.</td> </tr> <tr> <td>(4G)</td> <td>LTE/4G network available.</td> </tr> </table>	“Without”	2G network only available, voice, no data possible	(G)	GPRS network available.	(4G)	LTE/4G network available.
“Without”	2G network only available, voice, no data possible						
(G)	GPRS network available.						
(4G)	LTE/4G network available.						
<b>IMEI</b>	International Mobile Station Equipment Identity (IMEI), a unique 15-digit serial number that can be used to uniquely identify each wireless mobile end device. This number is also given directly on the module.						
<b>Subscriber Number</b>	<p>Telephone number assigned to the SIM card.</p>  <p><b>Note</b> The SIM card telephone number is only displayed if your service provider has saved the telephone number on the card.</p>						
<b>IMSI</b>	International Mobile Subscriber Identity, used in wireless mobile networks to uniquely identify network subscribers.						
<b>IP Address (GUI only)</b>	IP address of the wireless mobile module. This IP address is dynamically assigned by the wireless mobile network (2G/GPRS, 4G/LTE).						
<b>Version</b>	The hard- and software versions of the wireless mobile module.						
<b>Reset (GUI only)</b>	Used to restart the wireless mobile module without powering down the alarm panel. The wireless mobile module begins connecting to the wireless mobile network again.						

## Hybrid module

Nummer	Name	Version
HyMo 1	"HyMo 1"	v1.03
HyMo 2	"HyMo 2"	v1.03

Name/function	Explanation
<b>Number</b>	The internal number of the hybrid module
<b>Name</b>	The unique programmed name of the hybrid module
<b>Version</b>	The software version of the respective hybrid module

**Customisation**
Log out

**ABUS**

About | **Customisation**

Please offer this code for panel customisation:

E002589AB9C75F43

Please enter code:

---

---

Submit

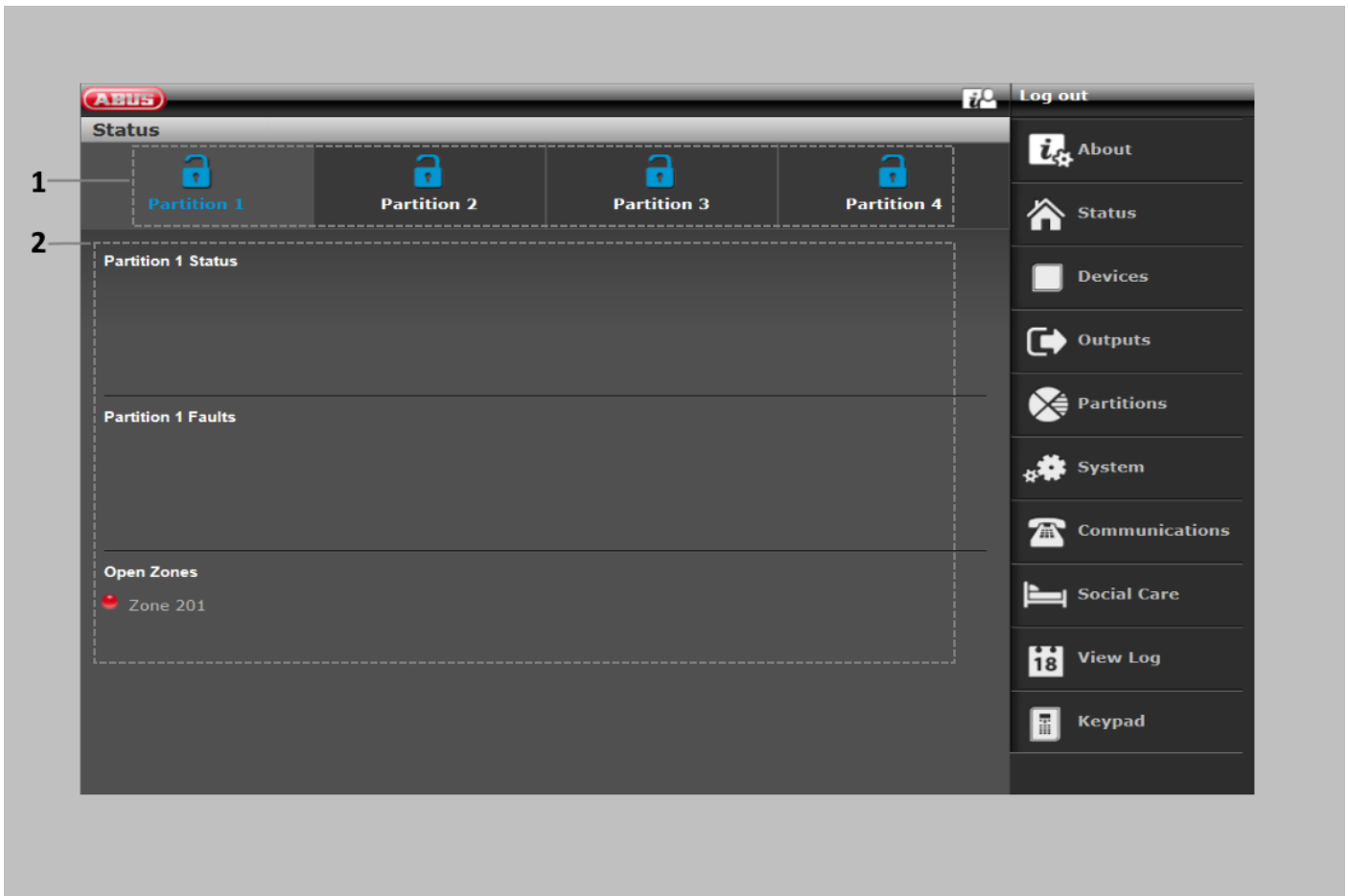
- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- View Log
- Keypad

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

**Note**  
 The possibility of individual customisation via this menu is currently only intended for special applications upon consultation with sales or support.

61

## Status



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

Only for the alarm control panel display

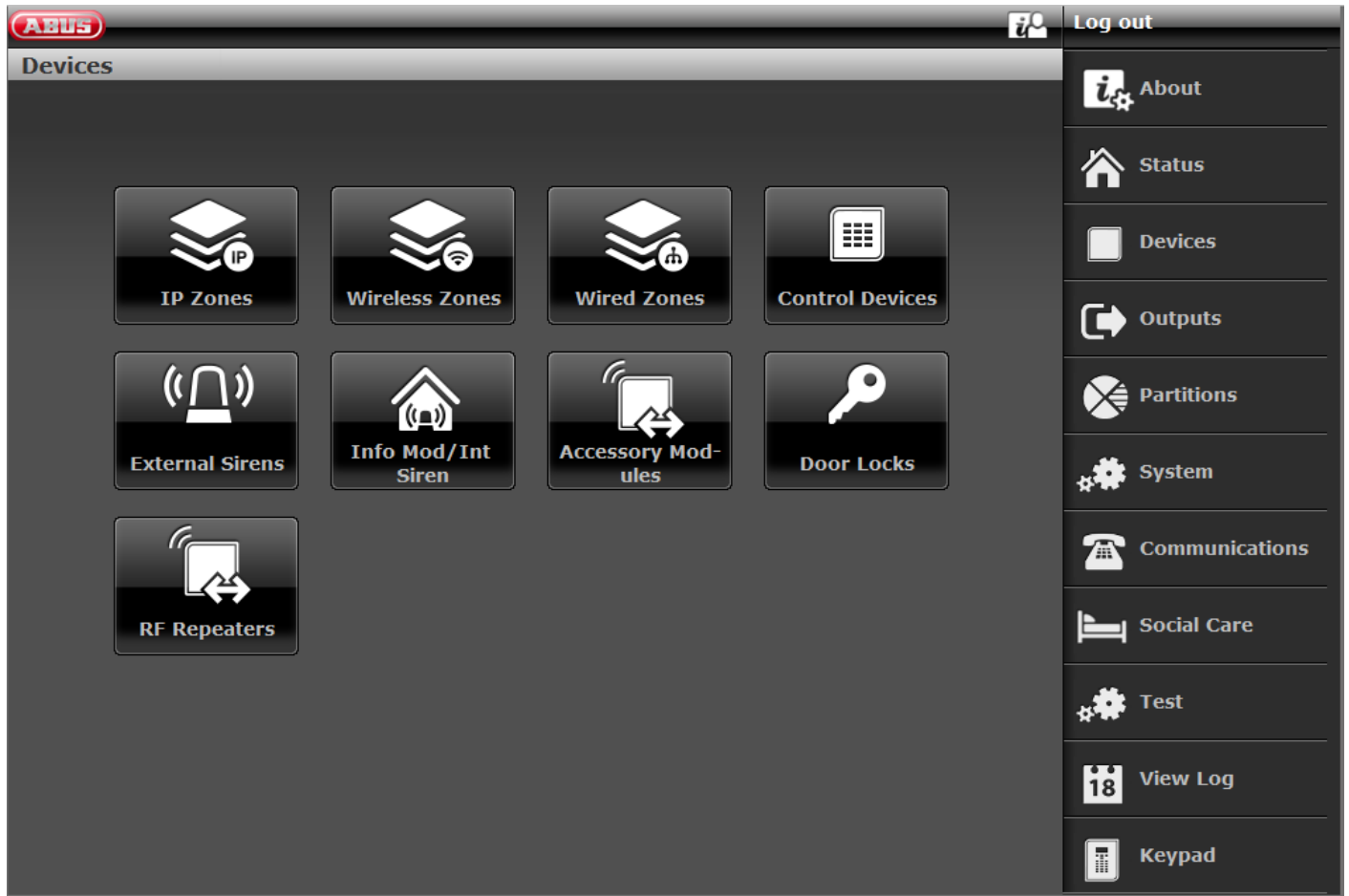


**Note:**

A "warning triangle" appears at the bottom of the display on the right-hand side if the alarm panel detects a problem. The explanation (description of the problem) is not shown unless an access level 2 (user) or access level 3 (installer) code is entered. After a valid code has been entered the message appears in plain text (problem, fault, warning, alarm etc.) The message is hidden again once the user has acknowledged or confirmed it. The notification disappears automatically after a one-minute time out.

## Components

### Teach-in via web interface




# Configuration


S/W >= 3.00.05

**ABUS** Log out


**Devices**




IP Zones




Wireless Zones




Wired Zones




Control Devices




External Sirens




Info Modules




Accessory Modules



Door Locks














RF Repeaters



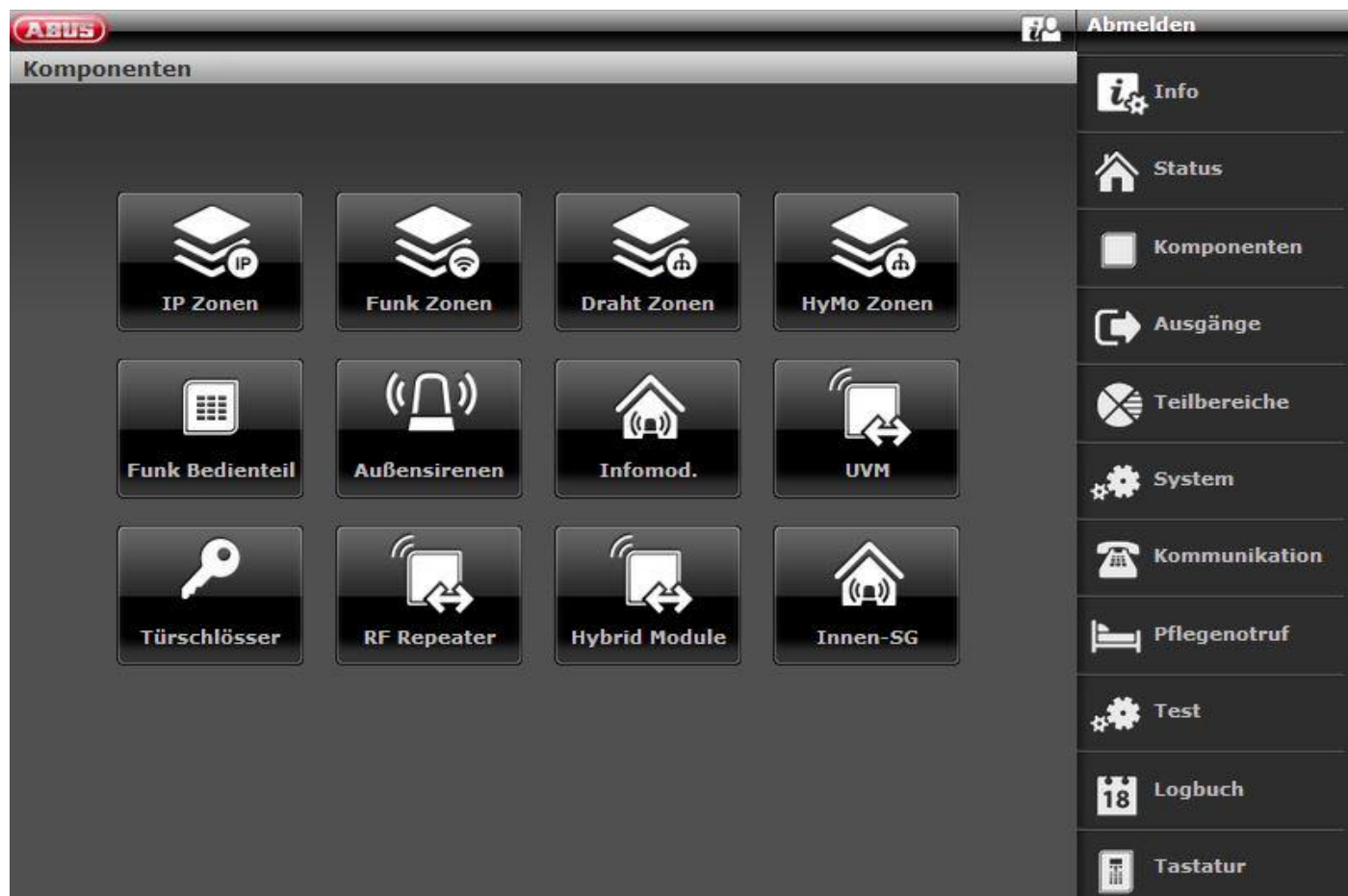
Indoor Sounders

Log out

-  About
-  Status
-  Devices
-  Outputs
-  Partitions
-  System
-  Communications
-  Social Care
-  Test
-  18 View Log
-  Keypad



S/W &gt;= 3.01.14

**Note**

From S/W 2.00.00 onwards, teach-in is possible via the web interface. To do this, simply click on an as yet unassigned zone, siren etc. The system will guide you through the teach-in process. Once teach-in is complete in the web interface, you must define the zone type.

The creation of a wireless zone is given here as an example:

## Configuration












**ABUS**
Log out

Devices | Wireless Zones | **Z204 Radio**

Radio detector learned: No

Type: \*Not Used ▼ Name: Zone 204

Partitions:  1  2  3  4

-  About
-  Status
-  Devices
-  Outputs
-  Partitions
-  System
-  Communications
-  Social Care
-  Test
-  View Log
-  Keypad

Name/function	Explanation
<b>Name</b>	Unique name of the zone
<b>Partition</b>	Partition of the individual zone
<b>Type</b>	Type of the individual wireless zone
<b>Attributes</b>	Overview of the attributes for the individual wireless zone

# Configuration

## Detectors


## IP zones

Number	Name	Partitions	Type	Attributes
Z101 IP	"Mini Dome"	1	Normal Alarm	
Z102 IP	"Big Dome"	1	Normal Alarm	
Z103 IP	"Zone 103"	None	Not Used	
Z104 IP	"Zone 104"	None	Not Used	
Z105 IP	"Zone 105"	None	Not Used	
Z106 IP	"Zone 106"	None	Not Used	

Attributes: Low Battery, Omit, Supervision fail, Tamper, Open SS:

Buttons: About, Status, Devices, Outputs, Partitions, System, Communications, Social Care, Test, View Log, Keypad, Delete All

Name/function	Explanation
<b>Number</b>	The number comprises the zone name and the component type (IP).
<b>Name</b>	Unique name of the zone
<b>Partition</b>	Partition of the individual zone
<b>Type</b>	Type of the individual IP zone
<b>Attributes</b>	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 or IPCx Range).  
 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.



**Note**

From S/W 1.01.00 onwards:

- 6 IP zones are available to you
- Unchanged function of the TVIP41550; "Camera mix" (TVIP41550/IPCxyyyyy) is possible
- Default value for camera "User name" and "Password" was removed

## Configuration

- IP zones "attributes" are hidden if the camera's "Trigger Mode" is set to "External"

For further details on integrating cameras from the IPCx range, see the "ABUS\_FUAA500xx\_IPCx\_Kameraintegration\_Secvest\_DE\_1.01.00.pdf" document.

Compatibility with the IPCx camera range

- Integration of up to 6 cameras
- External recording triggers from alarm pictures and/or video streams
- Recordings from the IPCxyyyyy are stored on the camera's integrated SD card
- Recordings (videos/pictures) from the IPCxyyyyy cameras can only be called up via the camera's web server or via the ABUS iDVR App (not via the alarm control panel log book)
- URL/link to the camera in the log book for all events for which there are recordings available

### Add/delete

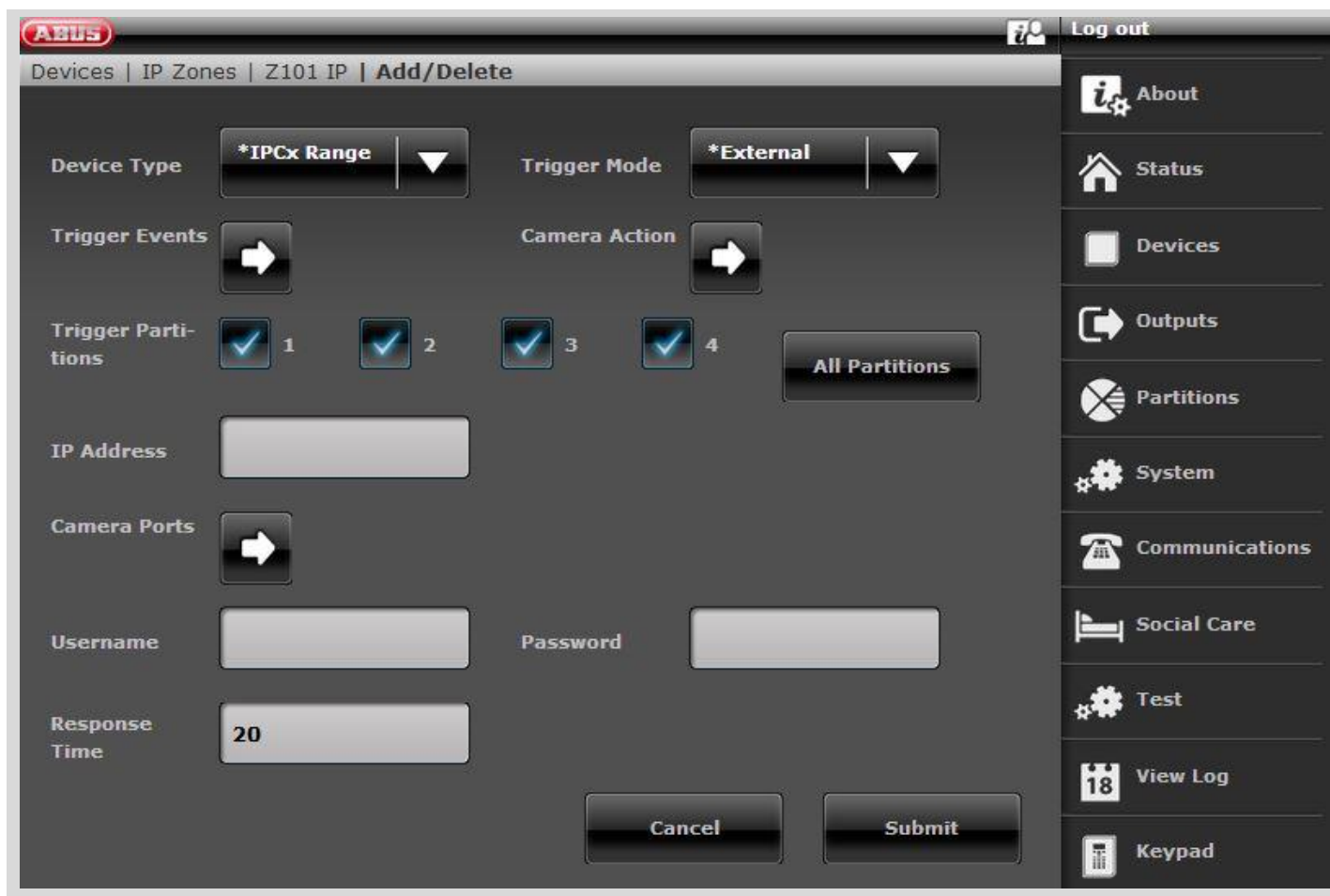
Select the desired IP zone in the menu "Devices" → "IP Zones". Use the "Add/delete..." button to open the following view where devices are integrated:

The screenshot shows the ABUS configuration interface for adding or deleting a device. The main window is titled "Devices | IP Zones | Z101 IP | Add/Delete". The interface is dark-themed and contains the following fields and controls:

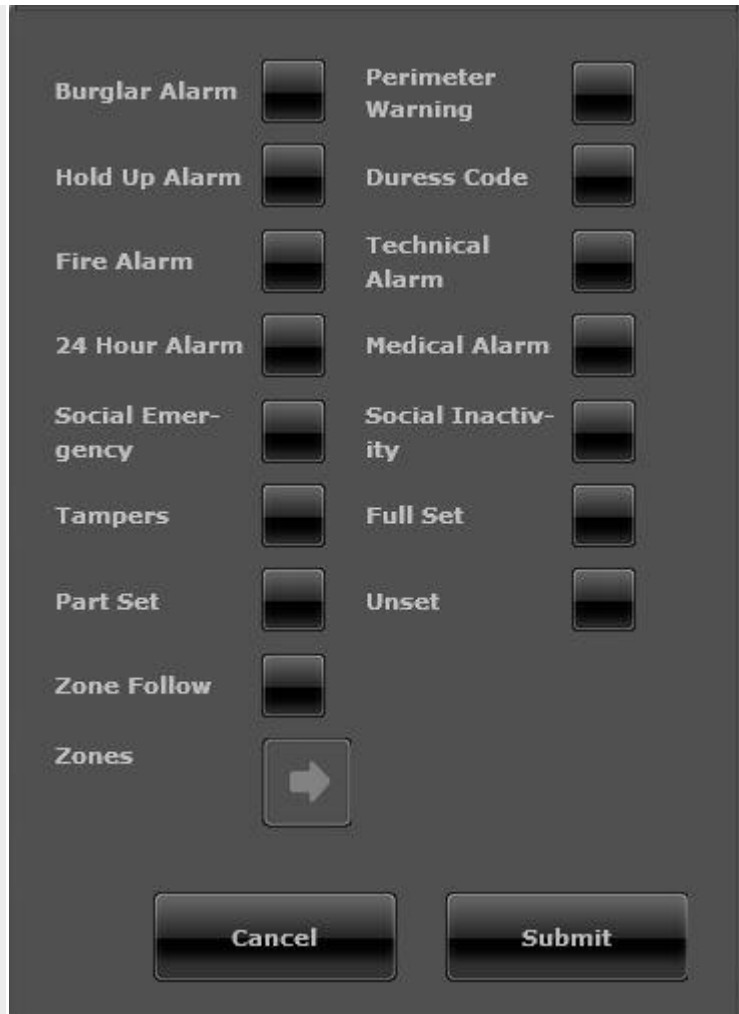
- Device Type:** A dropdown menu set to "Camera" with "TVIP41550" selected below it.
- Trigger Mode:** A dropdown menu set to "Int. + Ext.".
- Trigger Events:** A button with a right-pointing arrow.
- Trigger Partitions:** Four checkboxes labeled 1, 2, 3, and 4, all of which are checked. An "All Partitions" button is located to the right.
- IP Address:** An empty text input field.
- Camera Ports:** A button with a right-pointing arrow.
- Username:** An empty text input field.
- Password:** An empty text input field.
- Response Time:** A text input field containing the value "20".
- Buttons:** "Cancel" and "Submit" buttons at the bottom.

On the right side of the interface, there is a vertical sidebar menu with the following items:

- Log out
- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- Test
- View Log
- Keypad



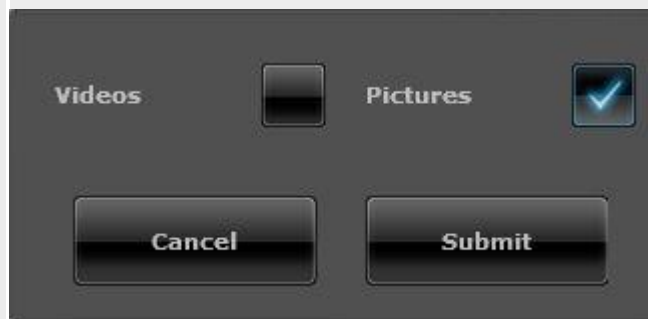
Name/function	Explanation
Device Type	Camera TVIP41550 IPCx Range
Trigger Mode	<p><b>Internal</b> TVIP41550 only The camera starts recording as soon as the integrated PIR sensor is triggered.</p> <p><b>External</b> The camera starts taking pictures or recording video (IPCx range) as soon as one of the defined trigger events occurs on the alarm panel.</p> <p><b>Int. + Ext.</b> TVIP41550 only 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.</p>
Trigger Events	<p><b>(for "External" or "Int. + Ext." trigger mode only)</b> Events which cause the camera to start taking pictures or recording video (IPCx range).</p>



A dark-themed dialog box for configuring alarm settings. It features two columns of settings, each with a label and a square checkbox. The settings are: Burglar Alarm, Hold Up Alarm, Fire Alarm, 24 Hour Alarm, Social Emergency, Tampers, Part Set, Zone Follow, Perimeter Warning, Duress Code, Technical Alarm, Medical Alarm, Social Inactivity, Full Set, and Unset. Below these settings is a 'Zones' label with a right-pointing arrow button. At the bottom are 'Cancel' and 'Submit' buttons.

**Camera Action**

IPCx range **only**  
Pictures and/or videos will be taken/recorded.



A dark-themed dialog box for configuring camera actions. It has two options: 'Videos' with an unchecked checkbox and 'Pictures' with a checked checkbox (indicated by a blue checkmark). Below the options are 'Cancel' and 'Submit' buttons.


**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

**Camera ports**

<b>HTTP Port Internal</b>	HTTP port of the camera in the internal network (default setting: "80")
<b>HTTP Port External</b>	External HTTP port for which port forwarding in the router is configured
<b>RTSP Port Internal</b>	RTSP port of the camera in the internal network (default setting: "554")
<b>RTSP Port External</b>	External RTSP port for which port forwarding in the router is configured
<b>User name</b>	<p>TVIP Default setting "Root" SW &gt;= 1.01.00: no user name is assigned</p> <p> <b>Danger</b> IP cameras, e.g. IPCB42500A Use user names from the camera "installer level". The system thus has access to the SD card in the event of an alarm. User names from the camera "master level" do not have access to the SD card.</p>
<b>Password</b>	Default setting – no password assigned
<b>Reaction time</b>	<p>Indicates the maximum amount of time that the alarm panel will wait for command responses from the camera. If the response time exceeds the configured time, a fault indication will be generated.</p> <p>Default setting – 20 s, range of 1 s to 99 s</p>

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**

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**.

1. Click in the **Name** text field.
2. Delete the preset name (Zone 01).

## 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**




### Note










Please note that the status of a zone (open or closed) must be kept for at least > 400 ms to ensure the alarm panel is able to detect the status change.

EN 50131-1 Chapter 8.9.1 Break-in detection, tampering, triggering and detecting faults – time requirements: "Break-in, intrusion and tampering signals with an active duration of over 400 ms must be processed."

Type	Explanation
<b>Not used</b>	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.
<b>Normal Alarm</b>	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).
	<p><b>Note</b></p> <p>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).</p> <p>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.</p>
<b>Zone Lock</b>	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.
	<p><b>Note</b></p> <p>This zone type was used in the Secvest 2WAY as a zone attribute rather than a zone type.</p>
<b>Exit Norm Alm</b>	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.







Type	Explanation
Panic 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	<p>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, on the outdoor siren (external siren) and other sounders as a pulsed fire alarm sound. Teach in only smoke alarm devices or fire alarm buttons in this zone.</p> <p>This zone always triggers a communication if these are enabled.</p>  <p><b>Note</b> regarding Partition -&gt; Alarm reaction</p> <p>The fire zone type, the fire double keys on the alarm panel and the fire double keys on the control panel <b>always</b> trigger an ARC/ESCC reporting if the call mode for ARC/ESCC reporting is enabled and if the "Fire" group is enabled for CID/SIA events.</p> <p>Example: Partition X -&gt; Alarm reaction -&gt; Siren Fire alarm transmission to ARC/ESCC</p>
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	<p>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.</p> <p>The wireless outdoor sirens flash and sound for approx. 1 s every five seconds.</p> <p>The info module beeps every 1 s and the red alarm LED lights up.</p> <p>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.</p> <p>(This tone is an "info" tone rather than an "alarm" tone.)</p> <p>All signals are active for a duration of 30 s.</p> <p>A "Perimeter Warning" output is activated for 30 s.</p> <p>When the system is disarmed only the doorbell ("chime") sounds, if configured.</p>
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.
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 <b>Enabled</b> to <b>Disarmed</b> , or from <b>Disarmed</b> to <b>Enabled</b> (in accordance with the programmed output mode).

Type	Explanation
	<p> <b>Note</b> So-called key switches can also be outputs for applications in access control and home automation.</p> <p> <b>Note</b> With the zone attribute "<b>Part Set</b>" = <b>ON</b> A change to this zone changes the status of the alarm panel from <b>Part Set</b> to <b>Disarmed</b>, or from <b>Disarmed</b> to <b>Part Set</b> (in accordance with the programmed output mode).</p> <p> <b>Note</b> The attributed "<b>inverted</b>" (only for wired zones) switches the behaviour of this zone.</p> <p> <b>Note</b> Implement cable tamper monitoring for wired zones of this type, particularly for access control and home automation applications. The user cannot reset the system from a key switch zone.</p>
<b>Key Switch (Latched)</b>	<p>A (latched) key switch can be connected to the alarm panel. A change to this zone changes the status of the alarm panel from <b>Enabled</b> to <b>Disarmed</b>, or from <b>Disarmed</b> to <b>Enabled</b> (in accordance with the programmed output mode).</p> <p> <b>Note</b> Do not assign more than one "Key switch duration" to a partition. 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.</p> <p> <b>Note</b> So-called key switches can also be outputs for applications in access control and home automation.</p> <p> <b>Note</b> With the zone attribute "<b>Part Set</b>" = <b>ON</b> A change to this zone changes the status of the alarm panel from <b>Part Set</b> to <b>Disarmed</b>, or from <b>Disarmed</b> to <b>Part Set</b> (in accordance with the programmed output mode).</p> <p> <b>Note</b> The attributed "<b>inverted</b>" (only for wired zones) switches the behaviour of this zone.</p> <p></p>

Type	Explanation
	<p><b>Note</b></p> <p>Implement cable tamper monitoring for wired zones of this type, particularly for access control and home automation applications.</p> <p>The user cannot reset the system from a key switch zone.</p>
<b>Key Box</b>	<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>
<b>Tamper Activated</b>	<p>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.</p>
<b>Log only</b>	<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>
<b>Exit Terminate</b>	<p>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.</p>
<b>Lock Set</b>	<p>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.</p>
<b>Ext WD Fault</b>	<p>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.</p>
<b>HUD Fault</b>	<p>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.</p>
<b>Tamper Return</b>	<p>This zone is used to monitor the tampering 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.</p>
<b>Ext PSU A/C fault</b>	<p>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.</p>
<b>Ext PSU Batt Fault</b>	<p>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.</p>
<b>Ext PSU Low Volts</b>	<p>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</p>

## Configuration

---

Type	Explanation
	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.
<b>Ext PSU Fault</b>	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.
<b>Only enabled</b>	<p>This zone is used to ONLY ENABLE the alarm panel for access control and home automation applications. With this zone, the alarm panel CANNOT BE DISARMED due to EN 50131 and VdS requirements.</p> <p>Clear user authentication or user identification is not always available in home automation.</p> <p>An output of an access control or home automation application can be connected to the burglar alarm system.</p> <p>A change to this zone changes the status of the alarm panel from <b>Disarmed</b> to <b>Enabled</b> (in accordance with the programmed output mode).</p> <p> <b>Note</b></p> <p>Please note that the access control or home automation application in this zone must be closed again after a specified period (but &gt; 400 ms). When the status is not known, e.g. when the zone is open but disabled on the control panel at the same time, the alarm panel may return to the "Set" status.</p> <p> <b>Note</b></p> <p>With the zone attribute "<b>Part Set</b>" = <b>ON</b></p> <p>A change to this zone changes the status of the alarm panel from <b>Disarmed</b> to <b>Part Set</b> (in accordance with the programmed output mode).</p> <p> <b>Note</b></p> <p>The attributed "<b>inverted</b>" (only for wired zones) switches the behaviour of this zone.</p> <p> <b>Note</b></p> <p>Implement cable tamper monitoring for wired zones of this type, particularly for access control and home automation applications.</p> <p>The user cannot reset the system from an Only enabled zone.</p>

### 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.

A settings option for the partitions can be found in the section "Configuring Secvest via web server -> Partitions" in this guide.

**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
<b>Supervision</b>	<p><b>for IP zones</b></p> <p>If a camera has had no contact with the alarm panel for longer than the reaction time, the alarm panel creates a log entry and indicates a warning (e.g. IP Zone Missing, IP-Zone Timeout).</p> <p><b>for wireless zones</b></p> <p>This attribute is available for wireless zones and enables monitoring to be blocked for individual zones.</p> <p>For the ON setting (standard setting), the monitoring for this zone corresponds to the selected global option in System -&gt; Security -&gt; RF Supervision.</p> <p>When the setting is on OFF, the monitoring for this zone is disabled.</p>

	<p>In wired zones: not available</p> <p>In HyMo zones: not available</p>
<b>Chime</b>	Each time this zone is triggered when the alarm panel is disarmed, the panel sounds an acoustic signal.
<b>Force Set Omit</b>	<p>If a zone is given this attribute, this zone is automatically omitted if it was open when the system was armed.</p> <p> <b>Note</b> The <b>Force SetOmit</b> function must <b>also</b> still be activated in menu <b>System -&gt; Security Settings -&gt; Force Set.</b></p>

Attribute	Explanation
<b>Omittable</b>	<p>If a zone is given this attribute, a user can omit this zone before arming the system.</p> <p>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.</p> <p>The user can acknowledge this warning and continue the arming process.</p>
<b>Dis. Sabotage</b>	<p>This attribute is an additional attribute for mechatronic ABUS door and window locks. The "Normal Alarm" zone type must be selected.</p> <p>When the "Dis. Sabotage" attribute is selected, pry-attempt monitoring of the supported mechatronic products is switched off when the alarm system / the partition is <b>disarmed</b>. This attribute is not recommended and is only necessary in special cases.</p> <p>A "W" appears in the attribute line on the alarm panel display.</p> <p> <b>Note</b> Conversely, if the system activates the partition or is internally activated (even if the detector is not being monitored), an entry attempt is detected and signalled.</p>

<b>Soak Test</b>	<p>If a detector tends to trigger a false alarm, activate the soak test.</p> <p>This setting resets automatically after 14 days.</p> <p>The detector <b>does not trigger any alarms</b> on the alarm panel during this time.</p> <p>However, all triggers are written to the memory (log book) for analysis purposes.</p> <p></p> <p><b>Note</b></p> <p>If the zone is triggered within these 14 days when the system is activated, the arming of system will log the event as "soak test fault Znnn alarm" (nnn is the zone number). No sirens will be actuated or communications started.</p> <p>If the alarm panel is deactivated, the display will show a triangular symbol to inform the user. An <b>installer</b> must enter <b>their access code</b> to reset the alarm.</p> <p>When activated, the display will show a short message to inform the user that one or more zones are in the soak test.</p> <p>You can use this attribute for the following zone types: Normal alarms, entry route and tamper.</p> <p></p> <p><b>Note</b></p> <p>The <b>Soak Test</b> function should only be set if a detector tends to trigger <b>false alarms</b>.</p>
------------------	--

	<p>This function works automatically. To test the range of the detector, use the "walk test" function and do <b>not</b> activate the soak test, as this function <b>stops the detector from triggering any alarms when the wireless alarm system is armed</b> and only saves a message to the memory instead.</p> <p>After 14 days the wireless alarm system resets the zone and brings it back to normal operation.</p>
<b>Part Set</b>	This zone is monitored when the partition of this zone or all partitions are internally armed.
<b>Activity Mon.</b>	<p>The function of the detector is reversed (inverted). <b>This should only be used in connection with the social care emergency call.</b></p> <p>An alarm is triggered on the alarm panel when the detector does not register any alarm within a certain time period.</p>
<b>Inverted</b>	<p>Only in wired zones</p> <p>Switches the behaviour of the indicator.</p> <p>Closed = alarm</p> <p>Open = no alarm</p>

## Wireless Zones

**ABUS**
Log out

Devices | **Wireless Zones**

Low Battery  
Omit  
Supervision fail  
Tamper  
Open  
SS:

Number	Name	Partitions	Type	Attributes
Z201 Radio	"MK"	1	Normal Alarm	9 (9)
Z202 Radio	"FTS 96"	2	Normal Alarm	9 (9)
Z203 Radio	"Smoke"	1	Fire Alarm	9 (9)
Z204 Radio	"Zone 204"	None	Not Used	
Z205 Radio	"Zone 205"	None	Not Used	
Z206 Radio	"Zone 206"	None	Not Used	
Z207 Radio	"Zone 207"	None	Not Used	
Z208 Radio	"Zone 208"	None	Not Used	

◀ ... 1 2 3 4 5 ... ▶

Delete All

ⓘ About

🏠 Status

📱 Devices

➡ Outputs

🗘 Partitions

⚙️ System

☎️ Communications

🛏️ Social Care

⚙️ Test

📅 View Log

📞 Keypad

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

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

### Add/Del Detectors

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

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

### Adding detectors

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

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

**Note**

## Configuration


---

After programming via the WBI, you still need to configure the zone.

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, "RSSI:" (received signal strength) is displayed. To have good communication, this value should be higher than 3.



### Note

If a detector has 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.

### 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 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.

### Clear all

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.



**Wired Zones**

ABUS Log out

Devices | **Wired Zones**

Number	Name	Partitions	Type	Attributes
Z301 Wired	"Zone 301"	None	Not Used	Low Battery Omit Supervision fail Tamper Open SS:
Z302 Wired	"Zone 302"	None	Not Used	
Z303 Wired	"Zone 303"	None	Not Used	
Z304 Wired	"Zone 304"	None	Not Used	

**Delete All**

- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- Test
- View Log
- Keypad

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

## HyMo zones

ABUS Abmelden

Komponenten | HyMo Zonen

Nummer	Name	Teilbereiche	Typ	Eigenschaften
Z401 HyMo	"Zone 401"	1	Normal Alarm	Türgong, Intern überwacht
Z402 HyMo	"Zone 402"	2	Normal Alarm	Türgong, Intern überwacht
Z403 HyMo	"Zone 403"	3	Normal Alarm	Türgong, Intern überwacht
Z404 HyMo	"Zone 404"	4	Normal Alarm	Türgong, Intern überwacht
Z405 HyMo	"Zone 405"	1-4	Normal Alarm	Türgong, Intern überwacht
Z406 HyMo	"Zone 406"	1	Nur Aktiv	
Z407 HyMo	"Zone 407"	2	Nur Aktiv	
Z408 HyMo	"Zone 408"	3	Nur Aktiv	

← ... 1 2 ... →

**Entfernen Alle**

Info

Status

Komponenten

Ausgänge

Teilbereiche

System

Kommunikation

Pflegenotruf

Test

Logbuch

Tastatur

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

### Delete All

1. Select **Delete All**.
2. Confirm the selection with **Next**.
3. Confirm the security prompt with **Yes** to delete the zone or select **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.

ABUS

Komponenten | HyMo Zonen | Z401 HyMo

Typ: \*Normal Alarm

Name: Zone 401

Teilbereiche:  1  2  3  4 Alle Teilbereiche

Eigenschaften:

- Türgong
- Ausblendbar Zwangsaktiv
- invertiert
- Aktivitätsüberwachung
- Belastungstest
- Intern überwacht
- Ausblendbar
- Ignoriere Hebel

Abbruch Übernehmen

Abmelden

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



### Note

#### S/W >= 3.01.16

Zones on the hybrid module can only be assigned to the partitions to which the HyMo is also assigned.

Example: If you have selected partitions 1 and 2 for the HyMo, zones on this HyMo can also only be assigned to partitions 1 and 2.

Refer to the assignment of partitions for the hybrid module. Notifications from the hybrid module, such as tamper or DC fault notifications, are then assigned to these partitions.

#### S/W < 3.01.16

Hybrid module zones can be assigned to other partitions but they should be hybrid module partitions.

Refer to the assignment of partitions for the hybrid module. Notifications from the hybrid module, such as tamper or DC fault notifications, are then assigned to these partitions.



### Note

The wiring type (**Wired Zone Type**) for the zone inputs of this hybrid module can be set under **Components -> Hybrid Module**.



### Note

#### Zones

##### Hybrid module 1

401 to 410 where 2-wire is chosen as the zone type

401 to 405 where 4-wire is chosen as the zone type

##### Hybrid module 2

411 to 420 where 2-wire is chosen as the zone type












411 to 415 where 4-wire is chosen as the zone type

**Wireless control panel**

**ABUS**
Log out


Devices | **Control Devices**

Number	Name	Partitions
CDV 1	"Ctrl Dev 01"	1-4
CDV 2	Not added	
CDV 3	Not added	
CDV 4	Not added	
CDV 5	Not added	
CDV 6	Not added	
CDV 7	Not added	
CDV 8	Not added	



-  About
-  Status
-  Devices
-  Outputs
-  Partitions
-  System
-  Communications
-  Social Care
-  Test
-  View Log
-  Keypad

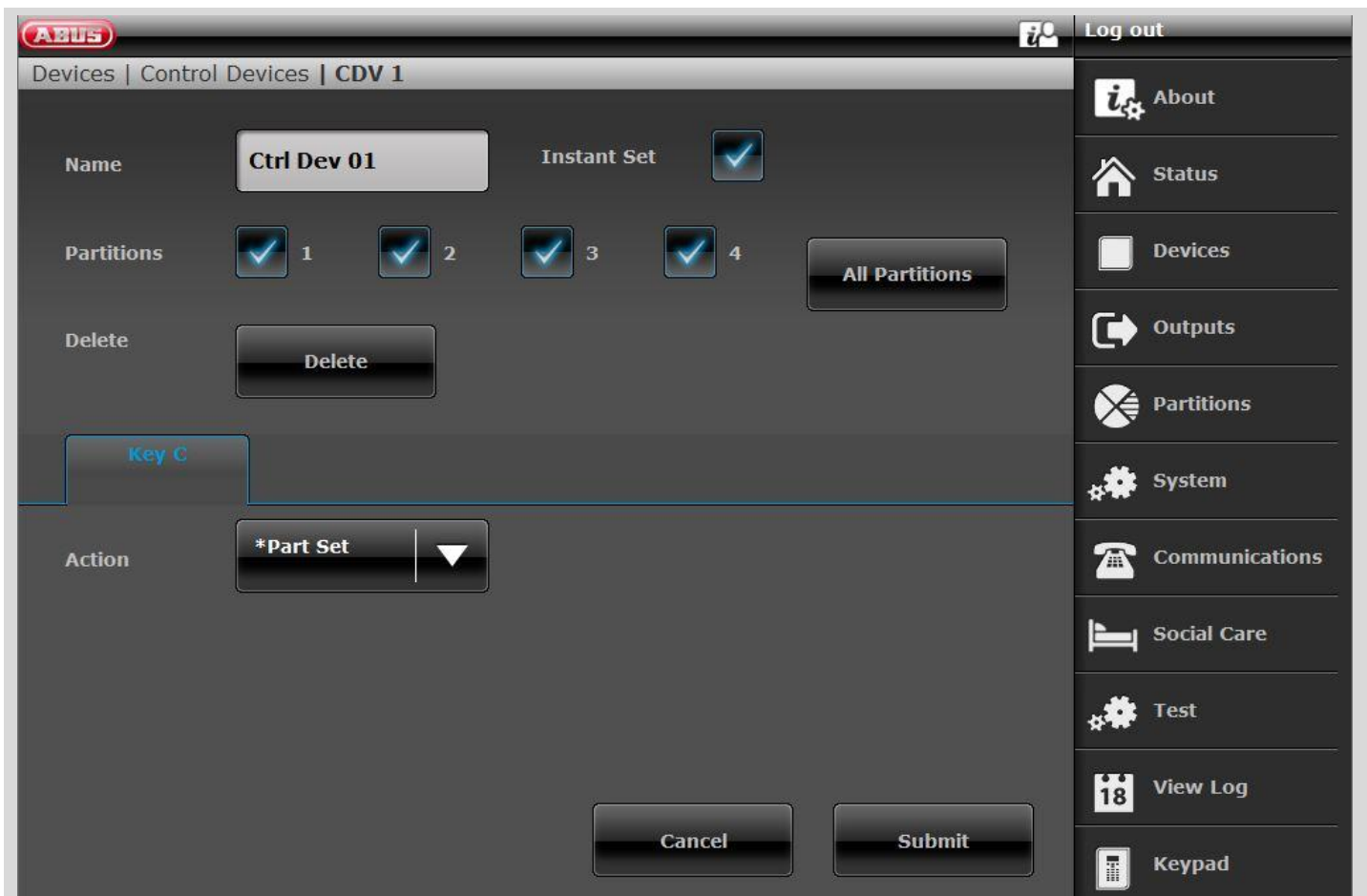
Name/function	Explanation
<b>Number</b>	The number comprises the component type (CDV) and a consecutive number.
<b>Name</b>	Unique name of the control device
<b>Partitions</b>	Assigned partitions of the individual control device

**Add wireless control panel**

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

## External Sirens

### Wireless sirens

Number	Name	Partitions
Radio SRN 1	Not added	
Radio SRN 2	Not added	
Radio SRN 3	Not added	
Radio SRN 4	Not added	

Name/function	Explanation
<b>Number</b>	The number comprises the component type (radio siren) and a consecutive number.
<b>Name</b>	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

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**

**ABUS**
 Log out

Devices | External Sirens | **Wired Sirens**

Number	Name
Wired SRN 1	"Wired SRN 01"

About

Status

Devices

Outputs

Partitions

System

Communications

Social Care

Test

View Log

Keypad

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



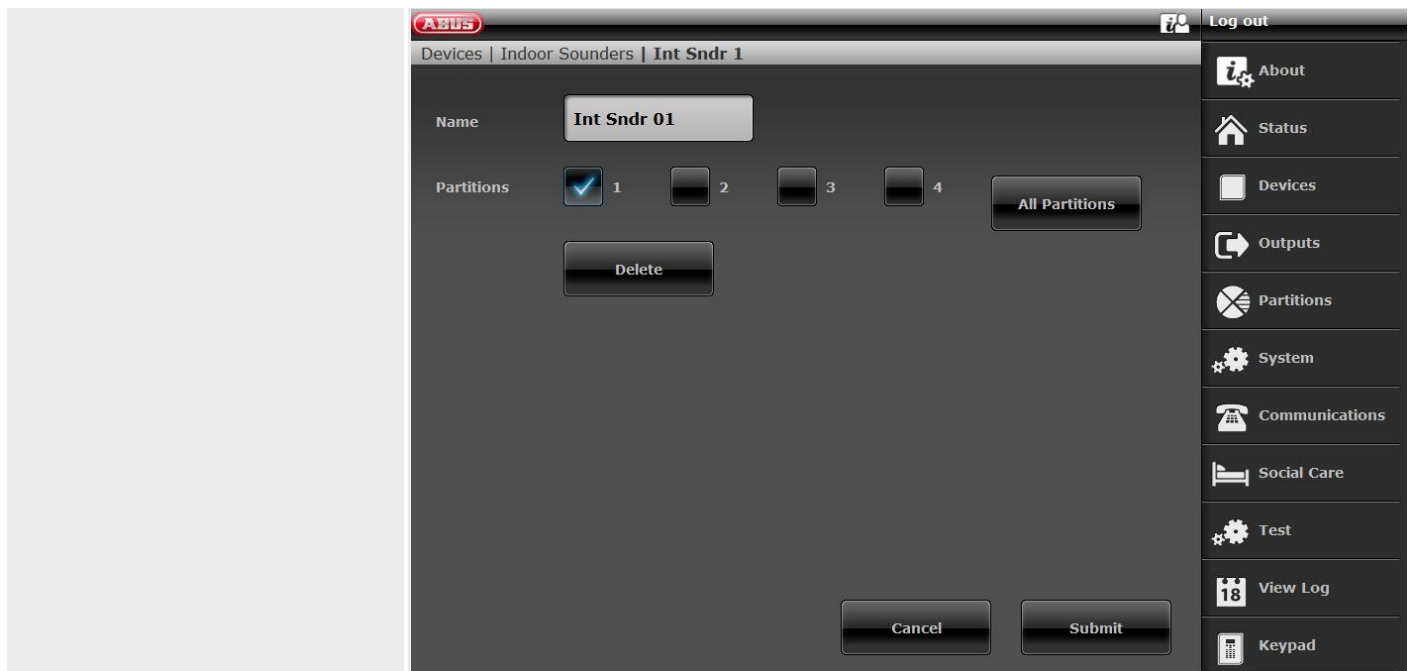
Indoor sounder

Number	Name	Partitions
Int Sndr 1	"Int Sndr 01"	1
Int Sndr 2	Not added	
Int Sndr 3	Not added	
Int Sndr 4	Not added	

**Delete All**

- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- Test
- View Log
- Keypad

Name/function	Explanation
<b>Number</b>	The number comprises the component type (indoor SG) and a consecutive number.
<b>Name</b>	Unique name of the indoor sounder (maximum 12 characters possible).
<b>Not added</b>	By clicking on the respective indoor sounder, you will arrive at the "Add" mode. The following course of action is the same as is described above for programming in the web interface.
<b>Int Sndr 1</b>	By clicking on the respective indoor sounder, you will arrive at the "Edit" mode.



The following course of action is the same as is described for the alarm panel's menu guidance below.

<b>Delete All</b>	Click on this field and in the next step confirm the security prompt to delete all indoor sounders.
<b>Remove</b>	Click on this field and in the next step confirm the security prompt to delete this indoor sounder.
<b>Partitions</b>	Numbers of the partitions to which the indoor sounder is assigned.

## Add indoor sounder (alarm panel)

1. Select **Indoor sounder**.
2. Select **Add/Del**.
3. Select the corresponding indoor sounder.
4. Trigger the tamper contact of the indoor sounder.




### Note

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

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



### Note

If an indoor sounder has been taught in, the symbol  appears next to the indoor signal generator number on the alarm panel display. A maximum of **4** indoor sounders can be added.

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

## Edit

Select the corresponding indoor sounder.

The following sub-menu items appear.

### Name:

Assign a unique name for this indoor sounder.

## Delete All

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



### **Danger**

The settings in the user menu:

User menu -> Configuration -> Volume Settings

Operator Sounds

Info tones:

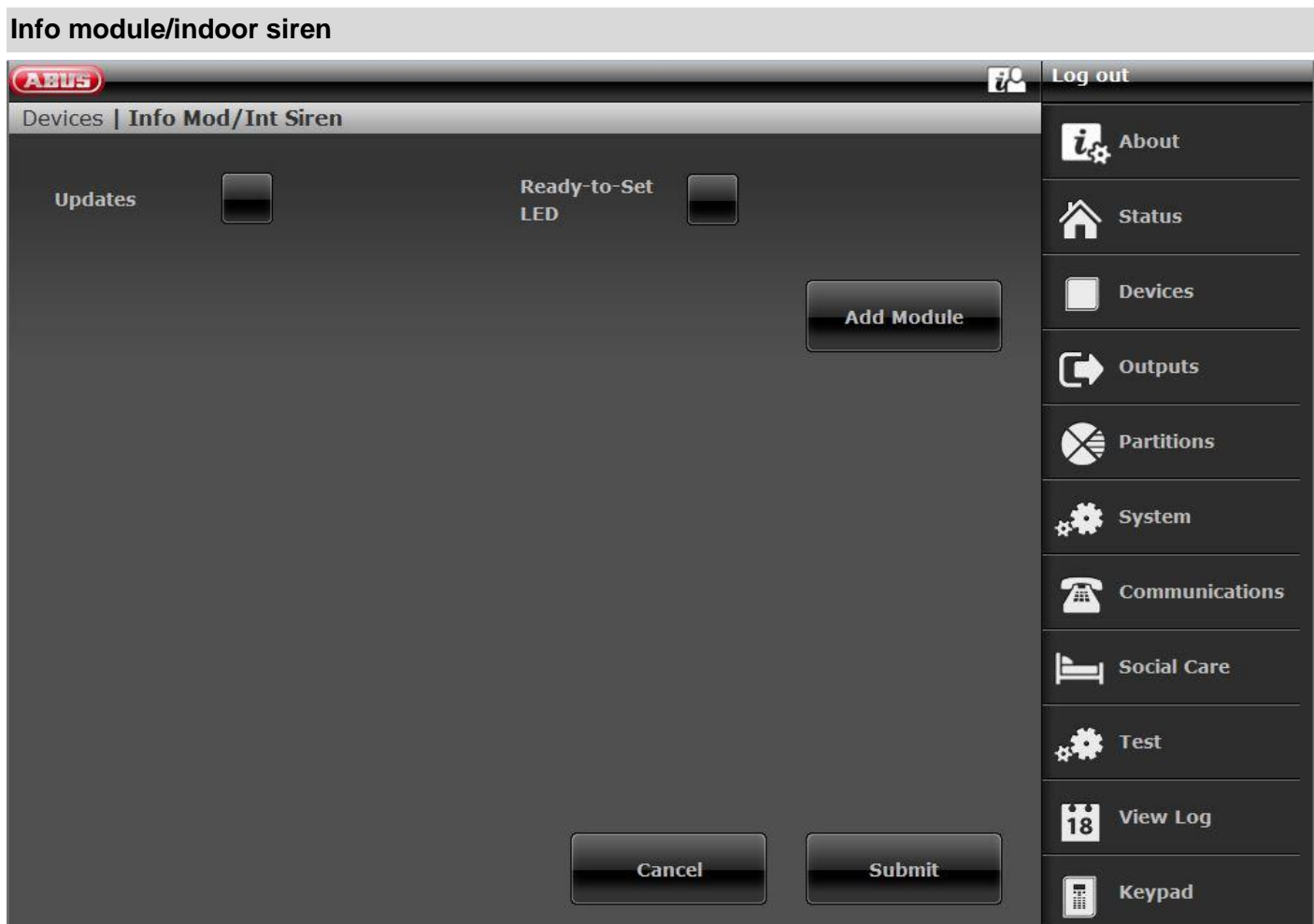
Alarm tones:

also affect the volume of the tones of the indoor sounder.



### **Note**

If the indoor sounder is operated by battery only, only alarm tones are sounded. No operation tones or info tones are sounded.



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



## WUM (Wireless Universal Module)

**ABUS**
Log out

Devices | **Accessory Modules**

Number	Name
Wam 1	Not added
Wam 2	Not added
Wam 3	Not added
Wam 4	Not added
Wam 5	Not added
Wam 6	Not added
Wam 7	Not added
Wam 8	Not added

- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- Test
- View Log
- Keypad

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

### Adding a wireless universal module.

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

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

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

1. Select **Add/Del WAM**.
2. **Select** the corresponding wireless universal module (WAM). Up to **eight** wireless universal 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 universal module.

5. Select **WAM Info**.

6. Select **WAM 1**.



**Note**

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

Function	Explanation
Not used	The wireless universal 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 universal 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 WUM.

See the instructions for the wireless universal module (WUM) for this.

**WAM as output module (WAM function 2)**



**Note**

If the wireless universal 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 universal accessory module (WUM) for this.

**WAM as zone and output module (WAM function 3)**



**Note**

If the wireless universal 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 universal module (WUM) 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 siren.

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



**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**

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

 Log out

Devices | Door Locks

Number	Name	Partitions
Door Lock 1	Not added	
Door Lock 2	Not added	
Door Lock 3	Not added	
Door Lock 4	Not added	
Door Lock 5	Not added	
Door Lock 6	Not added	
Door Lock 7	Not added	
Door Lock 8	Not added	

Delete All

- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- Test
- View Log
- Keypad

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

### Adding door locks (alarm panel)

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**

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**.

**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.

### Edit

Select the corresponding door lock. The following sub-menu items appear:

#### Name

Assign a unique name for this door lock.

#### Partitions

Select the partitions to which the door lock should be assigned.

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



### Disabled after breaking and entering (S/W >= 3.01.16)

#### Yes

Secvest Key and an additional door lock can activate and deactivate the assigned partitions.

#### NO

Assigned partitions **without** intruder alarm:

Secvest Key and an additional door lock can activate and deactivate the assigned partitions

Assigned partitions **with** intruder alarm:

Regardless of which assigned partition has an intruder alarm, Secvest Key and an additional door lock **cannot** deactivate the assigned partitions.

You must enter a code into the alarm panel or use another component for deactivation.

**Non-assigned partitions with** intruder alarm:

Secvest Key and an additional door lock can deactivate the assigned partitions.

#### Delete door lock

Confirm the security prompt with **Yes** to delete the door lock or **Back** if you are not sure.

#### Delete All

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.

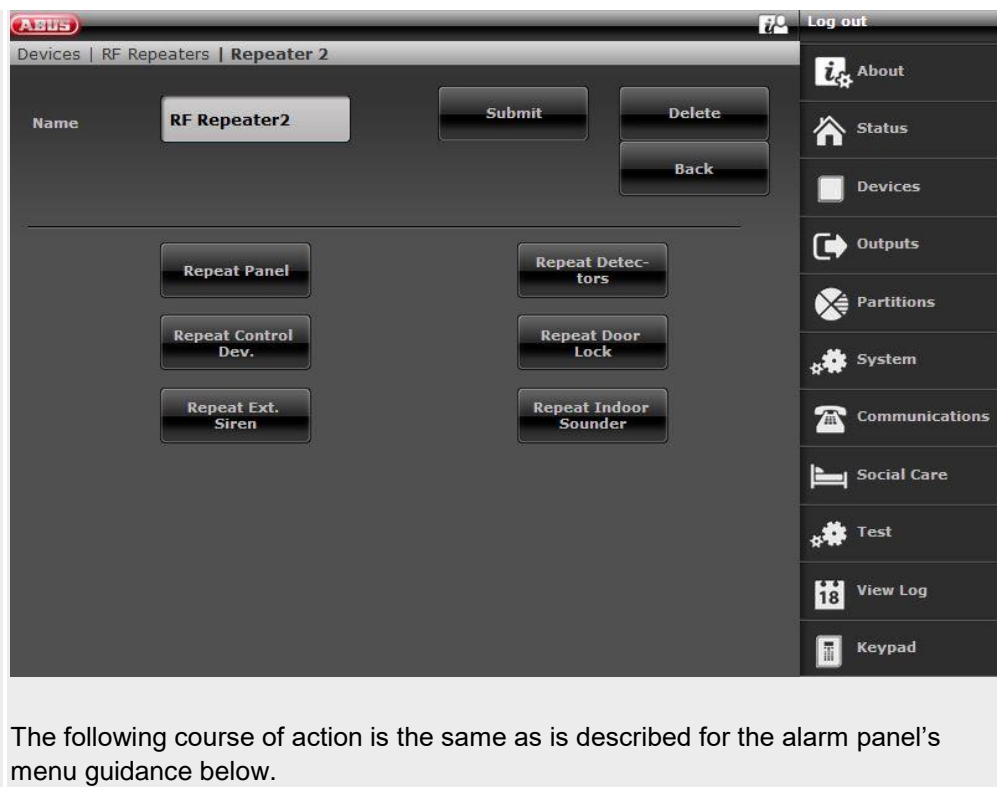
## RF repeater

The screenshot displays the 'RF Repeaters' configuration screen. At the top left is the 'ABUS' logo. The main area contains a table with the following data:

Number	Name
Repeater 1	"RF Repeater1"
Repeater 2	Not added
Repeater 3	Not added
Repeater 4	Not added


Below the table is a 'Delete All' button. On the right side, there is a vertical menu with icons and labels: About, Status, Devices, Outputs, Partitions, System, Communications, Social Care, Test, View Log, and Keypad. The top right corner features a 'Log out' button.

Name/function	Explanation
<b>Number</b>	The number comprises the component type (RF repeater) and a consecutive number.
<b>Name</b>	Unique name of the repeater (maximum 12 characters possible).
<b>Not added</b>	By clicking on the respective repeater, you will arrive at the "Add" mode. The following course of action is the same as is described for the alarm panel's menu guidance below.
<b>RF repeater1</b>	By clicking on the respective repeater, you will arrive at the "Edit" mode.



	
	<p>The following course of action is the same as is described for the alarm panel's menu guidance below.</p>
<p><b>Delete All</b></p>	<p>Click on this field and in the next step confirm the security prompt to delete all repeaters.</p>

**Add RF repeater (alarm panel)**

1. Select **RF repeater**.
2. Select **Add/Del**.
3. Select the corresponding repeater.
4. Trigger the tamper contact of the repeater.

 **Note**  
 When a repeater has been taught in, the wireless alarm panel beeps twice to confirm. A message appears on the display to confirm that the repeater was added, and the value for the received signal strength is shown. You can see the receiving signal strength of the alarm panel on the repeater through the status LEDs. Details on this can be found in the repeater manual.

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

 **Note**  
 If a repeater has been taught in the symbol  appears next to the repeater number on the alarm panel display. A maximum of **4** repeaters can be added

6. Exit this display with Back.

**Edit**

Select the corresponding repeater. The following sub-menu items appear.

**Name:**

Assign a unique name for this repeater.

**Repeat alarm panel**

Select whether wireless messages from the alarm panel should be repeated by this repeater.



**Note**

- Messages from the alarm panel could be:
- Broadcast alarm panel status – is necessary for the permanent display of the status of the partitions on the control panel FUBE5000x
  - Control of external sirens (e.g. FUSG50100/1 or FUSG50000)
  - Control of internal sirens (e.g. FUSG50010) and information modules (e.g. FUMO50030)
  - Control of indoor sounder (e.g. FUSG50110)
  - Control of hybrid modules (e.g. FUMO50110) – is necessary for the configuration and/or requesting of current and voltage values, the software version, the resistance values, the outputs, the loudspeaker and the signal strength.

## Configuration

---

Control of wireless outputs (e.g. wireless socket  
FUHA50010)

## Repeat detectors

Select which wireless zones/detectors should be repeated by this repeater. All detectors that have been learned in will be displayed.

## Repeat wireless control panel

Select which wireless control panel should be repeated. All wireless control panels that have been learned in will be displayed.

## Repeat door locks

Select which wireless door locks should be repeated. All wireless door locks that have been learned in will be displayed.

## Repeat outdoor sirens

Select which wireless external sirens should be repeated. All wireless external sirens that have been learned in will be displayed.

## Repeat indoor sounder

Select which indoor sounder should be repeated. All indoor sounders that have been learned in will be displayed.

## Repeat HyMo

Select which hybrid module should be repeated. All hybrid modules that have been learned in will be displayed.



### Note

A repeater can repeat a maximum of 10 components.

Remote controls and emergency transmitters (intrusion, medical emergency, care alarm) are always repeated when they are within the repeater's range.


## Delete All

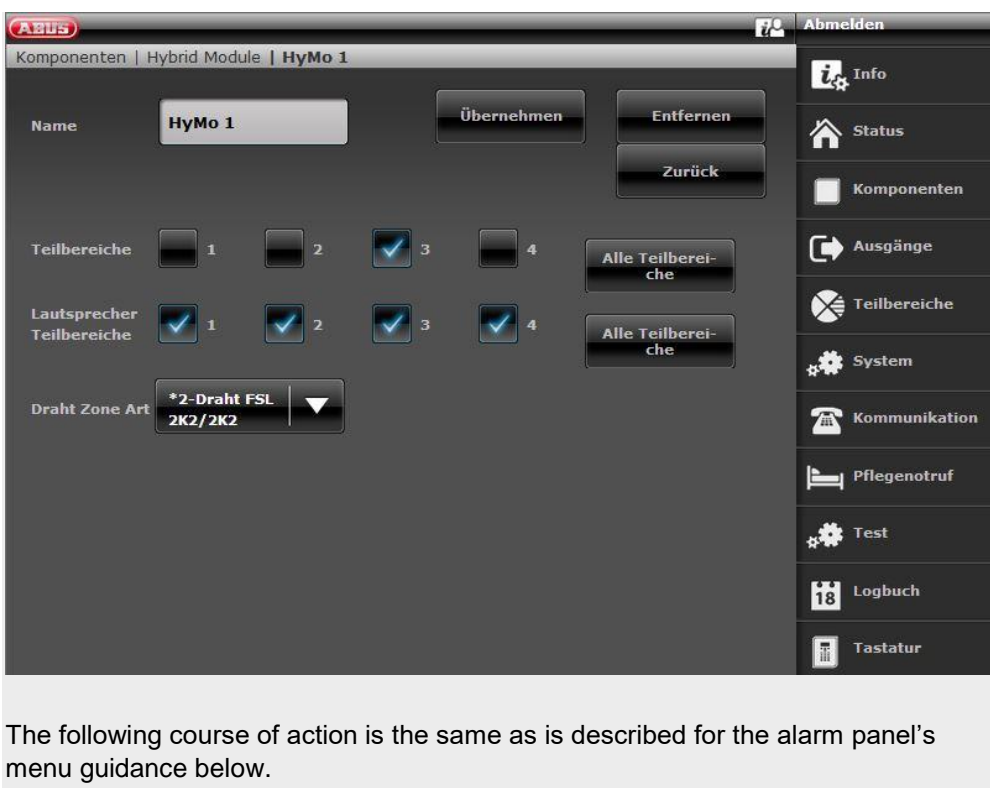
1. Select **Delete All**.
2. Confirm the selection with **Next**.
3. Confirm the security prompt to delete all repeaters with **Yes**. Select **Back** if you are not sure.

## Hybrid module

S/W >= 3.01.14


Nummer	Name	Teilbereiche	Lautsprecher Teilbereiche
HyMo 1	"HyMo 1"	3	1-4
HyMo 2	"HyMo 2"	1	1-4

Name/function	Explanation
<b>Number</b>	<p>The number comprises the component type (hybrid module) and a consecutive number.</p>  <p>Note A maximum of 2 hybrid modules can be added</p>
<b>Name</b>	Unique name for the hybrid module (maximum 12 characters possible).
<b>Not added</b>	By clicking on the respective hybrid module, you will arrive at the "Add" mode. The following course of action is the same as is described for the alarm panel's menu guidance below.
<b>HyMo 1</b>	By clicking on the respective hybrid module, you will arrive at the "Edit" mode.



	
<p><b>Delete All</b></p>	<p>The following course of action is the same as is described for the alarm panel's menu guidance below.</p> <p>Click on this field and in the next step confirm the security prompt to delete all hybrid modules with <b>Yes</b>. Select <b>Back</b> if you are not sure.</p>

**Add hybrid module (alarm panel)**

1. Select **Hybrid Module**.
2. Select **Add/Del**.
3. Select the corresponding hybrid module.
4. Trigger the tamper contact of the hybrid module.

 **Note**  
 When a hybrid module has been taught in, the wireless alarm panel beeps twice to confirm this. A message appears on the display to confirm the hybrid module has been added, and the value for the received signal strength is shown.

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

 **Note**  
 If a hybrid module has been taught in, the symbol  appears next to the hybrid module number on the alarm panel display  
 A maximum of 2 hybrid modules can be added

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

**Edit**

Select the corresponding hybrid module.

The following sub-menu items appear.

**Name:**

Assign a unique name to this hybrid module.

**Partitions**

Numbers of the partitions to which the hybrid module is assigned.



**Note**

Refer to the assignment of partitions for the hybrid module. Notifications from the hybrid module, such as tamper or DC fault notifications, are then assigned to these partitions.

**SW >= 3.01.16**

This partition assignment also determines the assignment of zones and outputs to partitions.

Example: If you have selected partitions 1 and 2 here, zones on this HyMo can also only be assigned to partitions 1 and 2.

**SW < 3.01.16**

Hybrid module zones and outputs can be assigned to other partitions but they should be hybrid module partitions.

## Wired Zone Type

Select which wiring type should be supported for the zone inputs of this hybrid module.



### Note

It is possible to select a different type of wiring for the alarm panel and for each of the 2 hybrid modules.

Possible wiring types:

- 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

The variants are the same as for the alarm panel, see also:

System -> Hardware -> Wired Zone Type

## Loudspeaker partitions

Select the partitions for which the optionally connected loudspeaker should provide a signal.



### Note

The loudspeaker repeats the signal tones:

You can set the volume of the different signal tones for the loudspeaker in the user menu.

User menu -> Configuration -> Volume settings ->

Operator Sounds

Info tones:

Alarm tones:



### Note

Loudspeaker partitions for the hybrid module can be assigned to other partitions but they should be hybrid module partitions.

## Zone types and attributes

Are selected in the HyMo Zones section. All available types and attributes for wired zones are possible. See IP Zones for details.

### Hybrid module 1

401 to 410 where 2-wire is chosen as the zone type

401 to 405 where 4-wire is chosen as the zone type

### Hybrid module 2

411 to 420 where 2-wire is chosen as the zone type

411 to 415 where 4-wire is chosen as the zone type



### Note

## Outputs

### Output types and attributes

Are selected in the HyMo Outputs section. All available types and attributes for wired outputs are possible. See Wireless Outputs for details.

### Hybrid module 1

401 to 404

### Hybrid module 2

405 to 408



### Note

## Hybrid module TR terminal

If this input is controlled by the hybrid module, the alarm panel signals

"Hybrid Module X Sounder Tamper"



### Note Zones



### Note

## Hybrid module terminal MAINS FAIL



If this input is controlled by the hybrid module,  
the alarm panel signals  
"Hybrid Module X PSU Network Fault"

If this input is controlled by the hybrid module,  
the alarm panel signals  
"Hybrid Module X PSU Battery Fault"

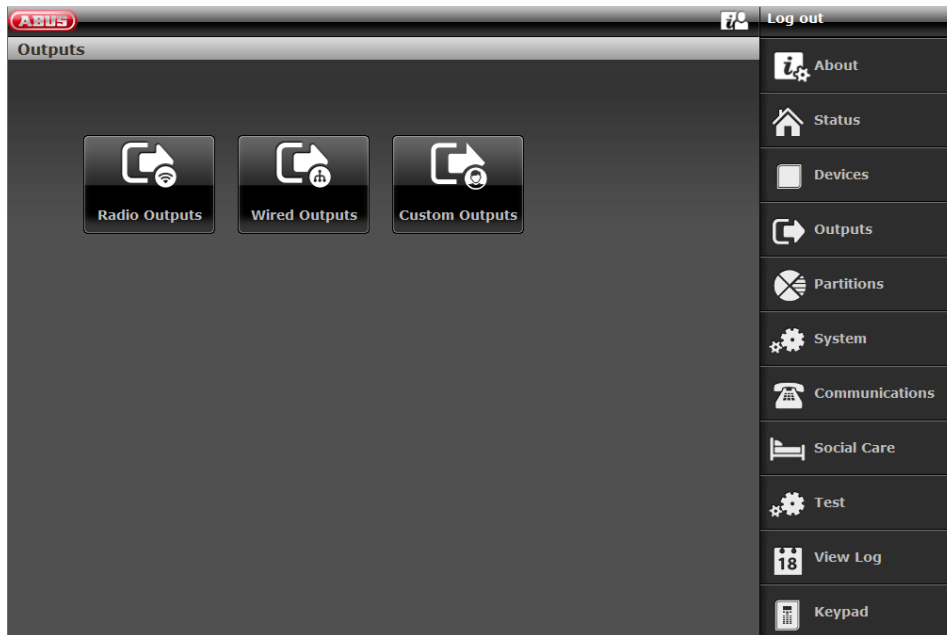


**Note**

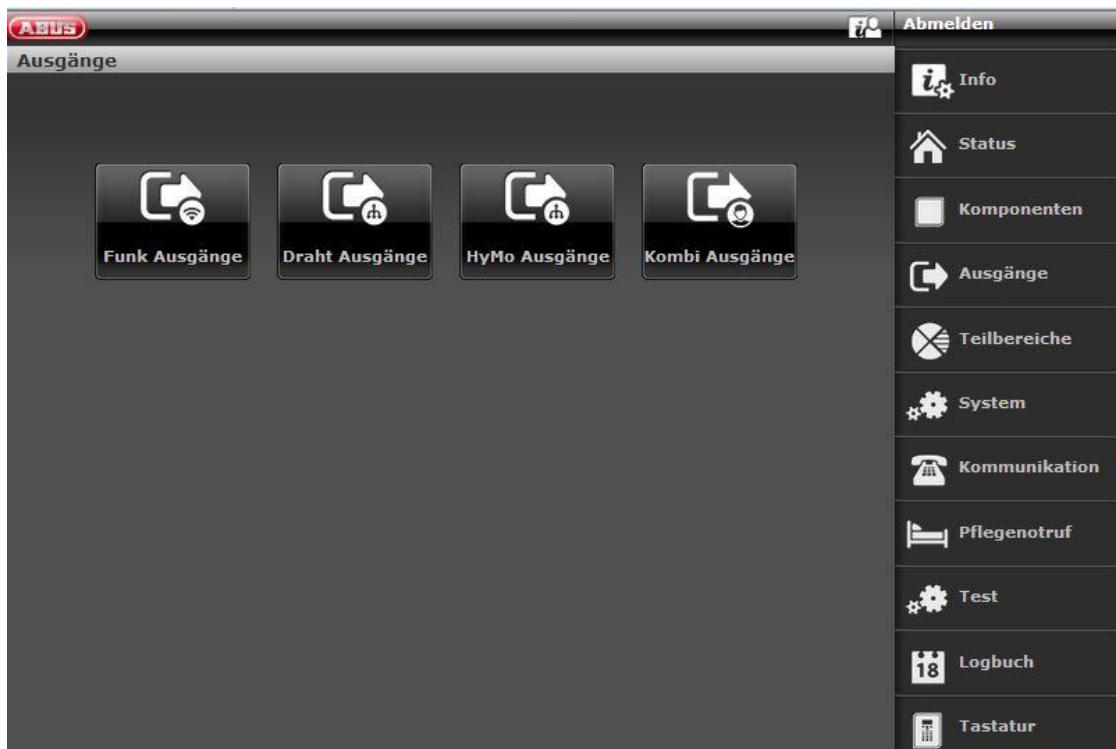
Hybrid module terminal LOW BATT

## Outputs

S/W < 3.01.14



S/W >= 3.01.14



**Radio Outputs**

**ABUS**
 **Log out**

Outputs				
Number	Name	Type	Status	Attributes
Radio O/P 201	"Ausgang 201"	User Defined		
Radio O/P 202	"Ausgang 202"	Not Used		
Radio O/P 203	"Ausgang 203"	Not Used		
Radio O/P 204	"Ausgang 204"	Not Used		
Radio O/P 205	"Ausgang 205"	Not Used		
Radio O/P 206	"Ausgang 206"	Not Used		
Radio O/P 207	"Ausgang 207"	Not Used		
Radio O/P 208	"Ausgang 208"	Not Used		
Radio O/P 209	"Ausgang 209"	Not Used		
Radio O/P 210	"Ausgang 210"	Not Used		

◀
...
1
2
3
4
...
▶

**About**
 **Status**

**Devices**
 **Outputs**

**Partitions**
 **System**

**Communications**
 **Social Care**

**View Log**
 **Keypad**

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




## Configuration

Type	Explanation	Can be assigned to partitions
<b>not used</b>	This output is not used and not activated at any time.	Yes
<b>Intruder alarm</b>	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"> <li>• Normal Alarm</li> <li>• Tamper (only when system is armed)</li> <li>• Entry Route</li> <li>• Tamper zone (only when system is armed)</li> <li>• Entry delay expired</li> <li>• 24 hour alarm (only when system is armed)</li> </ul>	Yes
<b>Conf. Intruder alarm</b>	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"> <li>• two "normal alarms" are triggered in the same partition during the confirmation time</li> <li>• a "normal alarm" and a tamper alarm are triggered in the same partition during the confirmation time.</li> </ul> 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
<b>Burg Confirm Timer</b>	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
<b>Perimeter Warning</b>	The output is activated when a perimeter warning is triggered.	Yes
<b>Panic alarm</b>	This output is activated when a hold up alarm is triggered.	Yes
<b>HUA Confirm</b>	A confirmed hold up alarm has occurred. The alarm panel activates the output under the following conditions: <ul style="list-style-type: none"> <li>• Users trigger an alarm at at least two different hold up transmitters during the hold up confirmation time.</li> <li>• A hold up transmitter is activated and a tamper alarm of a hold up transmitter is triggered during the confirmation time.</li> </ul> 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.	No

Type	Explanation	Can be assigned to partitions
<b>HUA Confirm Timer</b>	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
<b>Duress Code</b>	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
<b>Confirmed Alarm</b>	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
<b>Fire</b>	This output is activated when a fire alarm is triggered.	yes
<b>Technical Alarm</b>	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
<b>24 hours)</b>	This output is activated when a zone with the attribute "24 Hour Alarm" triggers an alarm.	Yes
<b>Zone Alarm</b>	This output is activated when the selected zone reports an alarm and is deactivated again when the alarm is reset.	No
<b>External Siren</b>	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
<b>Internal Siren</b>	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
<b>External Strobe</b>	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 <b>EXTERNAL</b> strobe signal for confirmation has been activated.	Yes
<b>Internal Strobe</b>	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 <b>INTERNAL</b> strobe signal for confirmation has been activated.	Yes
<b>Alarm Abort</b>	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

## Configuration

Type	Explanation	Can be assigned to partitions
<b>Alarm Abort</b>	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
<b>Medical Alarm</b>	This output is activated when a medical emergency call is triggered.	Yes
<b>Emergency call</b>	This output is activated when a social care call is triggered.	Yes
<b>Tamper Activated</b>	The output is activated when the alarm panel receives a tamper alarm from one of the following devices: <ul style="list-style-type: none"> <li>• Alarm panel (cover or wall tampering)</li> <li>• Control device (cover or wall tampering)</li> <li>• Zone with zone type "Tamper"</li> <li>• All wireless detectors or WAM</li> <li>• Sirens</li> </ul> The alarm panel deactivates the output as soon as the cause of tampering has been corrected.	Yes
<b>Radio frequency failure</b>	This output is activated as soon as one of the three RF faults listed below occur: This may be the following: RF Low Battery, RF Supervision, RF Jamming. The output is deactivated only when the fault is reset on the alarm panel.	Yes
<b>RF Supervision</b>	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
<b>RF Jamming</b>	The corresponding output is activated when signal jamming is detected. The output remains activated until the signal jamming is corrected.	No
<b>RF Low Battery</b>	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
<b>Battery Fault</b>	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

Type	Explanation	Can be assigned to partitions
<p><b>A/C fault</b></p>	<p>The output is activated when the alarm panel does not have voltage OR any zone with type "Ext PSU A/C fault" is triggered.</p> <p>The delay until this output is activated depends on the value set under "System -&gt; A/C Fault Delay (minutes)".</p> <p>  <b>Note</b>                      The system is VdS <b>compliant</b> if you use this output type for signalling an <b>AC fault</b>.</p>	<p>No</p>
<p><b>Ext PSU Fault</b></p>	<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>	<p>No</p>
<p><b>Ext PSU Low Volts</b></p>	<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>	<p>No</p>
<p><b>General Fault</b></p>	<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"> <li>• RF Low Battery</li> <li>• RF Supervision</li> <li>• RF Jamming</li> <li>• A/C fault</li> <li>• Battery Fault</li> <li>• Ext PSU Fault</li> <li>• Tamper Activated</li> </ul> <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> <p>  <b>Danger</b>                      SW &lt; 3.01.11                      The system is <b>no</b> longer VdS compliant if you use this output type to signal an <b>AC Fault</b> because it triggers automatically.                      Use this to signal an <b>AC Fault</b> type to be VdS compliant.</p> <p>  <b>Note</b>                      SW &gt;= v3.01.11</p>	<p>Yes</p>

## Configuration

---

	The system is VdS <b>compliant</b> if you use this output type for signalling an <b>AC fault</b> . This output type is now triggered after a VdS-compliant delay in the event of an AC fault.	
<b>Fault comm. path</b>	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.	No
<b>Full Set Ready</b>	This output is activated when the partition is ready to be 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
<b>Full Setting Complete</b>	The output is activated as soon as the system is successfully armed. The output is activated for approx. 10 seconds.	Yes



Type	Explanation	Can be assigned to partitions
<b>Complete arming</b>	This output is only activated when all of the partitions configured in the system are armed.	Yes
<b>Setting Complete</b>	This output is activated (for approx. 10 seconds) when the system or partition is armed or internally armed.	Yes
<b>Enabled</b>	This output is activated when the partition is armed.	Yes
<b>Rearmed</b>	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
<b>Part Set Ready</b>	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
<b>Part Setting Complete</b>	This output is activated (for approx. 10 seconds) when the system or partition is <b>INTERNALLY</b> armed.	Yes
<b>Part Set</b>	This output is activated when a partition is internally armed.	Yes
<b>Set Fault</b>	This output is activated when arming fails. It remains activated until the user confirms the fault.	yes
<b>Autoset Warning</b>	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
<b>Unset Complete</b>	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
<b>Zone Omit (Setting)</b>	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

## Configuration











Type	Explanation	Can be assigned to partitions
<b>Zone Omit (System)</b>	<p>(Output only functions when confirmation mode DD243 or BS8243 is selected.)</p> <p>When there is an unconfirmed alarm the alarm panel re-arms when the confirmation time has expired.</p> <p>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.</p> <p>The alarm panel restores the zone and resets the output when a user or installer resets the system.</p>	
<b>Entry Exit Follow</b>	<p>This output is activated for the duration of the delay time (entry delay or exit delay).</p> <p>The output is not activated if the partition has been configured in "Instant Set" or "Silent Set" mode.</p>	Yes
<b>Locking actively unlocked</b>	<p>A zone lock exists.</p> <p>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.</p>	No
<b>Open/Close</b>	<p>The output is activated when the system (or partition) is disarmed.</p> <p>It is deactivated when the system (or partition) is armed.</p> <p>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.</p> <p>Note: the function of this output is already inverted by default compared to the other outputs.</p> <p>There are 0 volts at this output when the system is disarmed.</p>	Yes
<b>Zone Follow</b>	<p>This output follows the status of a zone.</p> <p>If this type is selected, an overview of the zones is provided.</p> <p>Select a corresponding zone.</p>	No
<b>Indoor lighting</b>	<p>This output is activated while the entry/exit delay time is running and deactivated 10 seconds after the entry/exit delay time has expired.</p>	Yes
<b>Installer on Site</b>	<p>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.</p>	No
<b>Walk Test</b>	<p>The output is activated when a user starts a walk test both as an installer and as a normal user.</p> <p>The output is also activated in the time between an alarm being muted and the alarm confirmation.</p>	No

Type	Explanation	Can be assigned to partitions
<b>User Defined</b>	<p>An output of this type can be controlled remotely via different user-defined components such as remote control, control panel or alarm panel.</p> <p>The “Switch by user” and “configure by user” options grant the user permissions for the configuration of the output in the user menu view.</p> <p>The “Polarity” button can be used to invert the switching statuses.</p> <p>If the output should only be switched for a specific time (pulse behaviour), then un-tick the “Continuous” checkbox and set the desired duration.</p> <p>The output can also be assigned a time plan, which specifies when it should be activated or deactivated. The “Continuous” checkbox must be ticked for this. Then set the switching on time, the switching off time and select the desired days of the week.</p> <p>The output can also be switched by the occurrence of events. On the “Events” tab, you can set up to 3 events. The list contains all possible output types.</p>	No
<b>Smoke Sensor Reset</b>	<p>This output is always activated (0 V) except when a user confirms a fire alarm.</p> <p>After this confirmation, the alarm panel deactivates the output for 3 seconds.</p> <p>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).</p>	Yes
<b>PIR Set Latch</b>	<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 activated with +12 V when activated and 0 V when deactivated. Use the "Inverted" polarity to reverse the function of this output.</p>	Yes
<b>Combination Output 1</b>	<p>An output of this type combines various events. Details on this can be found in the "Combination Outputs" chapter.</p>	
...		
<b>Combination output 10</b>		

**Wired Outputs**


**ABUS**
Log out

Outputs				
Number	Name	Type	Status	Attributes
Wired O/P 301	"Ausgang 301"	Not Used		
Wired O/P 302	"Ausgang 302"	Not Used		
Wired O/P 303	"Ausgang 303"	Not Used		
Wired O/P 304	"Ausgang 304"	Not Used		

-  About
-  Status
-  Devices
-  Outputs
-  Partitions
-  System
-  Communications
-  Social Care
-  View Log
-  Keypad


Name/function	Explanation
<b>Number</b>	The number comprises the component type (wired output) and a consecutive number.
<b>Name</b>	Unique name of the wired output
<b>Type</b>	Type of the wired output
<b>Status</b>	Current status of the wired output
<b>Attributes</b>	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**  
An overview of the different output types can be found in the "Wireless outputs" section.

1. Select menu item **Type**.

## HyMo outputs

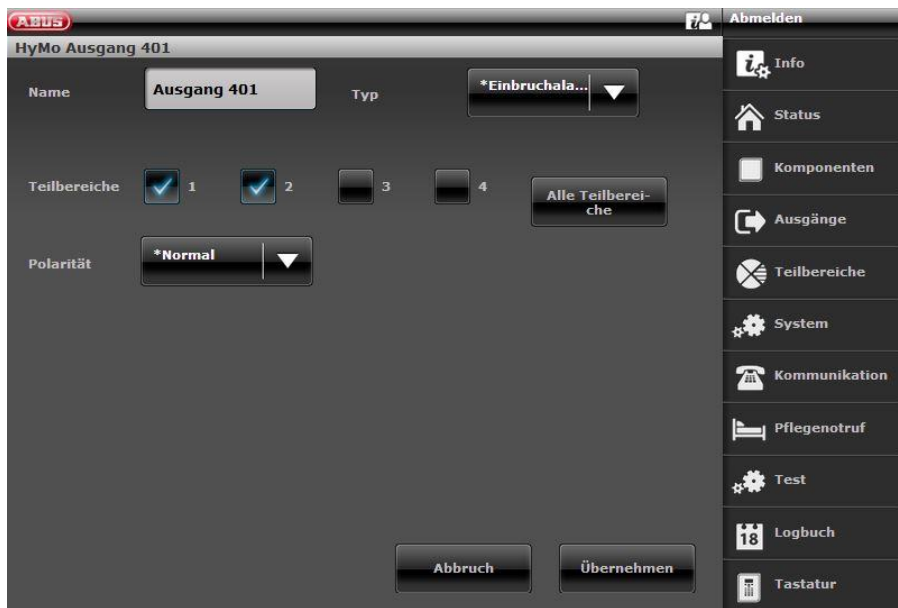
ABUS
Abmelden

Ausgänge			
Nummer	Name	Typ	Status
HyMo Ausgang 401	"Ausgang 401"	Einbruchalarm	Aus
HyMo Ausgang 402	"Ausgang 402"	Aktivierung fertig	Aus
HyMo Ausgang 403	"Ausgang 403"	RF Batt. schwach	Aus
HyMo Ausgang 404	"Ausgang 404"	Ben. definiert	Aus
HyMo Ausgang 405	"Ausgang 405"	Überfallalarm	Aus
HyMo Ausgang 406	"Ausgang 406"	Einbruchalarm	Aus
HyMo Ausgang 407	"Ausgang 407"	Externe Sirene	Aus
HyMo Ausgang 408	"Ausgang 408"	Externer Blitz	Aus

Abmelden

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

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



## Configuring HyMo wired outputs



### Note

Each hybrid module features four relay or 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)

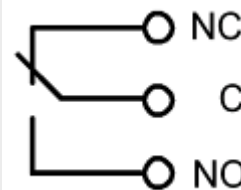


### Note

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

The HyMo output is a relay output.

For **Normal**:



It is possible to open (NC-C) or close (NO-C) a connected circuit.

If **inverted** the opposite is the case!

It is possible to open (NO-C) or close (NC-C) a connected circuit.

## Selecting the output type



### Note

An overview of the different output types can be found in the "Wireless outputs" section.

1. Select menu item **Type**.



### Note

#### **S/W >= 3.01.16**

Outputs on the hybrid module can only be assigned to the partitions to which the HyMo is also assigned. Example: If you have selected partitions 1 and 2 for the HyMo, outputs of this HyMo can also only be assigned to partitions 1 and 2.

Refer to the assignment of partitions for the hybrid module. Notifications from the hybrid module, such as tamper or DC fault notifications, are then assigned to these partitions.

#### **S/W < 3.01.16**

Hybrid module outputs can be assigned to other partitions but they should be hybrid module partitions.

Refer to the assignment of partitions for the hybrid module. Notifications from the hybrid module, such as tamper or DC fault notifications, are then assigned to these partitions.



### Note

#### **Outputs**

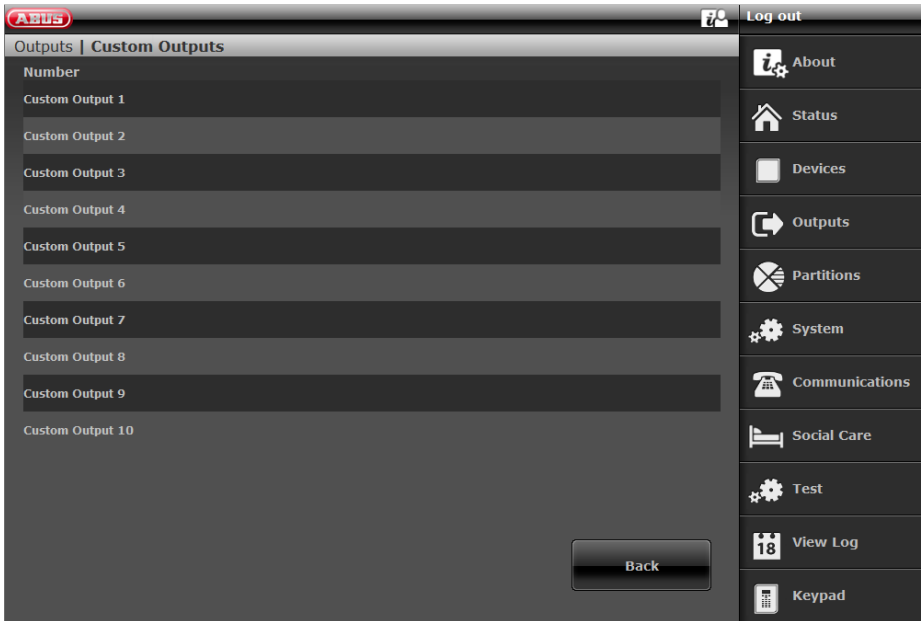
**Hybrid module 1**

**401 to 404**

**Hybrid module 2**

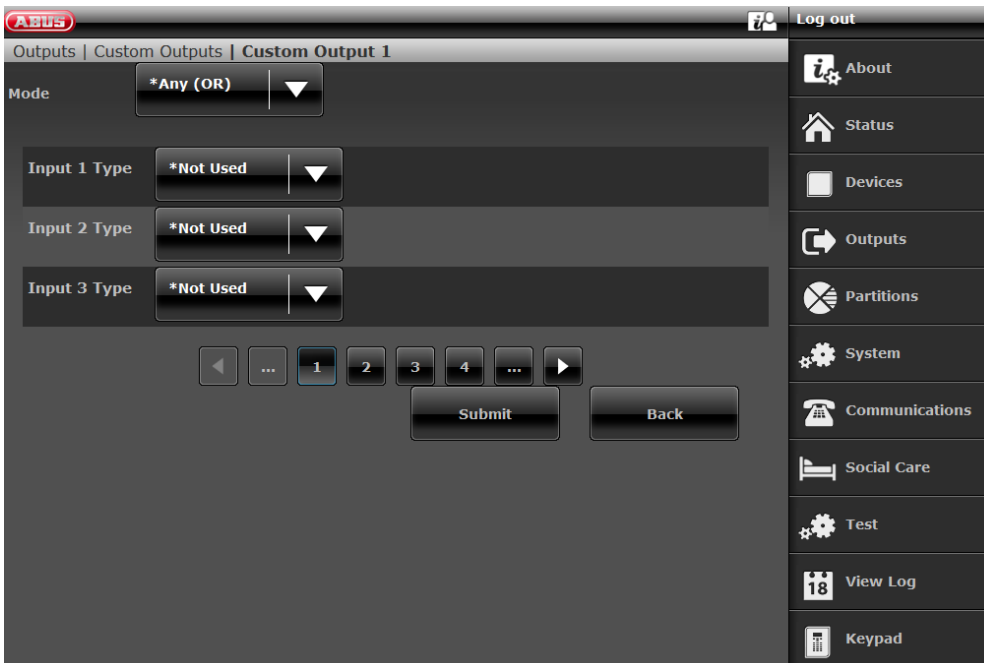
**405 to 408**

## Combination outputs



A "combination output" is a virtual logical element within the alarm panel.

It is similar to an AND-gate or OR-gate in digital electronics, but only exists within the configuration of the alarm panel. A "combination output" can have up to 10 inputs. A virtual input is an event such as a "burglar alarm" or a "panic alarm".



You can use a "combination output" to enable a wireless or wired output.

On the wireless or wired output, select the type "Combination output".



You have set up "Combination output 1". You can use this to enable "Wireless output 203" on the alarm panel. Assign "Combination output 1" as the type for "Wireless output 203".

You have to select one mode for each "combination output". This mode can be ALL (AND) or ANY (OR).

For the AND mode, **all** inputs of the "combination output" have to be enabled for it to function.

For the OR mode, **any** inputs of the "combination output" may be enabled for it to function.

### Example:

Requirement:

A wireless output should switch when a door (Zone 203) is open AND an installer has logged in in installer mode.

The solution:

Configure the wireless output with the type "Combination output 1" and configure "Combination output 1" as follows:

Combination output	Mode	input
1	ALL (AND)	Input 1 type = Installer on site Input 2 type = Zone follow (Zone 203)



### Note

An input may be the output of another "combination output". However, you can only select "combination outputs" with a number higher than the inputs.

For example, if the alarm panel supports 10 "combination outputs", and you specify "Combination output 8", you can only use the outputs from "Combination output 9" and "Combination output 10" as inputs.

**Partitions**

**ABUS**
 Log out

**Partitions**

Index	Name
Partition 1	"Partition 1"
Partition 2	"Partition 2"
Partition 3	"Partition 3"
Partition 4	"Partition 4"
Full set link	Partitions: None

About

Status

Devices

Outputs

Partitions

System

Communications

Social Care

View Log

Keypad

About

Status

Devices

Outputs

Partitions

System

Communications

Social Care

View Log

Keypad

Name/function	Explanation
<b>Index</b>	List of partitions Partition 1 to partition 4 and full set link
<b>Name</b>	Name of the partition assigned during configuration. The selected partitions appear in the "Full set link" line
<b>Full set link</b>	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.

## Configure partitions



Please consult the user guide for details on activating and deactivating the system, and on the behaviour of the alarm control panel and the display (user interface). Choose a unique name for each partition, e.g. apartment, workshop, office (max. 12 characters)!

### Complete arming

Name/function	Explanation
<b>Name</b>	<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>
<b>Complete arming</b>	<p>Settings for the complete arming of the partition</p>
<b>Exit Mode</b>	<p>Select the mode of arming when exiting the premises.</p> <p>Note:</p> <p>See also user guide Chapter "8. Arming and disarming the system"</p> <p><b>Timed Set</b></p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• This option does not comply with BS8243:2010.</li> </ul>

Name/function	Explanation
Exit Mode, cont.	<p><b>Final Door Set</b></p> <ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li><li>• The alarm panel saves the start time of arming (and not the arming itself) in the log book.</li><li>• 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.</li></ul> <p><b>Instant Set</b></p> <ul style="list-style-type: none"><li>• The partition is armed immediately without any acoustic warning tone. If the partition has been armed, an acoustic confirmation sounds.</li><li>• Note: This option does not comply with BS8243:2010.</li></ul> <p><b>Silent Set</b></p> <ul style="list-style-type: none"><li>• 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.</li><li>• During entry time the acoustic warning tone can be heard.</li><li>• Note: This option does not comply with BS8243:2010.</li></ul> <p><b>Lock Set</b></p> <ul style="list-style-type: none"><li>• 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.</li></ul> <p><b>Arming the partition</b></p> <ul style="list-style-type: none"><li>• 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:<ol style="list-style-type: none"><li>a) closes the last exit door and then</li><li>b) locks the door and therefore activates the lock switch contact.</li></ol>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.</li></ul>

Name/function	Explanation
<p><b>Exit Mode, cont.</b></p>	<p><b>Disarming the partition</b></p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• To comply with BS8243, "After Entry" must be set to "Never" in order to prevent confirmation.</li> </ul> <p><b>Exit Terminate</b></p> <ul style="list-style-type: none"> <li>• Arming the partition</li> <li>• The user must first start the arming sequence. Then the user ends the arming process after existing the monitoring area.</li> <li>• 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-&gt;System-&gt;User Access-&gt;Remote Inst. Set).</li> <li>• The user ends arming by activating a zone with type "Exit Terminate" (see explanation of zone types).</li> <li>• 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.</li> <li>• Disarming the partition</li> <li>• 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.)</li> </ul> <p><b>As SA (partition) 1</b></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>
<p><b>Settle time [s]</b></p>	<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>

Name/function	Explanation
<b>Exit Time [s]</b>	This option only appears for modes "Timed Set" and "Silent Set". Time for the exit delay in seconds The exit time can be any value between 10 s and 120 s.
<b>Entry Time [s]</b>	Time for the entry delay in seconds The entry time can be any value between 10 s and 120 s.
<b>Alarm Response</b>	<p>Select the response here for when an alarm occurs in this partition.</p> <p><b>Internal</b></p> <ul style="list-style-type: none"><li>• Alarm panel, indoor siren, info module and control device.</li></ul> <p><b>Siren</b></p> <ul style="list-style-type: none"><li>• Alarm panel, indoor siren, info module and control device.</li><li>• External Sirens</li></ul> <p><b>Sirens and ESCC reporting</b></p> <ul style="list-style-type: none"><li>• Alarm panel, indoor siren, info module and control device.</li><li>• External Sirens</li><li>• Communication with ARC/ESCC</li></ul> <p>A siren delay goes into effect for alarm response "Siren + ESCC reporting".</p> <p><b>Strobe</b></p> <ul style="list-style-type: none"><li>• Alarm panel, indoor siren, info module and control device.</li><li>• Outdoor sirens (with STROBE only)</li></ul> <p><b>Strobes and ESCC reporting</b></p> <ul style="list-style-type: none"><li>• Alarm panel, indoor siren, info module and control device.</li><li>• Outdoor sirens (with STROBE only)</li><li>• Communication with ARC/ESCC</li></ul> <p>A siren delay goes into effect for alarm response "Strobe + ESCC reporting".</p> <p> Note When "Siren Delay (user-based)" is enabled (&gt; 0), the behaviour of the siren delay is as follows: Siren Delay (User) <b>only</b> affects the outdoor sirens when it comes to the following configurations: <b>Partition -&gt; Alarm reaction</b>     Sirens and ESCC reporting or     Strobes and ESCC reporting In the other variants     internal, siren and strobe this siren delay is effective for all components (alarm panel, indoor siren, information module, control panel and outdoor siren). This means that all these components only signal after the delay time has elapsed.</p> <p> Note This does not affect the voice dialler, text message, email and push notification communication methods.</p>



**Note**

regarding Partition -> Alarm reaction

The fire zone type, the fire double keys on the alarm panel and the fire double keys on the control panel **always** trigger an ARC/ESCC reporting if the call mode for ARC/ESCC reporting is enabled and if the "Fire" group is enabled for CID/SIA events.

Example:

Partition X -> Alarm reaction -> Siren  
Fire alarm transmission to ARC/ESCC

**Siren Delay [min] (ARC)**

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.

**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 will not be active when "Installer Mode->System->Confirmation->Confirmation Mode->DD243 or BS8243" and "Installer Mode->System->Confirmation->Siren On ->Unconfirm" are set.

If sounders are assigned to multiple partitions, the alarm panel uses the shortest siren delay set for the partitions in question.



**Note**

If under System -> Security, "Siren Delay (user-based)" is enabled (> 0), this menu item does **not** appear here.

And the entire behaviour of the siren delay (ARC) is blocked!



**Note**

The main purpose of the siren delay is to give communication with the ARC time and to be able to react from there, before the siren warns the intruder that the alarm has been triggered.

**The siren delay occurs when:**

Partition -> Alarm reaction -> Siren + ESCC Reporting / Flash + ESCC Reporting  
Communication ARC: yes

Confirmation -> Confirmation Mode -> Basic

Sounder On -> Confirm

Exceptions: Unconfirm see below

Siren On -> Confirm

Settings		Effect
<b>Sounder On</b>	<b>Siren On</b>	
Unconfirm	Unconfirm	<b>Unconfirmed alarm:</b> the internal sounders and sirens sound <b>constantly</b> and for the entire <i>siren time</i>

		<b>Confirmed alarm:</b> the alarm panel retriggers the sirens and internal sounder, which then sound for the entire <i>siren time</i> , even if this has previously elapsed.
Unconfirm	Confirm	<b>Unconfirmed alarm:</b> the internal sounders sound constantly and for the entire <i>siren time</i> . <i>No external sirens</i>
		<b>Confirmed alarm:</b> the alarm panel waits for a potential <b><i>siren delay</i></b> and then starts both the internal sounder and the external sirens. These both sound for the entire siren time.
Confirm	Confirm	<b>Unconfirmed alarm:</b> No sounders or sirens.
		<b>Confirmed alarm:</b> the alarm panel waits for a potential <b><i>siren delay</i></b> and then starts both the internal sounder and the external sirens. These both sound for the entire <i>siren time</i> .

### No siren delay if:

No siren delay if Unconfirm for both (factory settings). See table above.

1. The siren delay does not come into effect if the alarm reaction mode does not require any communication or if a wiring error is identified.
  2. The siren delay also does not come into effect when System Options -> Confirmation mode is set to DD243 or BS8243 OR System options -> Confirmation -> Sirens On is set to "Unconfirm".
  3. Sounders to which two or more partitions have been assigned use the shortest siren delay among the partitions assigned to the sounder.
- The siren delay is also prevented when System Options - Confirmation Mode is set to Basic and Siren On is set to "Unconfirm" (default settings). These are the default settings for the alarm panel.
- The siren delay is also prevented when the ARC communication is disarmed.

No siren delay in the case of fire alarm, panic alarm or 24h alarm.



Name/function	Explanation
<b>Ext. Siren Time [min]</b>	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 are assigned to multiple partitions, the alarm panel uses the longest siren time set for the partitions in question.  The time for which the sounders are active can also be extended to the longest siren delay for that partition.
<b>Strobe on Set</b>	<b>On</b> After successfully arming the partition, there is <b>one</b> visual acknowledgement on the wireless external siren. "Strobe" outputs are activated for 10 s after successfully arming the partition. <b>Off</b> After successfully arming the partition, there is <b>no</b> visual acknowledgement on the wireless external siren.
<b>Strobe on Unset</b>	<b>On</b> After successfully disarming the partition, there is <b>one</b> visual acknowledgement on the wireless external siren. "Strobe" outputs are activated for 10 s after successfully arming the partition. <b>Off</b> After successfully disarming the partition, there is <b>no</b> visual acknowledgement on the wireless external siren.

## Configuration

---

Name/function	Explanation
<b>Beep on Set</b>	<p><b>On</b> After successfully arming the partition, there is <b>one</b> acoustic acknowledgement on the wireless external siren. "Siren" outputs are activated for 10 s after successfully arming the partition.</p> <p><b>Off</b> After successfully arming the partition, there is <b>no</b> acoustic acknowledgement on the wireless external siren.</p>
<b>Beep on Unset</b>	<p><b>On</b> After successfully disarming the partition, there is <b>one</b> acoustic acknowledgement on the wireless external siren. "Siren" outputs are activated for 10 s after successfully arming the partition.</p> <p><b>Off</b> After successfully disarming the partition, there is <b>no</b> acoustic acknowledgement on the wireless external siren.</p>
<b>Int. siren time [min]</b>	<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. If sounders are assigned to multiple partitions, the alarm panel uses the longest siren time set for the partitions in question.</p> <p>The time for which the sounders are active can also be extended to the longest siren delay for that partition.</p> <p><b>Note</b> Internal sirens always sound after a fire or hold up alarm until the alarm is confirmed by a user for safety reasons. For safety reasons there is no time limit for a fire alarm or hold up alarm. Special response when an entry delay is used:</p> <p><b>Requirement</b></p> <ul style="list-style-type: none"><li>• The internal sounders (alarm panel, wireless indoor siren, wireless info module) are muted again after the internal siren time has expired.</li><li>• The alarm panel has automatically rearmed.</li><li>• (See also "Installer Mode → System -&gt; Security → Auto Rearm")</li></ul> <p><b>Response</b></p> <ul style="list-style-type: none"><li>• 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 <b>alarm tone</b>.</li><li>• The <b>normal entry tone</b> is <b>not signalled</b> in this case.</li></ul>

Name/function	Explanation
<p><b>Siren time int. [min], cont.</b></p>	<p><b>Note</b>            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.            The delay time runs anyway. Disarm the alarm panel within the delay time.  <b>Do so only if you feel it is safe, however. An intruder could still be inside the property!</b>            If you do not disarm the system, an additional burglar alarm is triggered once the delay time has expired.  <b>Notify others who have access to your property of this response of the alarm panel.</b></p>
<p><b>Endless</b></p>	<p><b>On</b>            Internal sirens signal the alarm tone until an alarm is acknowledged by a user.  <b>Off</b>            The time for the duration of the internal siren(s) is used.</p>

## Configure partitions

### Part Set

**ABUS**
Log out

Partitions | **Partition 1**

Name

Full Set
Part Set
Unset
HUA response

Exit Mode Exit Terminate ▼

Entry Time

Alarm Response \*Siren ▼

Ext. Siren Time

Settle Time

Siren Delay

Pt.Set Final Exit \*Final Exit ▼


Cancel
Submit

- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- Test
- View Log
- Keypad

Name/function	Explanation
<b>Name</b>	<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>
<b>Part set</b>	Settings for the internal arming of the partition
<b>Exit Mode</b>	<p>Select the mode of internal arming when exiting the premises.</p> <p>Note: See also user guide Chapter "8. Arming and disarming the system"</p> <p><b>Timed Set</b></p> <ul style="list-style-type: none"> <li>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.</li> <li>This option does not comply with BS8243:2010.</li> </ul>

Name/function	Explanation
Exit Mode, cont.	<p><b>Final Door Set</b></p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• The alarm panel saves the start time of internal arming (and not the internal arming itself) in the log book.</li> <li>• 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.</li> </ul> <p><b>Instant Set</b></p> <ul style="list-style-type: none"> <li>• The partition is internally armed immediately without any acoustic warning tone. If the partition has been internally armed, an acoustic confirmation sounds.</li> <li>• Note: This option does not comply with BS8243:2010.</li> </ul> <p><b>Silent Set</b></p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• During entry time the acoustic warning tone can be heard.</li> <li>• Note: This option does not comply with BS8243:2010.</li> </ul> <p><b>Lock Set</b></p> <ul style="list-style-type: none"> <li>• The "Lock Set" mode affects both internal arming and disarming of the partition.</li> <li>• 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.</li> </ul> <p><b>Internally arming the partition</b></p> <ul style="list-style-type: none"> <li>• 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:             <ol style="list-style-type: none"> <li>a) closes the last exit door and then</li> <li>b) locks the door and therefore activates the lock switch contact.</li> </ol>             After the lock switch contact is activated, the partition is internally 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.           </li> <li>•</li> </ul>

Name/function	Explanation
<b>Exit Mode, cont.</b>	<p><b>Disarming the partition</b></p> <ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li><li>• To comply with BS8243, "After Entry" must be set to "Never" in order to prevent confirmation.</li></ul> <p><b>Exit Terminate</b></p> <p><b>Internally arming the partition</b></p> <ul style="list-style-type: none"><li>• The user must first start the arming sequence. Then the user ends the arming process after existing the monitoring area.</li><li>• 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-&gt;System-&gt;User Access-&gt;Remote Inst. Set).</li><li>• The user ends arming by activating a zone with type "Exit Terminate" (see explanation of zone types).</li><li>• 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.</li></ul> <p><b>Disarming the partition</b></p> <ul style="list-style-type: none"><li>• 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.)</li></ul> <p><b>As SA (partition) 1</b></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
<b>Settle time [s]</b>	<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 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>
<b>Exit Time [s]</b>	<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>
<b>Entry Time [s]</b>	<p>Time for the entry delay in seconds.</p> <p>The entry time can be any value between 10 s and 120 s.</p>
<b>Alarm Response</b>	<p>Select the response here for when an alarm occurs in this partition.</p> <p><b>Internal</b></p> <ul style="list-style-type: none"> <li>• Alarm panel, indoor siren, info module and control device.</li> </ul> <p><b>Siren</b></p> <ul style="list-style-type: none"> <li>• Alarm panel, indoor siren, info module and control device.</li> <li>• External Sirens</li> </ul> <p><b>Sirens and ESCC reporting</b></p> <ul style="list-style-type: none"> <li>• Alarm panel, indoor siren, info module and control device.</li> <li>• External Sirens</li> <li>• Communication with ARC/ESCC</li> </ul> <p>A siren delay goes into effect for alarm response "Siren + ESCC reporting".</p> <p><b>Strobe</b></p> <ul style="list-style-type: none"> <li>• Alarm panel, indoor siren, info module and control device.</li> <li>• Outdoor sirens (with STROBE only)</li> </ul> <p><b>Strobes and ESCC reporting</b></p> <ul style="list-style-type: none"> <li>• Alarm panel, indoor siren, info module and control device.</li> <li>• Outdoor sirens (with STROBE only)</li> <li>• Communication with ARC/ESCC</li> </ul> <p>A siren delay goes into effect for alarm response "Strobe + ESCC reporting".</p> <p></p> <p>Note</p> <p>When "Siren Delay (user-based)" is enabled (&gt; 0), the behaviour of the siren delay is as follows:</p> <p>Siren Delay (User) <b>only</b> affects the outdoor sirens when it comes to the following configurations:</p> <p><b>Partition -&gt; Alarm reaction</b></p> <p>Sirens and ESCC reporting or</p>

### Strobes and ESCC reporting

In the other variants

internal, siren and strobe

this siren delay is effective for all components (alarm panel, indoor siren, information module, control panel and outdoor siren). This means that all these components only signal after the delay time has elapsed.



Note

This does not affect the voice dialler, text message, email and push notification communication methods.



Note

regarding Partition -> Alarm reaction



The fire zone type, the fire double keys on the alarm panel and the fire double keys on the control panel **always** trigger an ARC/ESCC reporting if the call mode for ARC/ESCC reporting is enabled and if the "Fire" group is enabled for CID/SIA events.

Example:

Partition X -> Alarm reaction -> Siren

Fire alarm transmission to ARC/ESCC



Name/function	Explanation
<p><b>Siren Delay [min] (ARC)</b></p>	<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><b>Note</b>                      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 will not be active when "Installer Mode-&gt;System-&gt;Confirmation-&gt;Confirmation Mode-&gt;DD243 or BS8243" and "Installer Mode-&gt;System-&gt;Confirmation-&gt;Siren On -&gt;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> <p>  <b>Note</b>                      Detailed information on the siren delay can be found under Siren Delay Partitions All Set.</p> <p>  <b>Note</b>                      If under System -&gt; Security, "Siren Delay (user-based)" is enabled (&gt; 0), this menu item does <b>not</b> appear here.                      And the entire behaviour of the siren delay (ARC) is blocked!</p>
<p><b>Ext. Siren Time [min]</b></p>	<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.</p> <p>The time for which the sounders are active can also be extended to the longest siren delay for that partition.</p>
<p><b>Pt.Set Final Exit</b></p>	<p>This option controls how a "Final Door" zone is handled when the system is internally armed.</p> <p><b>Final Door</b></p> <ul style="list-style-type: none"> <li>• Every zone in this partition with type "Final Door" and the attribute "Part Set" continues to function as a "Final Door" zone.</li> </ul> <p><b>Normal Alarm</b></p> <ul style="list-style-type: none"> <li>• Every zone in this partition with type "Final Door" and the attribute "Part Set" functions as a "Normal Alarm" zone.</li> </ul>

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

Name/function	Explanation
<b>Beep on Set</b>	<p><b>On</b> After successfully internally arming the partition, there is <b>one</b> acoustic acknowledgement on the wireless external siren. "Siren" outputs are activated for 10 s after successfully arming the partition.</p> <p><b>Off</b> After successfully internally arming the partition, there is <b>no</b> acoustic acknowledgement on the wireless external siren.</p>
<b>Beep on Unset</b>	<p><b>On</b> After successfully disarming the partition, there is <b>one</b> acoustic acknowledgement on the wireless external siren. "Siren" outputs are activated for 10 s after successfully arming the partition.</p> <p><b>Off</b> After successfully disarming the partition, there is <b>no</b> acoustic acknowledgement on the wireless external siren.</p>
<b>Int. siren time [min]</b>	<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. If sounders are assigned to multiple partitions, the alarm panel uses the longest siren time set for the partitions in question.</p> <p>The time for which the sounders are active can also be extended to the longest siren delay for that partition.</p> <p><b>Note</b> Internal sirens always sound after a fire or hold up alarm until the alarm is confirmed by a user for safety reasons. For safety reasons there is no time limit for a fire alarm or hold up alarm.</p> <p><b>Special response when an entry delay is used</b></p> <p><b>Requirement</b></p> <ul style="list-style-type: none"> <li>• The internal sounders (alarm panel, wireless indoor siren, wireless info module) are muted again after the internal siren time has expired.</li> <li>• The alarm panel has automatically rearmed (see also "Installer Mode → System -&gt; Security → Auto Rearm").</li> </ul> <p><b>Response</b></p> <ul style="list-style-type: none"> <li>• 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 <b>alarm tone</b>.</li> <li>• The <b>normal entry tone</b> is <b>not signalled</b> in this case.</li> </ul>

## Configuration

---

Name/function	Explanation
<b>Siren time int. [min], cont.</b>	<b>Note</b> 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. The delay time runs anyway. Disarm the alarm panel within the delay time. <b>Do so only if you feel it is safe, however. An intruder could still be inside the property!</b> If you do not disarm the system, an additional burglar alarm is triggered once the delay time has expired. <b>Notify others who have access to your property of this response of the alarm panel.</b>
<b>Endless</b>	<b>On</b> Internal sirens signal the alarm tone until an alarm is acknowledged by a user.  <b>Off</b> The time for the duration of the internal siren(s) is used.

## Configure partitions

Deactivated

Name/function	Explanation
Alarm Response	<p>Select the response here for when an alarm occurs in this partition.</p> <p><b>Internal</b></p> <ul style="list-style-type: none"> <li>Alarm panel, indoor siren, info module and control device.</li> </ul> <p><b>Siren</b></p> <ul style="list-style-type: none"> <li>Alarm panel, indoor siren, info module and control device.</li> <li>External Sirens</li> </ul> <p><b>Sirens and ESCC reporting</b></p> <ul style="list-style-type: none"> <li>Alarm panel, indoor siren, info module and control device.</li> <li>External Sirens</li> <li>Communication with ARC/ESCC</li> </ul> <p>A siren delay goes into effect for alarm response "Siren + ESCC reporting".</p> <p><b>Strobe</b></p> <ul style="list-style-type: none"> <li>Alarm panel, indoor siren, info module and control device.</li> <li>Outdoor sirens (with STROBE only)</li> </ul> <p><b>Strobes and ESCC reporting</b></p> <ul style="list-style-type: none"> <li>Alarm panel, indoor siren, info module and control device.</li> <li>Outdoor sirens (with STROBE only)</li> <li>Communication with ARC/ESCC</li> </ul>

A siren delay goes into effect for alarm response "Strobe + ESCC reporting".



Note

When "Siren Delay (user-based)" is enabled (> 0), the behaviour of the siren delay is as follows:

Siren Delay (User) **only** affects the outdoor sirens when it comes to the following configurations:

**Partition -> Alarm reaction**

Sirens and ESCC reporting or  
Strobes and ESCC reporting

In the other variants

internal, siren and strobe

this siren delay is effective for all components (alarm panel, indoor siren, information module, control panel and outdoor siren). This means that all these components only signal after the delay time has elapsed.



Note

This does not affect the voice dialler, text message, email and push notification communication methods.



Note

regarding Partition -> Alarm reaction

The fire zone type, the fire double keys on the alarm panel and the fire double keys on the control panel **always** trigger an ARC/ESCC reporting if the call mode for ARC/ESCC reporting is enabled and if the "Fire" group is enabled for CID/SIA events.

Example:

Partition X -> Alarm reaction -> Siren  
Fire alarm transmission to ARC/ESCC

### Siren Delay [min] (ARC)

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.



**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 will not be active when "Installer Mode->System->Confirmation->Confirmation Mode->DD243 or BS8243" and "Installer Mode->System->Confirmation->Siren On ->Unconfirm" are set.

If sounders are assigned to multiple partitions, the alarm panel uses the shortest siren delay set for the partitions in question.

	<p>  <b>Note</b>            Detailed information on the siren delay can be found under Siren Delay Partitions All Set.</p> <p>  <b>Note</b>            If under System -&gt; Security, "Siren Delay (user-based)" is enabled (&gt; 0), this menu item does <b>not</b> appear here.            And the entire behaviour of the siren delay (ARC) is blocked!</p>
<p><b>Siren time Ext. [min]</b></p>	<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.</p> <p>The time for which the sounders are active can also be extended to the longest siren delay for that partition.</p>

Name/function	Explanation
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. If sounders are assigned to multiple partitions, the alarm panel uses the longest siren time set for the partitions in question.</p> <p>The time for which the sounders are active can also be extended to the longest siren delay for that partition.</p> <p><b>Note</b> Internal sirens always sound after a fire or hold up alarm until the alarm is confirmed by a user for safety reasons. For safety reasons there is no time limit for a fire alarm or hold up alarm.</p> <p><b>Special response when an entry delay is used</b></p> <p><b>Requirement</b></p> <ul style="list-style-type: none"> <li>• The internal sounders (alarm panel, wireless indoor siren, wireless info module) are muted again after the internal siren time has expired.</li> <li>• The alarm panel has automatically rearmed (see also "Installer Mode → System - &gt; Security → Auto Rearm").</li> </ul> <p><b>Response</b></p> <ul style="list-style-type: none"> <li>• 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 <b>alarm tone</b>.</li> <li>• The <b>normal entry tone</b> is <b>not signalled</b> in this case.</li> </ul> <p><b>Note</b> 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. The delay time runs anyway. Disarm the alarm panel within the delay time. <b>Do so only if you feel it is safe, however. An intruder could still be inside the property!</b> If you do not disarm the system, an additional burglar alarm is triggered once the delay time has expired. Notify others who have access to your property of this response of the alarm panel.</p>
Endless	<p>On <b>Internal sirens signal the alarm tone until an alarm is acknowledged by a user.</b></p> <p>Off <b>The siren time for the duration of the internal siren(s) is used.</b></p>



## Configure partitions

### Panic response:

Name/function	Explanation
<b>Name</b>	Unique name of the partition
<b>Panic response:</b>	<p>Select here the type of signalling used for a hold up alarm in the selected partition:</p> <p><b>Audible</b></p> <ul style="list-style-type: none"> <li>• 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).</li> <li>• A triangle warning appears on the alarm panel display to indicate the hold up alarm.</li> <li>• Details are displayed after a user code is entered.</li> <li>• The acoustic alarm is muted after a user code is entered.</li> </ul> <p><b>Silent</b></p> <ul style="list-style-type: none"> <li>• The hold up alarm is only signalled using communication messages.</li> <li>• There is no audible acoustic alarm.</li> <li>• "Siren" and "Hold Up" outputs are not activated.</li> <li>• The hold up alarm is <b>not</b> shown on the alarm panel display.</li> <li>• The display only indicates the hold up alarm when a user operates the alarm panel.</li> </ul>

## Configuration

---

Name/function	Explanation
HUA response, cont.	<p data-bbox="472 197 603 230"><b>Displayed</b></p> <ul data-bbox="472 237 1458 434" style="list-style-type: none"><li data-bbox="472 237 1458 331">• 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).</li><li data-bbox="472 338 1458 434">• 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.</li></ul> <p data-bbox="472 472 536 506"><b>Note</b></p> <p data-bbox="472 512 1473 564">No hold up alarms can be triggered or communicated when the system is in installer mode.</p>

System

The screenshot displays the ABUS System Configuration interface. At the top left, the 'ABUS' logo is visible. The main content area is titled 'System' and contains several configuration options represented by icons and text labels:

- General (gear icon)
- Installer Details (person with gear icon)
- User Access (person with key icon)
- User Reset (person with refresh icon)
- Confirmation (bell with checkmark icon)
- Hardware (chip icon)
- Security Settings (shield icon)
- Backup / Restore (clock with refresh icon)
- Report (gears icon)

On the right side, there is a vertical sidebar with a 'Log out' button at the top. Below it, a list of menu items is provided, each with a small icon:

- About (person with gear icon)
- Status (house icon)
- Devices (document icon)
- Outputs (arrow icon)
- Partitions (pie chart icon)
- System (gear icon)
- Communications (phone icon)
- Social Care (bed icon)
- Test (gear icon)
- View Log (calendar icon with '18')
- Keypad (keypad icon)

**General**

System | General

**Log out**

Display Text

A/C Fail Reporting



Ext DC Fail Reporting

A/C Fail Delay (minutes)



Ext DC Fail Delay (minutes)

- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- View Log
- Keypad

Name/function	Explanation (checkbox)
<b>Language</b>	<p>Only available on the alarm panel. Select the desired language with the desired version.</p> <p> <b>Note</b> The language file must be updated BEFORE updating the application file.</p> <p>See the "S/W upgrade with new SD card files" chapter in the appendix</p>
<b>Display Text</b>	<p>Name shown on the Secvest display. Max. 20 characters From S/W 1.01.00 onwards, max. 16 characters (reason: compatibility with the ABUS server)</p>
<b>Restore defaults</b>	<p><b>Only available on the alarm panel.</b></p> <p>Factory settings staggered Factory settings</p> <p> <b>Note</b> Create a back-up copy of the configuration before resetting the alarm panel to factory settings. You can do this via the alarm panel itself or the web interface. Details on this can be found in the "Backup/restore" chapter.</p>

<p><b>Factory settings staggered</b></p>	<p><b>Only available on the alarm panel.</b></p> <p>This menu option can be used to reset parts of the programming of the alarm panel to the factory settings without affecting the entire system.</p>  <p><b>Note</b> A reset</p> <ul style="list-style-type: none"> <li>• does <b>not</b> delete the log book</li> </ul> <p>You can select one or more of the following options:</p>  <p><b>Note</b> The default factory settings values are contained in the Appendix.</p>
--	---

Option	Effect
User	<p>Deletes all users, including their codes, proximity tags, remote controls, panic alarms, medical emergency transmitters and emergency call buttons.</p> <p>After the reset you will be prompted to enter a new installer code and a new administrator code.</p> <p>This option has the same effect as using "Code Reset Pins" . See Chapter "Device overview -&gt; Device rear" for more details.</p>
Zones	<p>Resets all zones; type, partitions and attributes.</p> <p>In wireless zones, the alarm panel holds the IDs of all detectors that have already been taught in in the alarm panel.</p>
Wireless components	<p>Deletes the IDs of taught-in wireless components. Scroll through the list of components and select Yes for every type that you want to delete. Then press OK to confirm your selection.</p> <p>All components Deletes all taught-in wireless components</p> <p>Detectors Deletes only these components. The zones are also reset.</p> <p>Ext. Sirens Deletes only these components.</p> <p>Int.Sirens Deletes only these components.</p> <p>Wireless control panel Deletes only these components.</p> <p>WAM Deletes only these components.</p> <p>Door locks Deletes only these components.</p> <p>RF repeater Deletes only these components.</p>

	Outputs	Resets all outputs; type, partitions and attributes.
	Activations	Resets all activations, e.g. output mode. This applies to the “Partitions” menu and the “Time schedules active/inactive” user menu.
	System	Resets all options in the “System” menu. Resets all options in the “Configuration” user menu.   <b>Note</b> <b>Not</b> reset in the “Configuration” user menu: <ul style="list-style-type: none"> <li>• Activity monitor</li> <li>• Remote controls</li> <li>• Web Access</li> <li>• Level 4 updates</li> <li>• Time schedules enabled/disabled</li> </ul>
	<ul style="list-style-type: none"> <li>• Communication</li> </ul>	Resets all options in the “Communication” menu. Specifically also the menu “Network -> Network Setup -> Web Server Blocked/Enabled”  This also applies to the menu “System -> Security -> Level4 Updates”.
<b>Factory settings</b>	<p><b>Only available on the alarm panel.</b></p> <p>This menu item resets the device back to its factory defaults.</p>  <b>Note</b> The default factory settings values are contained in the Appendix. <p>After confirmation the following menus appear:</p> <p><b>Language</b></p> <ul style="list-style-type: none"> <li>• Deutsch x.yz – installed</li> <li>• English x.yz</li> <li>• Nederlands x.yz</li> <li>• Francais x.yz</li> <li>• Dansk x.yz</li> <li>• Svenska x.yz</li> <li>• Italiano x.yz</li> <li>• Español x.yz</li> <li>• Polski x.yz</li> <li>• ...</li> </ul> <p><b>Note</b>  Only the languages available for the corresponding article number are shown.</p> <p><b>Upgrade Panel Application</b></p> <ul style="list-style-type: none"> <li>• v2.00.00 – installed</li> </ul>	

- v2.00.00 07/10/2016 (2621440)
- v1.01.02 25/07/2016 (2293760)
- v1.01.00 16/02/2016 (2293760)
- v1.00.04 01/10/2015 (2293760)
- v1.00.02 26/05/2015 (2293760)
- ...

**Country Defaults**

- |               |               |
|---------------|---------------|
| • UK          | • Switzerland |
| • Italy       | • Austria     |
| • Spain       | • Ireland     |
| • Portugal    | • Norway      |
| • Netherlands | • Denmark     |
| • France      | • Sweden      |
| • Belgium     | • Greece      |
| • Germany     | • Luxembourg  |

**Note**

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.

The country defaults are used for the following:

All countries

Automatic time adjustment for summer/winter time (start and end of summer time, country-specific)

France

FTA (First To Alarm zone lockout) operation  
This locks the zone in which the alarm was first triggered in a partition so that it cannot trigger any further alarms/faults until the zone has been restored or the alarm control panel has been disarmed.

Denmark

PSTN modem ring tone detection  
The PSTN modem ring tone detection algorithm must allow additional time between the ring tones to establish whether the ringing has stopped. 6 s is normal, but for Denmark it is 8 s.

Netherlands

The handshake tone frequencies for Fast Format and the Scancom/Scanfast social care protocols are different in the Netherlands. Usually, the handshake tone frequencies for Fast Format are 1400 Hz/2300 Hz but they are 1600 Hz/2000 Hz in the Netherlands.

Default settings

The following factory defaults are currently affected by the country defaults, see below and the "Factory defaults" appendix.

UK

"Installer Mode -> System -> Security -> Jamming" "TAMPER PROTECTION" factory default

and

"Installer Mode -> System -> Security -> Supervision" "TAMPER PROTECTION" factory default

to fulfil PD6662:2010

All other countries, FAULT factory default

"Installer Mode -> System -> Confirmation -> Confirmation Mode" BS8243 default setting

All other countries, BASIC factory default

Germany (S/W >= 1.01.00)

"Installer Mode -> Partitions -> Partitions 1–4 -> All set -> Siren time ext. -> 3 minutes"

"Installer Mode -> Partitions -> Partitions 1–4 -> Internal set -> Siren time ext. -> 3 minutes"

All other countries and Germany (S/W < 1.01.00), 15 minutes factory default

### Access Code Length

- 4-digit user code
- 6 digit user code

#### Note

You can delete all users with the help of the this menu.

For further information, please refer to the instructions under System -> Security-> 6 digit user code.

### Wired Zone Type

- 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

### Overview

- IP address: 192.168.178.002
- DHCP: On
- Version: v1.01.00
- S/N: SECVEST###E9000139AAE
- Part No.: FUAA50000

#### Note

Here you can see an overview of the most important data for the alarm panel.




### Login

- Installer
  - Name (Web Server): <Installer names> (Code=Name)
  - Code: <Installer Code>, as assigned in the Start Wizard
- Administrator
  - Name (Web Server): <Administrator names> (Code=Name)
  - Code: <Administrator Code>, as assigned in the Start Wizard

#### Note

Here you can see an overview of the current data for this user.  
The details are described in the individual chapters.



Name/function	Explanation (checkbox)
	<p>  <b>Note</b>                      Restoring the factory defaults:</p> <ul style="list-style-type: none"> <li>• deletes all taught-in and configured components, names and saved texts and numbers</li> <li>• does <b>not</b> delete the log book</li> <li>• does <b>not</b> delete the users with their codes and components</li> <li>• Does <b>not delete the Installer Name and Installer Code</b></li> <li>• does <b>not delete individually recorded voice messages.</b> <ul style="list-style-type: none"> <li>○ To delete voice messages recorded by a user, use the “Confidence Test”. When the “Confidence Test” has started, confirm the key “0” “Load Defaults”.</li> </ul> </li> </ul> <p>  <b>Note</b>                      Proceed as follows to delete all users (installer, admin and normal users) when re-setting to factory settings.                      Immediately after completing all steps of the Factory Reset function, remove all power to the control panel (230 V / 13.8 V power supply unit and batteries). You must not exit the installer mode during this process.                      After restoring power, the alarm panel starts with the complete Start Wizard.</p> <p>  <b>Note</b>                      You can delete individual users in the user menu.                      To completely delete all users, including installers, you can use "Code Rest Pins". See Chapter "Device overview -&gt; Device rear" for more details.                      All users, all proximity tags, all remote controls and all emergency buttons are deleted in the process. After the reset you will be prompted to enter a new installer code and a new administrator code.</p>
<b>A/C Fault Reporting</b>	<p><b>Enabled</b>                      Reports that a fault has occurred with the 230 V power supply.</p> <p><b>Deactivated</b>                      Function not possible.</p>
<b>A/C Fault Delay (minutes)</b>	<p>Delay time in minutes (0–60 minutes) until the message is sent.                      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).                      Power disruptions that last less than 9 s are not reported.                      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".                      If the power disruption lasts longer than 9 s, the following occurs:</p> <ul style="list-style-type: none"> <li>• If the value is set to 0 min, a warning tone is sounded after 10 s and the alarm panel reports the failure.</li> <li>• "A/C Fault" outputs are activated.</li> <li>• If the value is set to higher than 0 min, this timer is started 10 s after the disruption occurs.</li> </ul>

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.

No errors are reported.

If the fault still exists after the end of the configured time, a warning tone sounds and the error is reported.

"A/C Fault" outputs are activated.

A user can stop the warning tone by entering their code.

The alarm panel display shows details of the warning. "General Fault" and "A/C Fault" outputs remain activated.

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.

A user can reset the alarm and the "General Fault" outputs after entering their user code.



### Note

Fault delay for ARC/ESCC reporting only applies to

- alarm panel and
- HyMo with CID 301 or SIA AT/AR

The fault communication via

- Voice dialler
- SMS
- Email
- Push

starts IMMEDIATELY.


When it comes to a PSU fault of external components

- Control panel
- Indoor sounder
- WAM
- Repeater
- HyMo

the communication

- ARC/ESCC reporting
- Voice dialler
- SMS
- Email
- Push (only "Mains Fail" (AC fault) HyMo)

starts IMMEDIATELY.

Name/function	Explanation (checkbox)
<b>Ext DC Fault Reporting</b>	<p><b>Enabled</b> Reports that a fault has occurred with the external DC power supply.</p> <p><b>Deactivated</b> Function not possible.</p>
<b>Ext DC Fault Delay (minutes)</b>	<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"> <li>• 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.</li> <li>• If the value is set to higher than 0 min, this timer is started 10 s after the disruption occurs.</li> </ul> <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> <div style="text-align: center;">  </div> <p><b>Note</b></p> <p>Fault delay for ARC/ESCC reporting only applies to</p> <ul style="list-style-type: none"> <li>• alarm panel and</li> <li>• HyMo with CID 301 or SIA AT/AR</li> </ul> <p>The fault communication via</p> <ul style="list-style-type: none"> <li>• Voice dialler</li> <li>• SMS</li> <li>• Email</li> </ul> <p>starts IMMEDIATELY.</p> <p>When it comes to a PSU fault of external components</p> <ul style="list-style-type: none"> <li>• Control panel</li> <li>• Indoor sounder</li> <li>• WAM</li> <li>• Repeater</li> <li>• HyMo</li> </ul> <p>the communication</p> <ul style="list-style-type: none"> <li>• ARC/ESCC reporting</li> <li>• Voice dialler</li> <li>• SMS</li> </ul>

## Configuration

---

- Email starts IMMEDIATELY.

Installer details

Name/function	Explanation
<b>Installer Name</b>	<p>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</p> <p><b>Use a secure name. (See security tips)</b> After the initial start-up please change the <b>default installer name (code = name)</b> to a secure user name.</p>
<b>Installer Code</b>	<p>Password for the installer on the web server, access code on the alarm panel.</p> <ul style="list-style-type: none"> <li>• No installer code is preset by default.</li> <li>• The installer code is assigned in the Start Wizard during initial commissioning.</li> </ul> <p><b>Use a secure code. (See security tips)</b></p> <p><b>Note for S/W &lt;1.01.00</b> Factory settings</p> <ul style="list-style-type: none"> <li>• 9999 (4 digit user code)</li> <li>• 999999 (6-digit user code)</li> </ul> <p>It is a good idea to change this code.</p> <p>The installer code can be used to access installer mode and perform an installer re-set. The installer code cannot be used to arm or disarm the alarm panel.</p>
<b>Confirm New Code</b>	<p>Password confirmation for the installer when entering a new code</p>

## Configuration

---

### **Installer Tel No**

The telephone number of the installer can be stored here for user reference in the event of a fault.

**User access**
Log out

**ABUS**
System | User Access

Record Memo

Social Care Key

Quick Set

User Code Req'd

Remote Inst. Set

Dual Key Function

Omit All



Quick Omit


2 Way Replies

Duress Enable

Cancel
Submit

About
Status
Devices
Outputs
Partitions
System
Communications
Social Care
View Log
Keypad

Name/function	Explanation (checkbox)
<b>Record Memo</b>	<p><b>Enabled</b> Allows the user to record a memo message. Menu -&gt; Voice Memo</p> <p><b>Deactivated</b> Function not possible.</p>
<b>Dual Key Function</b>	<p><b>Enabled</b> 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.</p> <p> <b>Danger</b> S/W &gt;= 2.01.08 You are using the <b>touch</b> front on the alarm system. The backlighting is set to "When active" and the backlighting is <b>dark</b>. The <b>backlighting</b> is <b>first</b> activated when a key has been touched (first touch). <b>No</b> other <b>action</b> results from this "first touch". The keypad functions as <b>normal</b> from the <b>second</b> touch on. For details, see the user guide section 10.5.1 Functions - backlighting.</p> <p></p>

	<p>Note regarding Partition -&gt; Alarm reaction The fire zone type, the fire double keys on the alarm panel and the fire double keys on the control panel <b>always</b> trigger an ARC/ESCC reporting if the call mode for ARC/ESCC reporting is enabled and if the "Fire" group is enabled for CID/SIA events. Example: Partition X -&gt; Alarm reaction -&gt; Siren Fire alarm transmission to ARC/ESCC</p> <p><b>Deactivated</b> Function not possible.</p>
<b>Social Care Key</b>	<p><b>Enabled</b> Manual triggering of a social care alarm is possible by simultaneously pressing the corresponding dual keys on the alarm system or control device.</p> <p></p> <p><b>Danger</b> S/W &gt;= 2.01.08 You are using the <b>touch</b> front on the alarm system. The backlighting is set to "When active" and the backlighting is <b>dark</b>. The <b>backlighting</b> is <b>first</b> activated when a key has been touched (first touch). <b>No</b> other <b>action</b> results from this "first touch". The keypad functions as <b>normal</b> from the <b>second</b> touch on. For details, see the user guide section 10.5.1 Functions - backlighting.</p> <p><b>Deactivated</b> Function not possible.</p>
<b>Omit All</b>	<p><b>Enabled</b> All open zones can be omitted manually together when the alarm panel is armed.</p> <p><b>Deactivated</b> Open zones must be individually omitted manually when the alarm panel is armed.</p>



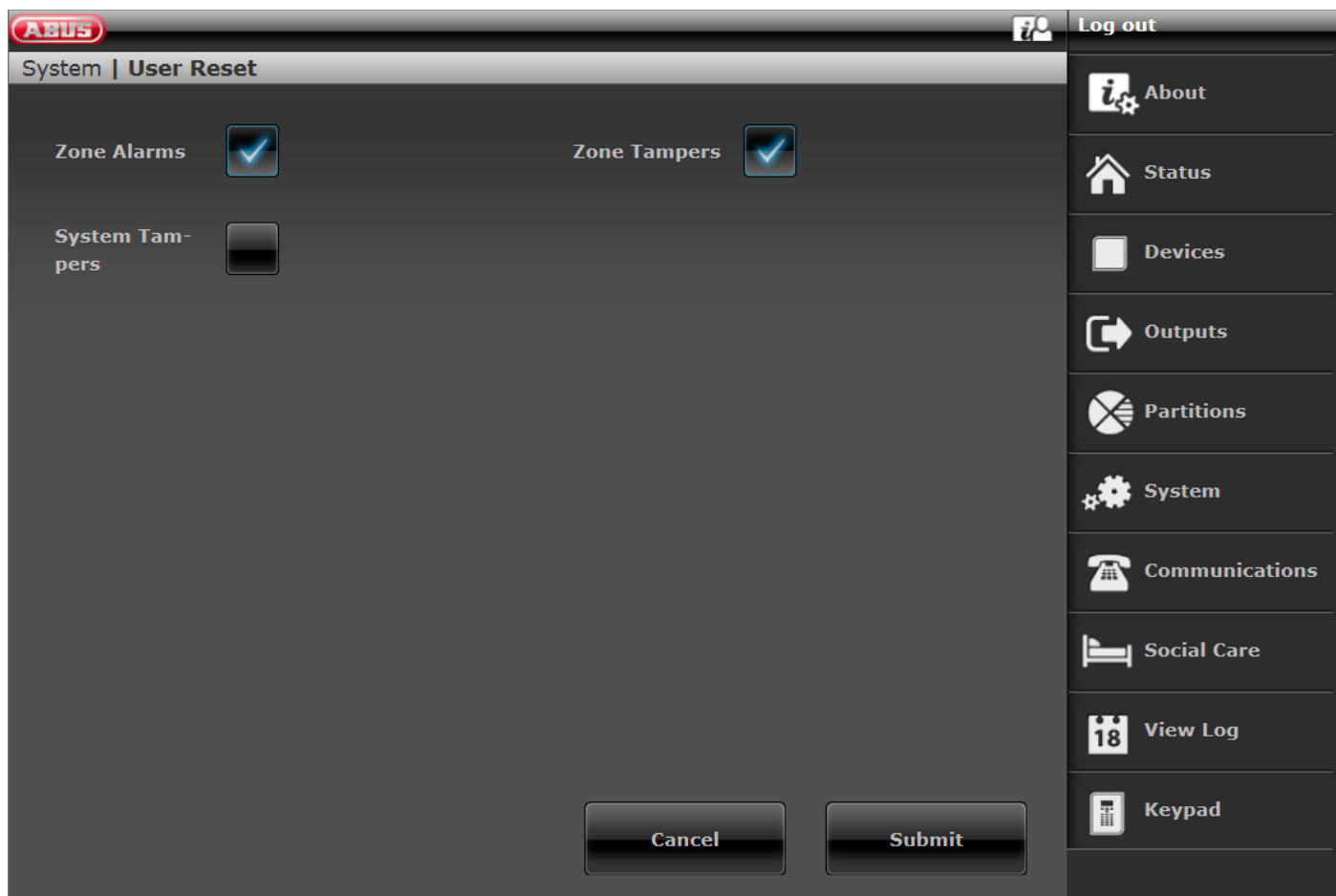
Name/function	Explanation (checkbox)
<b>Quick Set</b>	<p><b>Enabled</b> Alarm system can be armed using the symbol keys without entering the user code first.</p> <p><b>Deactivated</b> Alarm system can only be armed after the user code has been entered.</p>
<b>Quick Omit</b>	<p><b>Enabled</b> Open zones are automatically omitted when the alarm system is armed (if the zone attributes for omission allow).</p> <p><b>Deactivated</b> Open zones must be manually omitted when the alarm system is armed.</p>
<b>User Code Req'd</b>	<p>Use this option to ensure that an installer only has access to the system when a user is present.</p> <p><b>Activated / J (factory default)</b> 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><b>Alarm panel</b> Installer Mode -&gt; System -&gt; User Access -&gt; User Code Required J (factory default)</p> <p><b>Deactivated</b> The installer can access installer mode after entering their code; no additional user code is required.</p> <p><b>Note</b> The "Disarmed/No" setting is <b>not</b> compliant with EN50131.</p> <p>The factory default is required to be compliant, i.e. Level 2 users must be awarded Level 3 user access (Installer). EN 50131-1, chapter 8.3.1 access levels (with reference to EN 50131-3, chapter 8.3.1 access levels (AL)) "Access to access level 3 must be prevented unless either a) -&gt;access was enabled by a user with access level 2 or b) -&gt; ...."</p> <p>The "Disarmed/No" setting <b>only</b> complies with BS8243 when the user has provided written consent.</p>
<b>2 Way Replies</b>	<p><b>Enabled</b> 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><b>Deactivated</b> 2 Way Replies are deactivated.</p>

## Configuration

---



Name/function	Explanation (checkbox)
<b>Remote Inst. Set</b>	<p><b>Use this option to decide whether the alarm panel is armed or internally armed after the remote control is operated.</b></p> <p><b>Enabled</b> 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><b>Deactivated</b> The possible partitions are armed or internally armed according to the set exit mode.</p>
<b>Duress Enable</b>	<p><b>Enabled</b> The administrator has the option of creating a "Duress Code User". The system can be armed or disarmed using a duress code.</p> <p><b>Important</b> 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"><li>• The configured communication for duress is started.</li><li>• <b>No</b> sounders are activated.</li><li>• The alarm panel siren is <b>not</b> activated, and no triangle warning appears on the display.</li></ul> <p>The alarm panel can also be rearmed or internally armed again using . 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><b>Deactivated</b> There is no option to create a "Duress Code User".</p>




User Reset



Name/function	Explanation (checkbox)
	<p><b>These menus determine the circumstances under which a user or installer can reset the system after an alarm or after tampering.</b></p>
<p><b>Zone Alarms</b></p>	<p><b>Enabled</b> Allows the user to reset this alarm triggered for zones or detectors.</p> <p><b>Deactivated</b> User cannot perform a reset. The installer must reset the system after an alarm.</p>
<p><b>Zone Tamperers</b></p>	<p><b>Enabled</b> Allows the user to reset tamper alarms triggered for zones or detectors.</p> <p><b>Deactivated</b> User cannot perform a reset. The installer must reset the system. This setting is required for INCERT certification.</p>
<p><b>System Tamperers</b></p>	<p><b>Enabled</b> Allows the user to reset tamper alarms that affect the system.</p> <p><b>Deactivated</b> User cannot perform a reset. The installer must reset the system. This setting is required for INCERT certification.</p> <p>System tamperers can be caused by:</p> <ul style="list-style-type: none"> <li>• housing and wall tamper switches on the alarm panel</li> <li>• housing and wall tamper switches on control devices</li> <li>• tampering with connected wired sirens when the voltage at terminal TR is higher than approx. 3 V</li> <li>• jamming or supervision when set to "Tamper"</li> </ul>


## Confirmation

Name/function	Explanation (checkbox)
Conf. Mode	<p> <b>Note</b> Also follow the detailed information provided for the siren delay. This can be found under Siren Delay Partitions All Set.</p> <p> <b>Note</b> Confirmation mode functions only when alarm reaction is set to “Sirens and ESCC reporting” (see configuring partitions).</p> <p>Dropdown selection field for:</p> <ul style="list-style-type: none"> <li>• Basic           <ul style="list-style-type: none"> <li>○ When you select this option, the alarm panel activates an output that is configured as a “confirmed alarm” when a second zone is activated while the system is in alarm status. The second zone must belong to the partition in which the alarm has occurred. The installer can also choose whether the user can reset the system after a zone alarm.</li> <li>○ For the “basic” confirmation mode, the administrator can activate or deactivate the intrusion functions for all remote controls via “User menu - configuration - remote controls - intrusion functions”.</li> </ul> </li> </ul>


	<ul style="list-style-type: none"> <li>○ Note: Confirmed panic alarm is not available in the basic confirmation mode.</li> <li>• DD243</li> <li>• BS8243</li> </ul>  <p><b>Note</b> The DD243 and BS8243 settings are only relevant for the UK (United Kingdom). When selecting these options, detailed knowledge of these guidelines is required.</p>
<b>Sounder On</b>	<p>Dropdown selection field for:</p> <ul style="list-style-type: none"> <li>• Unconfirm <ul style="list-style-type: none"> <li>○ The system is armed. The alarm panel will now arm all internal sounders when an unconfirmed alarm occurs.</li> </ul> </li> <li>• Confirm <ul style="list-style-type: none"> <li>○ The system is armed. The alarm panel will now not arm any internal sounders until a confirmed alarm occurs.</li> </ul> </li> </ul> <p><b>Note</b> The alarm panel does not allow the following configuration: Siren on – confirm and sirens on – do not confirm</p>
<b>Siren On</b>	<p>Dropdown selection field for:</p> <ul style="list-style-type: none"> <li>• Unconfirm <ul style="list-style-type: none"> <li>○ The alarm panel triggers the external sirens for all alarms and overrides any siren delay.</li> </ul> </li> <li>• Confirm <ul style="list-style-type: none"> <li>○ The system is armed. The alarm panel will now not arm any sirens until a confirmed alarm occurs.</li> </ul> </li> </ul>  <p><b>Note</b> The alarm panel does not allow the following configuration: Siren on – do not confirm and sirens on – confirm</p>
<b>Confirmation Time</b> (for confirmation mode DD243 and BS8243 only.)	<p>Input field for the confirmation time for burglar alarms in minutes. The confirmation time can be set to between 1 and 60 minutes.</p>  <p><b>Note</b> Confirmation times &lt; 30 minutes do not meet the requirements set out in DD243 and BS8243.</p>
<b>Entry Keypad Lock</b> (for confirmation mode DD243 and BS8243 only.)	<p><b>Enabled</b> 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).</p> <p><b>Deactivated</b> 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).</p>
<b>Unconfirmed Reset</b> (for confirmation mode DD243 and BS8243 only.)	<p>Dropdown selection field for:</p> <ul style="list-style-type: none"> <li>• Installer</li> <li>• User</li> </ul>
<b>After Entry</b>	<p>Dropdown selection field for:</p> <ul style="list-style-type: none"> <li>• Never</li> </ul>

## Configuration

---

(for confirmation mode DD243 and BS8243 only.)	<ul style="list-style-type: none"><li>• 2 zones (DD243 only)</li><li>• 1 zone</li></ul>
<b>Confirmed Reset</b> (for confirmation mode DD243 and BS8243 only.)	Dropdown selection field for: <ul style="list-style-type: none"><li>• Installer</li><li>• User</li></ul>
<b>Confirmation Time Panic alarm</b> (for confirmation mode BS8243 only.)	Input field for the confirmation time for hold up alarms in hours.  <b>Note</b>  As per BS8243 confirmation time must be set to between 8 and 20 hours.
<b>Tamp as Tamp-Only</b> (for confirmation mode BS8243 only.)	<b>Enabled</b> <b>Deactivated</b>

**Hardware**











ABUS  Log out

System | Hardware

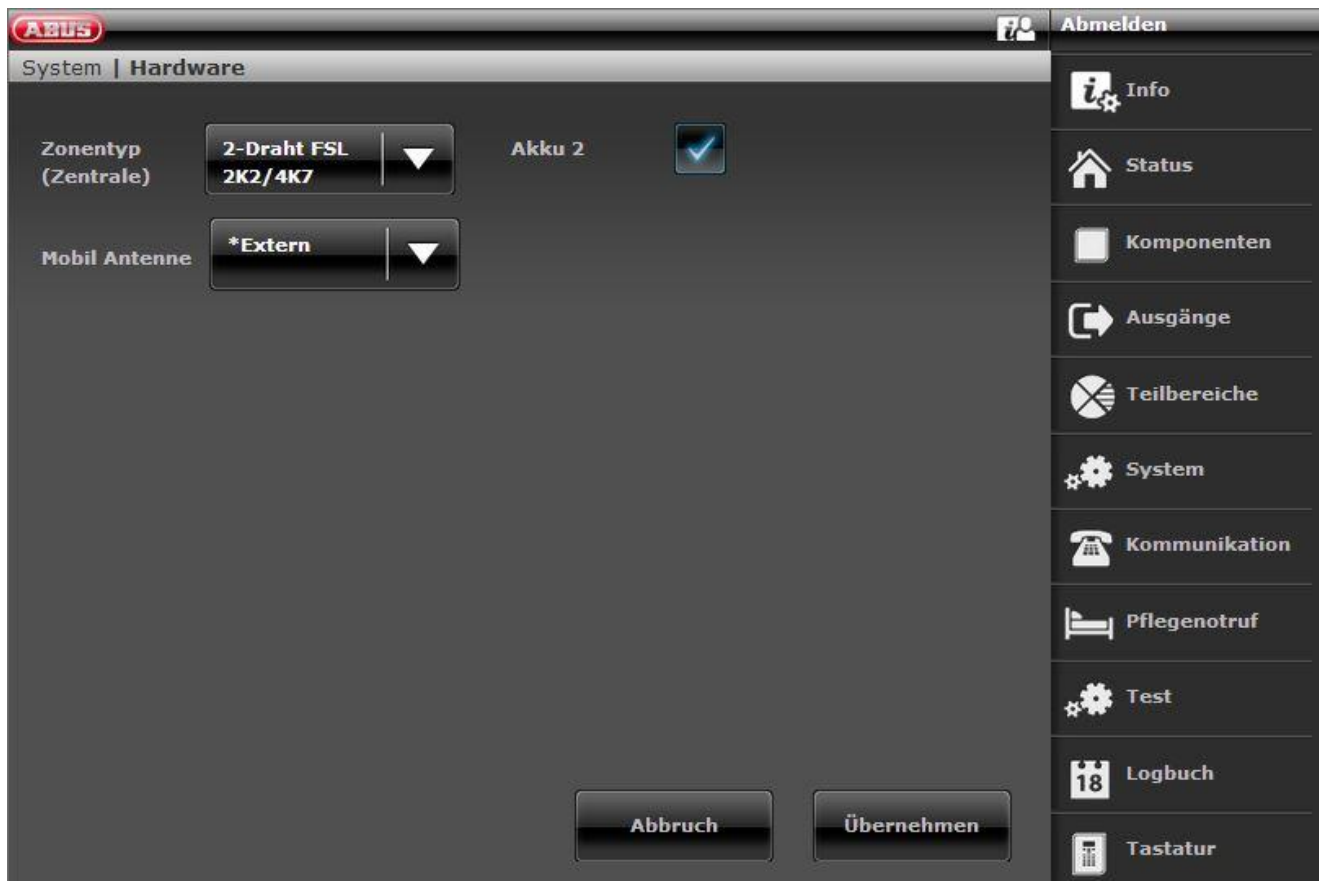
Zone Type (Panel) **Don't change** ▼ RF Siren Options **\*Siren+Strobe** ▼

Battery 2

**Cancel** **Submit**



-  About
-  Status
-  Devices
-  Outputs
-  Partitions
-  System
-  Communications
-  Social Care
-  **18** View Log
-  Keypad

SW >= 2.00.00



Name/function	Explanation (checkbox)
<b>Zone type (alarm panel)</b> <b>Wired Zone Type</b>	Dropdown selection field for: Use of inputs for wired zones <ul style="list-style-type: none"> <li>• Don't change</li> <li>• 2-wire FSL 2k2/4k7</li> <li>• 2-wire FSL 1k/1k</li> <li>• 2-wire FSL 2k/2k</li> <li>• 2-wire FSL 4k7/4k7</li> <li>• 4-wire CC</li> <li>• 2-wire CC</li> </ul>
<b>RF Siren Options</b>	<b>S/W &lt; 2.00.00</b> Dropdown selection field for: Siren configuration. Select here how the wireless siren responds to fire alarms, burglar alarms and hold up alarms. <ul style="list-style-type: none"> <li>• Siren+Strobe The wireless siren operates the siren and strobe when an alarm is triggered.</li> <li>• Strobe The wireless siren operates only the strobe when an alarm is triggered.</li> </ul> <b>S/W &gt;= 2.00.00</b> See Partitions -> Alarm Response
<b>Battery 2</b>	You have connected a second battery. Use this option to enable or block warning messages from being issued. <b>Activated / enabled</b> The alarm panel displays warning messages when battery 2 is missing or has low voltage. <b>Deactivated / blocked</b> The alarm panel ignores the presence or absence of the second additional battery.



Name/function	Explanation (checkbox)
<p><b>SD Card</b></p>	<p>Only available on the alarm panel.</p> <p><b>Safely Remove Hardware</b></p> <ul style="list-style-type: none"> <li>• Any ongoing read or write operations are stopped properly.</li> <li>• The SD card can then be safely removed.</li> </ul> <p><b>Enable Hardware</b></p> <ul style="list-style-type: none"> <li>• After insertion, the SD card is brought into operation again.</li> <li>• Read and write operations can run again.</li> </ul> <p>  <b>Danger</b>  <b>Data protection</b>  <b>Follow the SD card instructions in the "Decommissioning the alarm panel" chapter.</b></p>
<p><b>GSM antenna</b>  <b>Mobile antenna</b></p>	<p>The menu only appears when a GSM / wireless mobile module is installed.</p> <p><b>Internal</b></p> <ul style="list-style-type: none"> <li>• The antenna located directly on the wireless mobile module is used</li> </ul> <p><b>External</b></p> <ul style="list-style-type: none"> <li>• The antenna connected to the antenna connection of the wireless mobile module is used</li> </ul> <p>  <b>Danger</b>            External must be used for the additional installation of the WI-FI module.            The internal wireless mobile antenna on the PCB can affect or completely suppress the connection of the Wi-Fi signal.</p>

# Configuration

## Security settings

SW < 3.01.11

The screenshot shows the 'Security Settings' configuration page for an ABUS system. The interface is dark-themed. At the top left is the 'ABUS' logo. The title bar reads 'System | Security Settings'. A 'Log out' button with a user icon is in the top right. The main area contains two columns of settings:

- Supervision:** \*Fault (dropdown)
- Tamper Omit:**
- Remote Unset Full Set:** \*Always (dropdown)
- Ctrl Device Unset Full Set:** \*Always (dropdown)
- Auto Rearm:** \*Never (dropdown)
- Abort Time (seconds):** 120 (text input)
- Broadcast Panel Status:**
- RF Jamming:** \*Fault (dropdown)
- Force Set:** \*Off (dropdown)
- Remote Unset Part Set:** \*Always (dropdown)
- Ctrl Device Unset Part Set:** \*Always (dropdown)
- Silence Alerts:** \*User Code (dropdown)
- Entry Alarm Delay:**
- Remote Updates:**

At the bottom are 'Cancel' and 'Submit' buttons. On the right is a sidebar menu with the following items:

- Log out
- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- View Log
- Keypad

SW >= 3.01.11

**ABUS** Log out

System | Security Settings

**Panel** | Devices

RF Supervision	<b>*Fault</b> ▼	RF Jamming	<b>*Fault</b> ▼
Tamper Omit	<input type="checkbox"/>	Force Set	<b>*Off</b> ▼
Auto Rearm	<b>*Always</b> ▼	Silence Alerts	<b>*User Code</b> ▼
Abort Time (seconds)	120	Entry Alarm Delay	<input checked="" type="checkbox"/>
Broadcast Panel Status	<input checked="" type="checkbox"/>	Level4 Updates	<input checked="" type="checkbox"/>

- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- Test
- View Log
- Keypad


**ABUS** Log out

System | Security Settings

Panel | **Devices**

Camera Supervision	<b>*Fault</b> ▼	Siren Delay (User)	0
Remote Unset Full Set	<b>*Always</b> ▼	Remote Unset Part Set	<b>*Always</b> ▼
Ctrl Device Unset Full Set	<b>*Always</b> ▼	Ctrl Device Unset Part Set	<b>*Always</b> ▼

- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- Test
- View Log
- Keypad

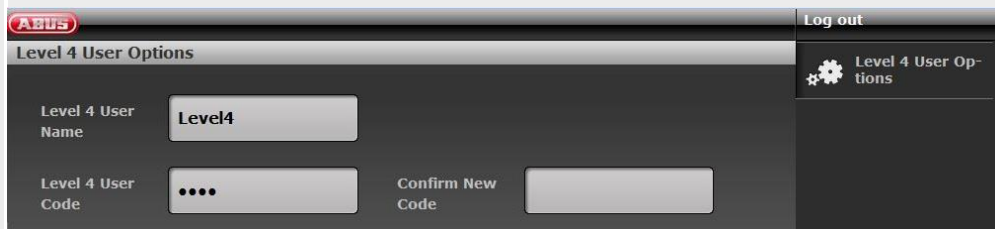
Name/function	Explanation (checkbox)															
<b>6 digit user code</b>	<p><b>Note:</b>  <b>From S/W 1.01.00 onwards</b>, this menu item no longer exists. It is only possible to decide between 4 Digit User Codes and 6 Digit User Codes in the Start Wizard. It is no longer possible to change the length of the code once the wizard has been completed.</p> <p><b>Enabled</b>            6-digit numerical code for installer and user</p> <p><b>Deactivated</b>            4-digit numerical code for installer and user</p> <p> <b>Note</b></p> <ul style="list-style-type: none"> <li>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".</li> <li>Switching from 6 to 4 digits                When switching from 6 to 4-digit numerical codes, all codes are reset. 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 also deleted)</li> </ul>															
Name/function	Explanation (checkbox)															
<b>RF Supervision</b>	<p><b>Dropdown selection field for alarm system response for RF supervision</b>            If a wireless detector has had no contact with the alarm control 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.</p> <p>If a wireless detector has had no contact with the alarm panel for more than 2 h, corresponding processes are activated as follows:</p> <table border="1" data-bbox="475 1532 1455 1998"> <thead> <tr> <th></th> <th>Alarm panel is armed</th> <th>Alarm panel is disarmed</th> </tr> </thead> <tbody> <tr> <td><b>Disabled</b></td> <td>No response</td> <td>No response</td> </tr> <tr> <td><b>Fault</b></td> <td> <ul style="list-style-type: none"> <li>Log book entry of this event</li> <li><b>No</b> display and no warning tones</li> <li>"RF Supervision" or "RF Fault" outputs are activated</li> <li>Supervision is reported</li> </ul> </td> <td> <ul style="list-style-type: none"> <li>Log book entry of this event</li> <li>Display and warning tones</li> <li>"RF Supervision" or "RF Fault" outputs are activated</li> <li>Supervision is reported</li> </ul> </td> </tr> <tr> <td><b>Tamper Activated</b></td> <td> <ul style="list-style-type: none"> <li>Log book entry of this event</li> <li>Tampering alarm</li> <li>Supervision is reported</li> </ul> </td> <td> <ul style="list-style-type: none"> <li>Log book entry of this event</li> <li>Tampering alarm</li> <li>Supervision is reported</li> </ul> </td> </tr> <tr> <td></td> <td><b>Note:</b></td> <td><b>Note</b></td> </tr> </tbody> </table>		Alarm panel is armed	Alarm panel is disarmed	<b>Disabled</b>	No response	No response	<b>Fault</b>	<ul style="list-style-type: none"> <li>Log book entry of this event</li> <li><b>No</b> display and no warning tones</li> <li>"RF Supervision" or "RF Fault" outputs are activated</li> <li>Supervision is reported</li> </ul>	<ul style="list-style-type: none"> <li>Log book entry of this event</li> <li>Display and warning tones</li> <li>"RF Supervision" or "RF Fault" outputs are activated</li> <li>Supervision is reported</li> </ul>	<b>Tamper Activated</b>	<ul style="list-style-type: none"> <li>Log book entry of this event</li> <li>Tampering alarm</li> <li>Supervision is reported</li> </ul>	<ul style="list-style-type: none"> <li>Log book entry of this event</li> <li>Tampering alarm</li> <li>Supervision is reported</li> </ul>		<b>Note:</b>	<b>Note</b>
	Alarm panel is armed	Alarm panel is disarmed														
<b>Disabled</b>	No response	No response														
<b>Fault</b>	<ul style="list-style-type: none"> <li>Log book entry of this event</li> <li><b>No</b> display and no warning tones</li> <li>"RF Supervision" or "RF Fault" outputs are activated</li> <li>Supervision is reported</li> </ul>	<ul style="list-style-type: none"> <li>Log book entry of this event</li> <li>Display and warning tones</li> <li>"RF Supervision" or "RF Fault" outputs are activated</li> <li>Supervision is reported</li> </ul>														
<b>Tamper Activated</b>	<ul style="list-style-type: none"> <li>Log book entry of this event</li> <li>Tampering alarm</li> <li>Supervision is reported</li> </ul>	<ul style="list-style-type: none"> <li>Log book entry of this event</li> <li>Tampering alarm</li> <li>Supervision is reported</li> </ul>														
	<b>Note:</b>	<b>Note</b>														

	<p>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>	<p>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>												
<p><b>Camera supervision</b></p>	<p><b>Dropdown selection field for alarm system response for IP camera supervision</b></p> <p>If a camera has had no contact with the alarm panel for longer than the reaction time, the alarm panel creates a log entry and indicates a warning (e.g. IP Zone Missing, IP-Zone Timeout).</p> <p>For reaction time, see: Components -&gt; IP zones -&gt; Add/delete -&gt; Reaction time</p> <p>Corresponding processes are activated as follows:</p> <table border="1" data-bbox="520 1086 1528 1489"> <thead> <tr> <th></th> <th>Alarm panel is armed</th> <th>Alarm panel is disarmed</th> </tr> </thead> <tbody> <tr> <td><b>Disabled</b></td> <td>No response</td> <td>No response</td> </tr> <tr> <td><b>Fault</b></td> <td> <ul style="list-style-type: none"> <li>Log book entry of this event</li> <li><b>No</b> display and no warning tones</li> </ul> </td> <td> <ul style="list-style-type: none"> <li>Log book entry of this event</li> <li>Display and warning tones</li> </ul> </td> </tr> <tr> <td><b>Tamper Activated</b></td> <td> <ul style="list-style-type: none"> <li>Tampering alarm</li> <li>Supervision is reported</li> </ul> </td> <td> <ul style="list-style-type: none"> <li>Tampering alarm</li> <li>Supervision is reported</li> </ul> </td> </tr> </tbody> </table>			Alarm panel is armed	Alarm panel is disarmed	<b>Disabled</b>	No response	No response	<b>Fault</b>	<ul style="list-style-type: none"> <li>Log book entry of this event</li> <li><b>No</b> display and no warning tones</li> </ul>	<ul style="list-style-type: none"> <li>Log book entry of this event</li> <li>Display and warning tones</li> </ul>	<b>Tamper Activated</b>	<ul style="list-style-type: none"> <li>Tampering alarm</li> <li>Supervision is reported</li> </ul>	<ul style="list-style-type: none"> <li>Tampering alarm</li> <li>Supervision is reported</li> </ul>
	Alarm panel is armed	Alarm panel is disarmed												
<b>Disabled</b>	No response	No response												
<b>Fault</b>	<ul style="list-style-type: none"> <li>Log book entry of this event</li> <li><b>No</b> display and no warning tones</li> </ul>	<ul style="list-style-type: none"> <li>Log book entry of this event</li> <li>Display and warning tones</li> </ul>												
<b>Tamper Activated</b>	<ul style="list-style-type: none"> <li>Tampering alarm</li> <li>Supervision is reported</li> </ul>	<ul style="list-style-type: none"> <li>Tampering alarm</li> <li>Supervision is reported</li> </ul>												

## Configuration

Name/function	Explanation (checkbox)												
<b>RF Jamming</b>	<p>Dropdown selection field for alarm system response for jamming:</p> <p>The alarm panel can detect jamming of wireless signals. Corresponding processes are activated as follows:</p> <table border="1" data-bbox="474 398 1461 969"> <thead> <tr> <th></th> <th>Alarm panel is armed</th> <th>Alarm panel is disarmed</th> </tr> </thead> <tbody> <tr> <td><b>Disabled</b></td> <td>No response</td> <td>No response</td> </tr> <tr> <td><b>Fault</b></td> <td> <ul style="list-style-type: none"> <li>Log book entry of this event</li> <li><b>No</b> display and no warning tones</li> </ul> </td> <td> <ul style="list-style-type: none"> <li>Log book entry of this event</li> <li>Display and warning tones</li> </ul> </td> </tr> <tr> <td><b>Tamper Activated</b></td> <td> <ul style="list-style-type: none"> <li>Tampering alarm</li> <li>Jamming is reported</li> </ul> <p><b>Note:</b> 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> </td> <td> <ul style="list-style-type: none"> <li>Tampering alarm</li> <li>Jamming is reported</li> </ul> <p><b>Note</b> 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> </td> </tr> </tbody> </table> <p><b>Note</b> 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 -&gt; User Reset -&gt; System Tamper = No the user cannot reset the system.</p>		Alarm panel is armed	Alarm panel is disarmed	<b>Disabled</b>	No response	No response	<b>Fault</b>	<ul style="list-style-type: none"> <li>Log book entry of this event</li> <li><b>No</b> display and no warning tones</li> </ul>	<ul style="list-style-type: none"> <li>Log book entry of this event</li> <li>Display and warning tones</li> </ul>	<b>Tamper Activated</b>	<ul style="list-style-type: none"> <li>Tampering alarm</li> <li>Jamming is reported</li> </ul> <p><b>Note:</b> 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"> <li>Tampering alarm</li> <li>Jamming is reported</li> </ul> <p><b>Note</b> 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>
	Alarm panel is armed	Alarm panel is disarmed											
<b>Disabled</b>	No response	No response											
<b>Fault</b>	<ul style="list-style-type: none"> <li>Log book entry of this event</li> <li><b>No</b> display and no warning tones</li> </ul>	<ul style="list-style-type: none"> <li>Log book entry of this event</li> <li>Display and warning tones</li> </ul>											
<b>Tamper Activated</b>	<ul style="list-style-type: none"> <li>Tampering alarm</li> <li>Jamming is reported</li> </ul> <p><b>Note:</b> 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"> <li>Tampering alarm</li> <li>Jamming is reported</li> </ul> <p><b>Note</b> 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>											
<b>Level4 updates</b>	<p>Alarm panel Installer Mode -&gt; System -&gt; Security -&gt; Level4 Updates -&gt; Blocked*/Enabled</p> <p>WBI Installer Mode -&gt; System -&gt; Security Settings -&gt; Level4 Updates -&gt; Blocked (deactivated, not ticked)*/Enabled (activated, ticked)</p> <p>Blocked (deactivated – not ticked)* Enabled (activated – ticked)</p> <p>If this option is activated, a new Level 4 code must be entered. This is only the case if this Level 4 code was never programmed to begin with (as delivered or since the last reset to the factory defaults). This Level 4 code has the same number of digits as the Installer code or the User code.</p> <p>Enter a "New Level 4 code" and "Confirm Level 4 code" (enter the code again to confirm it). A new user is added automatically. See "User" menu. Name: "Level4" Note: <b>For security reasons, you should change the "Level4" default name of the Level 4 user.</b> The user themselves or the administrator can change the name of this user.</p>												

If the Level 4 code is then used for accessing the alarm control panel, only the following menu options appear  
 Level 4 User Name  
 Level 4 User Code  
 to allow the user to change the name and code.



See "S/W Upgrade" appendix. You will find details about the S/W upgrade process there.

**Tamper Omit**


**If a user omits a zone, it may be necessary to also omit the associated tamper circuit for this zone.**

**Enabled**

The tamper contact is also omitted within an omitted zone.

**Deactivated**

The tamper contact continues to be monitored within an omitted zone.

Name/function	Explanation (checkbox)
<b>Force Set</b>	<p><b>S/W &gt;= 3.01.16</b></p> <p>The setting for Force Set (off, confirm or on) now applies to all activation components (e.g. remote control, control panel, additional door lock, Secvest key) and to all warnings which do not prevent activation (i.e. warnings which can be ignored).</p> <p>Faults which could prevent activation:</p> <ul style="list-style-type: none"><li>• Component no longer functions<ul style="list-style-type: none"><li>○ between 20 min and 120 min, signalisation via RF warning</li><li>○ &gt; 120 min, signalisation via supervision fault, always prevents activation</li></ul></li><li>• other faults, e.g. power supply faults or empty batteries</li><li>• Open zones<ul style="list-style-type: none"><li>○ Always prevent activation</li><li>○ Special behaviour with the zone attribute "<b>Force Set Omit</b>"</li></ul></li></ul> <p></p> <p><b>Note</b></p> <p>All activations on the alarm panel occur via code input and menu interaction. Quick activation bypasses but logs warnings on the display. Operation via app is a form of quick activation.</p> <p><b><u>Component no longer functions</u></b></p> <ul style="list-style-type: none"><li>• <b>Off</b></li></ul> <p>Activation without limitation and warning is possible less than 20 min after failure of a component.</p> <p>The alarm panel detects an RF warning from a component in between 20 min and 120 min. The behaviour during an activation attempt is then as follows:</p> <p>Alarm panel</p> <ul style="list-style-type: none"><li>Activation process begins</li><li>RF warning is displayed</li><li>OK is actuated (user noticed the warning and bypasses it)</li><li>Alarm panel is active</li></ul> <p>Remote control, control panel, additional door lock, Secvest key</p> <ul style="list-style-type: none"><li>Component is actuated</li><li>Fault message on the component corresponding to the component</li><li>Alarm panel cannot be activated</li></ul> <p><b>Note:</b></p> <p>In the event of a fault, the alarm panel can only be activated at the alarm panel itself.</p> <p><b>Special case supervision fault &gt;120 min</b></p> <p>Alarm panel, remote control, control panel, additional door lock, Secvest key</p> <ul style="list-style-type: none"><li>Fault message on the component corresponding to the component</li><li>Alarm panel cannot be activated</li></ul> <ul style="list-style-type: none"><li>• <b>Confirm</b></li></ul>



Activation without limitation and warning is possible less than 20 min after failure of a component.

The alarm panel detects an RF warning from a component in between 20 min and 120 min. The behaviour during an activation attempt is then as follows:

Alarm panel

- Activation process begins
- RF warning is displayed
- OK is actuated (user noticed the warning and bypasses it)
- Alarm panel is active

Remote control, control panel, additional door lock, Secvest key

- Component is actuated
- Fault message on the component corresponding to the component
- The alarm panel is not activated
- The component is actuated for a **second time**
- Alarm panel is now active

**Special case supervision fault >120 min**

Alarm panel, remote control, control panel, additional door lock, Secvest key

- Fault message on the component corresponding to the component
- Alarm panel cannot be activated

• **On**

Activation without limitation and warning is possible less than 20 min after failure of a component.

The alarm panel detects an RF warning from a component in between 20 min and 120 min. The behaviour during an activation attempt is then as follows:

Alarm panel

- Activation process begins
- RF warning is displayed
- OK is actuated (user noticed the warning and bypasses it)
- Alarm panel is active

Remote control, control panel, additional door lock, Secvest key

- Component is actuated
- Alarm panel is now immediately active

**Note:**

In the case of **Force Set = On**, the user is not informed about the fault on these components. However, the faults and the override are documented in the logbook.

**Special case supervision fault >120 min**

Alarm panel, remote control, control panel, additional door lock, Secvest key

- Fault message on the component corresponding to the component
- Alarm panel cannot be activated

**Other faults**

• **Off**

The behaviour during an activation attempt is as follows:

### Alarm panel

Activation process begins  
Fault is displayed  
OK is actuated (user noticed the warning and bypasses it)  
Alarm panel is active

Remote control, control panel, additional door lock, Secvest key

Component is actuated  
Fault message on the component corresponding to the component  
Alarm panel cannot be activated

#### **Note:**

In the event of a fault, the alarm panel can only be activated at the alarm panel itself.

### • **Confirm**

The behaviour during an activation attempt is as follows:

### Alarm panel

Activation process begins  
Fault is displayed  
OK is actuated (user noticed the warning and bypasses it)  
Alarm panel is active

Remote control, control panel, additional door lock, Secvest key

Component is actuated  
Fault message on the component corresponding to the component  
The alarm panel is not activated  
The component is actuated for a **second time**  
Alarm panel is now active

### • **On**

The behaviour during an activation attempt is as follows:

### Alarm panel

Activation process begins  
Fault is displayed  
OK is actuated (user noticed the warning and bypasses it)  
Alarm panel is active

Remote control, control panel, additional door lock, Secvest key

Component is actuated  
Alarm panel is now immediately active

#### **Note:**

In the case of **Force Set = On**, the user is not informed about the fault on these components. However, the faults and the override are documented in the logbook.

### Open zones

- **Off**

The behaviour during an activation attempt with the zone attribute "**Force Set Omit**" is as follows:

Alarm panel

- Activation process begins
- Fault is displayed
- The alarm panel can be activated once the zone is closed.

Remote control, control panel, additional door lock, Secvest key

- Component is actuated
- Fault message on the component corresponding to the component
- Alarm panel cannot be activated

**Note:**

- The alarm panel can be activated once the zone is closed.

- **Confirm**

The behaviour during an activation attempt with the zone attribute "**Force Set Omit**" is as follows:

Alarm panel

- Activation process begins
- Fault is displayed
- The alarm panel can be activated once the zone is closed.
- The zone can also be manually hidden.

Remote control, control panel, additional door lock, Secvest key

- Component is actuated
- Fault message on the component corresponding to the component
- The alarm panel is not activated
- The component is actuated for a **second time**
- The alarm panel is now active with **hidden** zones

- **On**

The behaviour during an activation attempt with the zone attribute "**Force Set Omit**" is as follows:

Alarm panel

- Activation process begins
- Fault is displayed
- The alarm panel can be activated once the zone is closed.
- The zone can also be manually hidden.

Remote control, control panel, additional door lock, Secvest key

- Component is actuated
- The alarm panel becomes immediately active with hidden zones

**Note:**

- In the case of **Force Set = On**, the user is not informed about the fault on these components. However, the faults and the override are documented in the logbook.

	<p><b>S/W &lt; 3.01.16</b></p> <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><b>Note</b></p> <p>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"> <li>• Off <ul style="list-style-type: none"> <li>• The user cannot force the system to arm with the remote control even if the corresponding zones have been given attribute "Force Set".</li> </ul> </li> <li>• Confirm <ul style="list-style-type: none"> <li>• The user can force the system to arm with the remote control. To do so, proceed as follows: <ol style="list-style-type: none"> <li>1. The user presses the "arm" button on the remote control.</li> <li>2. The system does not start arming.</li> <li>3. The user presses the same button on the remote control again to confirm that the system should arm.</li> </ol> </li> </ul> </li> <li>• On <ul style="list-style-type: none"> <li>• The user only has to press the corresponding button on the remote control once to start the arming process.</li> </ul> </li> </ul> <p><b>Note</b></p> <p>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>
<p><b>Remote Unset Full Set</b></p>	<p>Select whether <b>armed</b> partitions can only be disarmed using the <b>remote control</b> 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"> <li>• Always <ul style="list-style-type: none"> <li>• The user can always disarm the possible partitions without the entry time being started first.</li> </ul> </li> <li>• During entry time <ul style="list-style-type: none"> <li>• The user must first open a "Final Door" zone. This starts the entry delay. The user can now disarm the possible partitions.</li> <li>• Partitions for which no entry delay has started remain armed.</li> </ul> </li> </ul>
<p><b>Remote Unset Part Set</b></p>	<p>Select whether <b>internally armed</b> partitions can only be disarmed using the <b>remote control</b> 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"> <li>• Always</li> </ul>

- During entry time



- The user can always disarm the possible partitions without the entry time being started first.
- 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)
<b>Ctrl Device Unset Full Set</b>	<p>Select whether <b>armed</b> partitions can only be disarmed using the <b>wireless control device</b> 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"> <li>• Always</li> <li>• During entry time</li> </ul> <ul style="list-style-type: none"> <li>• The user can always disarm the possible partitions without the entry time being started first.</li> <li>• The user must first open a "Final Door" zone. This starts the entry delay. The user can now disarm the possible partitions.</li> <li>• Partitions for which no entry delay has started remain armed.</li> </ul>
<b>Ctrl Device Unset Part Set</b>	<p>Select whether <b>internally armed</b> partitions can only be disarmed using the <b>wireless control device</b> 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"> <li>• Always</li> <li>• During entry time</li> </ul> <ul style="list-style-type: none"> <li>• The user can always disarm the possible partitions without the entry time being started first.</li> <li>• The user must first open a "Final Door" zone. This starts the entry delay. The user can now disarm the possible partitions.</li> <li>• Partitions for which no entry delay has started remain armed.</li> </ul>
<b>Auto Rearm</b>	<p>Appears when the following is set: System-&gt;Confirmation-&gt;Confirmation Mode-&gt;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"> <li>• Never</li> <li>• 1 x, 2 x, 3 x, 4 x, 5 x</li> <li>• Always</li> </ul> <ul style="list-style-type: none"> <li>• The alarm panel never rearms. The alarm panel switches to the alarm status just one time.</li> <li>• The system rearms all closed zones but not the detectors still sending alarm signals.</li> <li>• One of these settings is required in order to comply with EN 50131</li> <li>• If the system is rearmed, an acoustic internal alarm instead of the normal entry tone is generated by the wireless alarm</li> </ul>

panel if a user enters through the entry route.

## Configuration

Name/function	Explanation (checkbox)
<b>Silence Alerts (silent warnings)</b>	<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"> <li>• User Code <ul style="list-style-type: none"> <li>• Warnings are sounded until a user enters their code to confirm the warning.</li> </ul> </li> <li>• 30 minutes</li> <li>• 60 minutes</li> <li>• 120 minutes</li> <li>• No alert tones <ul style="list-style-type: none"> <li>• Warnings are sounded for the set amount of time. The warning tones can be stopped by entering a user code.</li> <li>• No acoustic alerts are sounded.</li> </ul> </li> </ul> <p><b>Note</b> The alarm panel does not display any warnings as long as a partition is still armed.</p>
<b>Abort time</b>	<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. If an alarm occurs and a user disarms the system <b>within</b> this time, "Alarm Abort" outputs are activated and an alarm abort is reported.</p>
<b>Siren Delay (User)</b>	<p>"Siren Delay (User)" in minutes (value between 0 – 10). 0 means disarmed.</p> <p> <b>Note</b> When "Siren Delay (User-based)" is enabled (&gt; 0), the entire behaviour of the siren delay is blocked in the partition settings. <b>This does not comply with EN 50131.</b> ARC communication and Confirmation Mode affect the siren delay in the partition settings.</p> <p> <b>Note</b> Siren Delay (User) <b>only</b> affects the outdoor sirens when it comes to the following configurations: <b>Partition -&gt; Alarm reaction (all active, internally active, disabled)</b> Sirens and ESCC reporting or Strobes and ESCC reporting In the other variants internal, siren and strobe this siren delay is effective for all components (alarm panel, indoor siren, information module, control panel and outdoor siren). This means that all these components only signal after the delay time has elapsed.</p>





**Note**

In the event of a fire, intruder or 24h alarm, there is no siren delay (user)

**Alarm input delay**

Additional delay when deviating from the entry route.

Select whether the user is permitted an additional time of 30 seconds when deviating from the entry route, before an external alarm is started.

**Enabled**

Additional delay (30 s) activated when deviating from the entry route.

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.

If a user enters their code within these 30 s, the user can reset the system.

This setting is compliant with EN 50131.

**Deactivated**

No additional delay when deviating from the entry route.

An alarm is immediately triggered if a user deviates from the entry route and is caught by another detector in the process.

This setting is not compliant with EN 50131.

## Configuration

---

Name/function	Explanation (checkbox)
<b>Broadcast Panel Status</b>	<p><b>Enabled</b> 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><b>Deactivated</b> 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>

**Panel upgrade**

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

Details on upgrading the software to 1.01.00 can also be found in the "Software Upgrade" document in the Download area of the ABUS website.



**Note**

The "Panel Upgrade" menu is only available in this location up to S/W <1.01.00. From S/W 1.01.00 onwards, a new process has been established to ensure compliance with EN 50131.

New "Level/access level 4 user" authorisation level for SW updates

- It is no longer possible to run SW updates via the Installer menu of the web server
- Approval for "Level 4 User" must be granted in the User and Installer menu
- The user code for "Level 4 User" will be issued following approval

You will find further details in the "S/W Upgrade" appendix

## Configuration

---

### Only on the alarm panel

Installer Mode -> System -> Upgrade alarm panel



#### Note

The language file must be updated BEFORE updating the application file.

See the "S/W upgrade with new SD card files" chapter in the appendix

After pressing "Select", you will see a list of the available application software.

The first row of this list contains the currently installed software, and the other rows the available software files that are saved on the SD card.

#### Example

UPGRADE PANEL APPLICATION		
V3.01.14	Installed	
V1.01.00	10/02/2016	(2293760)
V2.00.00	04/10/2016	(2621440)
V2.00.06	06/03/2017	(2621440)
V2.01.08	15/06/2017	(2686976)
V3.00.04	12/12/2017	(2883584)
V3.01.01	10/05/2018	(2883584)
V3.01.11	17/10/2018	(2883584)
V3.01.14	11/03/2019	(2949120)
V3.01.16	25/11/2019	(2949120)
V3.01.17	10/12/2019	(2949120)

Select the desired application software.

Once the software has loaded, the first Start Wizard item appears (language selection). Follow the installation/Start Wizard instructions on the alarm panel.



#### Important

**SW >= 3.00.06, saving and restoring the configuration**


Before the alarm panel starts the upgrade, the configuration files and the SSL certificate are saved automatically on the internal flash drive. The new software is then installed, and the alarm panel restarted. At this point, the factory settings are used first, but the alarm panel then automatically reproduces the configuration files and the SSL certificate from the flash drive (as if the configuration had been saved/reproduced manually). This means that the Start wizard is not used and the SSL certificate is not regenerated.

### Checking for an upgrade?



#### Note

Due to conformity with EN 50131, this menu at this point in Installer mode is only available directly on the alarm panel. You will not find this menu in Installer mode when accessing via a web browser. This menu appears in the Level 4 menu. A Level 4 user must therefore log in. You will find further details in the "Software upgrade" chapter in the appendix.

Name/function	Explanation
Checking for an upgrade?	<p>After pressing "Select", the alarm panel automatically asks the ABUS FTP server: "Is new software available?"</p> <p>If the FTP server replies to this question with a "Yes", the following note appears: "Upgrade available".</p> <p>If the FTP server replies to this question with a "No", the following note appears: "Upgrade not available".</p>
Upgrade available	<p>If you would like to continue with the panel upgrade now, press OK.</p> <p>Wait until the panel accesses the language files Do not press "OK"</p> <p>Wait until the panel accesses the application file Do not press "OK"</p> <p> <b>Note</b> These files are stored on the SD card.</p> <p>Now reboot</p> <p>The alarm panel installs the new files from the SD card and performs a reboot.</p>




#### Important

#### SW >= 3.00.06, saving and restoring the configuration

Before the alarm panel starts the upgrade, the configuration files and the SSL certificate are saved automatically on the internal flash drive. The new software is then installed, and the alarm panel restarted. At this point, the factory settings are used first, but the alarm panel then automatically reproduces the configuration files and the SSL certificate from the flash drive (as if the configuration had been saved/reproduced manually). This means that the Start wizard is not used and the SSL certificate is not regenerated.

**Backup/restore**

Name/function	Explanation (checkbox)
<b>Load Configuration</b>	<p>Click the <b>Browse</b> button to specify the path and file name of the configuration to be restored.</p> <p>Click the <b>Load Configuration</b> button to import the configuration to be restored into the wireless alarm system.</p> <p>The wireless alarm system must then be restarted.</p>
<b>Backup</b>	<p>Click the <b>Backup</b> button to create a backup of the entire system configuration (including detector IDs). The backup file is saved in the default Downloads folder.</p> <p> <b>Note</b></p> <p>The configuration file is saved in the format <b>Secvest--01-09-2017-1051.cfg</b>.</p> <p>If it has not been possible for the PC or web browser to perform the sent instructions for changing the file name, they will be saved in the standard version "config.config".</p>

## Configuration

---

SW >=3.00.00

### Backup/restore (alarm panel GUI only)

#### Alarm panel

Installer Mode -> System -> Backup/restore

Backing up config to the SD card

After pressing "Select", the configuration file is written to the SD card. During this period, "**Writing file**" appears on the display

Loading config from SD card

Once you have selected the desired configuration file and pressed "Select", the configuration file is loaded from the SD card to the alarm panel. During this period, "**Reading file**" appears on the display



#### Note

The alarm panel creates a new folder on the SD card with the name "Config". All of the configuration files are written to this folder. Each new file is given a new file name. No old files are overwritten.

The alarm panel creates a file name that includes the Secvest, date and time.

Example (SW 3.00.00 to SW < 3.01.00):

**Secvest--01-09-2017-1051.cfg**

01-09-2017: Date

1051: Time, 10:51 a.m.

Example (SW >= 3.01.01):

**Secvest—2018-11-08-0935.cfg**

2018-11-08: Date, 8 November 2018

0935: Time, 9:35 a.m.



#### Note

You can also copy saved configuration files from the PC (via WEB) to the SD card. Copy the configuration files to the "Config" folder. If the alarm panel has not yet created the "Config" folder, you can create it manually.

Please note the following:

Sometimes, the configuration file is not saved in the format **Secvest--01-09-2017-1051.cfg** or **Secvest--2017-09-01-1051.cfg**.

If it has not been possible for the PC or web browser to perform the sent instructions for changing the file name, they will be saved in the standard version "config.config".

Simply change the file name "config.config" to the following format: **Secvest--01-09-2017-1051.cfg** or **Secvest--2017-09-01-1051.cfg**.

When doing so, it is important that:

- The file ending MUST be ".cfg"
- The file name must start with Secvest and two dashes or minus signs "**Secvest—**"

File names that do not follow this syntax will not be displayed in the "Loading config from SD card" menu in the alarm panel.

E.g. "config.config" or "Secvest--01-12-2017-1102.config"





**Danger**

**Data protection**

**Follow the SD card instructions in the "Decommissioning the alarm panel" chapter.**

## Report

SW >=3.00.01

Web interface only



Name/function	Explanation (checkbox)
<p><b>Report</b></p>	<p>When clicking on the <b>Report</b> button, a pop-up browser window will appear. The window will display the entire system configuration for the alarm panel in a clear format.</p> <div data-bbox="475 1214 963 1877" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <div style="text-align: right; margin-bottom: 10px;"> <input type="button" value="Print"/> </div> <h3 style="margin: 0;">Installation</h3> <p>Installation Site:                      Installation Address:                      Installer Name: "2419"                      Installer Tel No:                      Date: 18/01/2017</p> <h3 style="margin: 10px 0;">About Panel</h3> <p>Version: v3.00.02                      Language: English v1.22                      Serial Number: SECVEST###G7020971AAX    Part No.: FUA50000                      RF Device Exclusivity: No                      Zones: Available: 58    Used: IP: 0 Radio: 0 Wired: 0                      Control Devices: 0                      Radio Sirens: 0                      WAMs: 0                                  Door Locks: 0</p> </div>
<p><b>Print</b></p>	<p>To print the report, press the "Print" button in the top left of the form. The standard Windows "Print" dialog appears. Select your desired printer.</p>



**Note**

Which printers appear will depend on the printers installed on the computer.  
E.g. "Real" paper printer, or "PDF printer" such as PDF-Xchange, Freepdf.

**Content of the report**

The report contains all relevant settings and information from the installer mode as well as the volume settings from the user menu.



**Notes**

**"User defined" outputs**

Polarity: normal or inverted; for "inverted", the word "inverted" will appear. No additional word will appear for "normal".

If there is a time schedule, the selected weekdays appear as uppercase letters.

Example: Continuous 08:00 -> 16:00 **SmTwtfS**

Switch-on time 08:00, switch-off time 16:00



S	m	D	m	D	f	S
Sun	Mon	Tue	Wed	Thu	Fri	Sat
yes	no	yes	no	yes	no	yes



## Communication





## Network

The screenshot displays a web-based configuration interface. At the top left, there is a red 'ABUS' logo. The main header area shows 'Communications | Network'. Below this, four large buttons are arranged horizontally: 'Network Setup' (with a network diagram icon), 'IP Mobile Setup' (with a network diagram icon), 'Email Setup' (with an envelope icon), and 'Voip Dialler Setup' (with a 'VOIP' speech bubble and gear icon). On the right side, a vertical sidebar menu is visible, starting with a 'Log out' button and a user profile icon. Below these are menu items: 'About' (info icon), 'Status' (house icon), 'Devices' (document icon), 'Outputs' (arrow icon), 'Partitions' (pie chart icon), 'System' (gear icon), 'Communications' (phone icon), 'Social Care' (bed icon), 'Test' (gear icon), 'View Log' (calendar icon showing '18'), and 'Keypad' (keypad icon).

Network Setup

Name/function	Explanation (checkbox)
Internal HTTP port	<p>Internal HTTP port Standard value: 80</p> <p> <b>Note</b> Do not effect port forwarding on the router on port 80. This could lead to a network block. Use the "internal HTTPS port", e.g. 4433, as the target for port forwarding.</p>
Internal HTTPS port	<p>Internal HTTPS port Standard value: 4433</p> <p> <b>Note</b> SW &gt;= 3.00.05 The <b>change</b> to the internal HTTPS port only takes effect once the alarm panel has been <b>rebooted</b>. To do this, log out of Installer mode and reboot the alarm panel. More details can be found in the section "Manual restart (switching off and switching back on)".</p>
DHCP	Enabled

	<p>The Secvest receives the IP data from the DHCP server.</p> <p><b>Deactivated</b></p> <p>Manual input of IP data.</p>
<b>IP address</b>	<p>IP address</p> <p>SW &lt;2.00.00: If nothing is entered here, the alarm control panel automatically uses DHCP.</p> <p></p> <p><b>Note</b></p> <p>We recommend assigning a fixed IP address to prevent problems with port routing. It is possible to set the router so that the Secvest always assigns the same IP address via DHCP for this MAC Address. However, some routers assign a different IP address via DHCP after a certain time.</p>
<b>IP Subnet Mask</b>	IP subnet mask
<b>Gateway IP address</b>	Gateway IP address
<b>DNS primary IP address</b>	DNS primary IP address
<b>ABUS Server Enabled</b>	<p><b>Enabled</b></p> <ul style="list-style-type: none"> <li>Establishes a connection to the ABUS server and sends the public IP access data.</li> <li>SW &gt;= 3.01.16 The alarm panel sends an ICMP Ping to the ABUS server.</li> </ul> <p></p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>The alarm panel always sends the following information to the ABUS server every 30 minutes, even if no personal account has been created: MAC address, public IP address and public HTTPS port. You will have access to this data after creating a personal account. This <b>only</b> occurs via Ethernet, <b>not</b> via IP mobile.</li> <li>SW &gt;= 3.01.16 The alarm panel sends an ICMP Ping to the ABUS server every 30 minutes. This <b>only</b> occurs via Ethernet, <b>not</b> via IP mobile. The alarm panel thus tests the IP path, especially the path not directly on the Ethernet connection of the alarm panel and in the public area. Faults in these areas could be: <ul style="list-style-type: none"> <li>Public area (WAN) Public cable to the router defective, construction site in front of the house</li> <li>Private area (LAN) Note: the direct Ethernet interface at the alarm panel is monitored via "<b>Ethernet communication channel fault</b>". The router is switched off but the switch is functional (the alarm panel is directly connected to this switch). Problems with the Wi-Fi module Wi-Fi at the router is inoperative No new connection to the Wi-Fi after a long router shut-down Wi-Fi at the router switches off between e.g. 10 p.m. and 6 a.m. (sometimes a standard router setting or configured as a power saving function).</li> </ul> </li> </ul> <p>If this ICMP Ping does not have a positive result, the alarm panel immediately switches to IP mobile. A requirement for this is the use of a wireless mobile</p>

	<p>module as a redundancy and the corresponding setting for "IP Gateway" (Communication -&gt; Network -&gt; IP mobile setup).          IP mobile is used temporarily until the ICMP Ping delivers a positive result once more.</p> <p>  <b>Note</b>          If there is no wireless mobile module or only Ethernet is selected under IP Gateway, the alarm panel only signals a fault message.</p> <p><b>Deactivated</b>          Functions not possible.</p> <p>  <b>Note</b>          See also notes on the ABUS server in the chapter "S/W upgrade"</p>
<b>External HTTPS port</b>	Port number of the external port.
<b>ABUS Server User Name</b>	<p>User name on the ABUS server</p> <p>  <b>Note</b>          GUI input: max. 31 characters          WBI input: max. 15 characters</p>
<b>ABUS Server Password</b>	<p>Password on the ABUS server</p> <p>  <b>Note</b>          GUI input: max. 32 characters          WBI input: max. 15 characters</p>

## IP Mobile Setup

**ABUS**
Log out

Communications | Network | **IP Mobile Setup**

APN	<input type="text" value="internet.telekom"/>	Username	<input type="text" value="t-mobile"/>
IP Gateway	<input type="text" value="Ethernet - IP Mobile"/>	Password	<input type="text" value="tm"/>

- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- Test
- View Log
- Keypad

Name/function	Explanation (checkbox)
	<div style="text-align: center;"></div> <p><b>Note</b></p> <p>APN, user name and password are access data for IP-based transmission in the wireless mobile network.</p> <p>This data depends on the network provider and service provider. Request this data from your SIM card provider.</p> <p>Alternative: This data is usually stored on the SIM card. Insert the SIM card into a smartphone before you use it in the wireless mobile module. Read the data in the Data Settings menu.</p>
<b>APN</b>	Enter the "Access Point Name" here.
<b>User name</b>	The user name for data access in the wireless mobile network.
<b>Password</b>	The password for data access in the wireless mobile network
<b>IP Gateway</b>	<div style="text-align: center;"></div> <p><b>Note</b></p> <div style="text-align: center;"></div> <p><b>Danger</b></p> <p>The IP gateway settings are only relevant for the ARC IP-based communications, speech dialler and email.</p> <p>Ethernet is still used for</p>



- access to the web server via a web browser
- APP access
- for push notifications (SW <= v3.01.01)
- For cameras in the local network



**Note**



**Danger**

If the "IP mobile" transmission path is used by the control panel, the ABUS server is not updated.



**Note**

The alarm panel receives a public IP address from the mobile IP network of the wireless mobile network. Data and information is only exchanged when communication is activated through this path.



**Note**




You will find some access data in the Appendix. Due to the large number of mobile network providers in Europe and an even larger number of SIM card providers (service providers), this contains only a few selected examples.



**Note**

SW >= 3.01.16

See also the information on ICMP Ping at "ABUS server" (Communication -> Network -> Network Setup)

Name/function	Explanation (checkbox)
Ethernet	<p>Only Ethernet is used, 4G/2G is not used.</p> <p>  <b>Note</b>                      SW &gt;= 3.01.16                      See also the information on ICMP Ping at "ABUS server" (Communication -&gt; Network -&gt; Network Setup)</p>
IP Mobile – Ethernet	<p>4G/2G is used first. Ethernet is used when no 4G/2G signal is available.</p> <p>  <b>Note</b>                      4G/2G faults must first be detected by the alarm panel.</p> <p>  <b>Danger</b>                      Ethernet is still used for</p> <ul style="list-style-type: none"> <li>• access to the web server via a web browser</li> <li>• APP access</li> <li>• for push notifications (SW &lt;= v3.01.01)</li> </ul>

- For cameras in the local network

It is not possible to access the alarm panel with the app via the ABUS server and via IP mobile. It is not possible to access the web server of the alarm panel via IP mobile.



**Note**

**Push notifications**

The push notification only functions via the wireless mobile module (IP mobile) if a PPP connection (point to point protocol, IP mobile) is already active/configured for another service (e.g. e-mail).

E-mail must be at least enabled. However, no e-mails need to be sent. Configure the settings for this accordingly.

**Configure ABUS server, app and push via Ethernet.**

There must be an IP mobile fault (e.g. no longer logged into a wireless mobile network) for the IP stack to switch to Ethernet.



**Note**

SW >= 3.01.16

See also the information on ICMP Ping at "ABUS server" (Communication -> Network -> Network Setup)

**Ethernet – IP Mobile**

Ethernet is used first. 4G/2G is only used when there is an Ethernet fault.

This setting is recommended in order to establish a redundant, IP-based transmission path for ARC/ESCC reporting, e-mail and push.



**Note**

Ethernet faults must first be detected by the alarm panel.



**Note**

SW >= 3.01.16

See also the information on ICMP Ping at "ABUS server" (Communication -> Network -> Network Setup)







**Danger**

Ethernet is still used for

- access to the web server via a web browser
- APP access
- for push notifications (SW <= v3.01.01)
- For cameras in the local network

It is not possible to access the alarm panel with the app via the ABUS server and via IP mobile. It is not possible to access the web server of the alarm panel via IP mobile.



	<p><b>Note</b> <b>Push notifications</b> The push notification only functions via the wireless mobile module (IP mobile) if a PPP connection (point to point protocol, IP mobile) is already active/configured for another service (e.g. e-mail). E-mail must be at least enabled. However, no e-mails need to be sent. Configure the settings for this accordingly. <b>Configure ABUS server, app and push via Ethernet.</b> There must be an Ethernet fault for the IP stack to switch to IP mobile.</p>
<b>IP Mobile</b>	<p>Only 4G/2G is used, Ethernet is not used.</p> <p> <b>Note</b>  <b>Danger</b> Ethernet is still used for</p> <ul style="list-style-type: none"><li>• access to the web server via a web browser</li><li>• APP access</li><li>• for push notifications (SW &lt;= v3.01.01)</li><li>• For cameras in the local network</li></ul> <p>It is not possible to access the alarm panel with the app via the ABUS server and via IP mobile. It is not possible to access the web server of the alarm panel via IP mobile.</p> <p> <b>Note</b> <b>Push notifications</b> The push notification only functions via the wireless mobile module (IP mobile) if a PPP connection (point to point protocol, IP mobile) is already active/configured for another service (e.g. e-mail). E-mail must be at least enabled. However, no e-mails need to be sent. Configure the settings for this accordingly. <b>Configure ABUS server, app and push via Ethernet.</b></p> <p> <b>Note</b> SW &gt;= 3.01.16 The alarm panel sends an ICMP Ping to the ABUS server every 30 minutes. This <b>only</b> occurs via Ethernet, <b>not</b> via IP mobile. For details, see also the information on ICMP Ping at "ABUS server" (Communication -&gt; Network -&gt; Network Setup) In this configuration, it is useful to set the ABUS server to <b>disabled</b> in order to prevent malfunctions. With the IP mobile setting, it is not possible to use the app to access the alarm panel via the ABUS server.</p>



**Email Setup**
Log out

ABUS
Communications | Network | **Email Setup**

Server Name

Account

Password

IP Port Number

Username

SSL

About

Status

Devices

Outputs

Partitions

System

Communications

Social Care

Test

View Log

Keypad

Name/function	Explanation (checkbox)	Max. characters
<b>Server Name</b>	SMTP server name of the email service provider.	32
<b>IP Port Number</b>	IP port number	5
<b>Account</b>	Name of the email account (usually the email address)	90
<b>User name</b>	User name (depending on the provider, either the entire email address or a separate user name)	90
<b>Password</b>	Password for the email account	32
	<p><b>Note</b> This entry is case-sensitive.</p>	
<b>SSL</b>	<p><b>Enabled</b> An encrypted connection (SSL) to the provider is established.</p> <p><b>Deactivated</b> An unencrypted connection (SSL) to the provider is established.</p>	-

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.

**Note**

The alarm panel does not send information. A connection is only established when an e-mail is definitely sent, starting with a handshake. The information is then sent in accordance with the settings (e.g. encrypted or unencrypted) as well as the programmed texts and events.





**VoIP Dialler Setup**
Log out

ABUS
Communications | Network | **Voip Dialler Setup**


SIP Domain Name	<input type="text"/>	SIP Proxy	<input type="text"/>
SIP User ID	<input type="text"/>	SIP User Password	<input type="text"/>
SIP Port	<input type="text"/>	RTP Port	<input type="text"/>
SIP Test Call User ID	<input type="text"/>	SIP Dialler Enable	<input checked="" type="checkbox"/>
RFC 2833 DTMF Detection	<input checked="" type="checkbox"/>		

- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- Test
- View Log
- Keypad

Name/function	Explanation (checkbox)	Max. characters
<b>SIP domain name</b>	SIP server name of the individual SIP service provider e.g. sipgate.de	50
<b>SIP proxy</b>	Proxy of the individual SIP service provider e.g. sipgate.de	50
<b>SIP User ID</b>	User ID of the SIP service provider for your account	50
<b>SIP User Password</b>	SIP user password of the SIP service provider for your account	50
<b>SIP Port</b>	The port of the SIP service provider for your account Standard: 5060	5
<b>RTP Port</b>	RTP port number of the SIP service provider for your account	5
<b>SIP test call user ID</b>	User ID for the recipient of a test call via SIP Format S/W >=2.00.00 Phone number +49 (0)82071234567 ID, if the recipient has an account with the same SIP service provider 9876543  S/W <2.00.00 Phone number +4982071234567@sipgate.de	50

208



	<p>sipgate.de is the individual SIP service provider, as SIP server name</p> <p>ID, if the recipient has an account with the same SIP service provider</p> <p>9876543@sipgate.de</p>	
<b>SIP Dialler Enable</b>	<p><b>Enabled</b> The SIP dialler is enabled.</p> <p> <b>Note</b> The alarm panel does not send information. A connection is only established when a call is definitely made, starting with a handshake. The information is then sent in accordance with the settings as well as the recorded voice messages for the events.</p> <p><b>Deactivated</b></p>	-
<b>RFC 2833 DTMF Detection</b>	<p><b>Enabled</b> DTMF tones are also detected for SIP under certain requirements.</p> <p><b>Deactivated</b> No detection of DTMF tones.</p>	-



**Note**

The alarm control panel works through the communication types in the following order:

1. ARC/ESCC reporting
2. Email
3. Social care (protocol transmission)
4. SMS via GSM
5. Voice dialler
6. SMS via PSTN

Push notifications are independent of this sequence and may occur at any time.

## ARC reporting

**ABUS** Log out

Communications | **ARC Reporting**

Call Mode: **\*Disabled** | Report Type: **\*Fast Format**

**Phone Book** | Account Numbers | Fast Fmt Channels | More...

Tel. Recipient 1: **Keine**

Tel. Recipient 2: **Keine**


IP Recipient 1: **Keine** | Port: **1792**

IP Recipient 2: **Keine** | Port: **2750**

**Cancel** | **Submit**

- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- View Log
- Keypad

SW >= 3.00.03

Name/function	Explanation (checkbox)
<p><b>Call Mode</b></p>	<p>Dropdown selection field for:</p> <ul style="list-style-type: none"> <li>• Disabled</li> <li>• Single</li> <li>• Alternate</li> </ul> <p></p> <p><b>Note</b></p> <p>The alarm panel does not send information. A connection is only established when there is concrete ESCC reporting, starting with a handshake. The information is then sent in accordance with the settings (e.g. encrypted or unencrypted).</p>
<p><b>Log</b></p>	<p>Dropdown selection field for:</p> <ul style="list-style-type: none"> <li>• Fast Format</li> <li>• Contact ID</li> <li>• SIA 1</li> <li>• SIA 2</li> <li>• SC SIA 3</li> <li>• Ex SIA 3</li> <li>• Ex SIA 3 v2</li> </ul>

- Ex SIA 3 v3
- Contact ID in SMS



**Note**

A detailed description of the protocol formats can be found in the Appendix "ARC (ESCC) reporting protocol formats"

**ARC Reporting, Phone Book**

ABUS Log out

Communications | **ARC Reporting**

Call Mode: **\*Disabled** | Report Type: **\*Fast Format**

Phone Book | Account Numbers | Fast Fmt Channels | More...

Tel. Recipient 1: **Keine**

Tel. Recipient 2: **Keine**

IP Recipient 1: **Keine** | Port: **1792**

IP Recipient 2: **Keine** | Port: **2750**

Cancel | Submit

- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- View Log
- Keypad

Name/function	Explanation (checkbox)
<b>Tel Recipient #</b>	After clicking this field, the recipients that are stored in the phone book (contacts) appear. Select a recipient and their corresponding telephone number.
<b>IP recipient #</b>	After clicking this field, the recipients that are stored in the phone book (contacts) appear. Select a recipient and their corresponding IP address.
<b>Port</b>	To the right of the IP recipients, enter the port number that the ARC/ESCC has provided you with for this IP address.



**Note**

S/W >= 3.01.11

If the alarm panel was unable to reach the respective recipient during the first dialling attempt, the alarm panel will attempt to reach the respective recipient a maximum of three times.

S/W < 3.01.11

The alarm panel attempts to reach the respective recipient max. 16 times.



**Note**

## Configuration

---

Contacts/recipients that are used for monitoring station switching are no longer "visible" in the user menu's phone book. As a result of EN 50131 compliance, Level 2 users (access level 2) must not make any changes to the monitoring station switching.

### ARC Reporting, Account Numbers

ABUS
Log out

Communications | ARC Reporting

Call Mode: \*Disabled ▼

Report Type: \*Fast Format ▼

Phone Book
Account Numbers
Fast Fmt Channels
More...

Account No P1:

Account No P3:

Account No P2:

Account No P4:

Cancel
Submit

- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- View Log
- Keypad


Name/function	Explanation (checkbox)
<b>Account No P#</b>	<p>Input field for an account number with up to 6 digits for the partition in question. CID uses 4-digit account numbers</p> <p>With Fast Format, you can use 4, 5 or 6-digit account numbers. The alarm panel adds a leading zero to lengthen 5-digit account numbers into 6-digit codes.</p> <p>The alarm panel does not alter 4-digit or 6-digit account numbers.</p>

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

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



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

Name/function	Explanation (checkbox)
Fire	<b>Enabled</b>
Medical Alarm	Events from this group are transmitted to the ARC/ESCC.
Technical Alarm	
Set/Unset	<b>Deactivated</b>
Reset	<b>No</b> events from this group are transmitted to the ARC/ESCC.
Omit	
RF Supervision	
RF Battery/PSU	
Mains Fault	<b>Note</b>
Installer Mode	This menu only appears if you select "Contact ID" or one of the SIA versions as a protocol.
Time/Date Reset	If you approve a group using "Yes", the alarm control panel can send every event from this group.
Panic alarm	A detailed overview of the assignment can be found in the Appendix "CID/SIA Events".
Intruder alarm	To simplify the programming, the possible CID/SIA events are assigned to corresponding groups. In Table 1 and 3, you can see the CID/SIA events with the corresponding group assignment. In Table 2 and 4, you can see the groups with the corresponding CID/SIA events.
Tampers	
Part set	
Exit Timeout	
Key Box	
RF Jamming	
Panel Battery	

## Configuration

---

Faults  
User Code Chnge  
Camera supervision

## Encryption

From S/W v3.00.03 onwards, the message transmission to ARC/ESCC can also be encrypted.



### Note

This is where the provisions of the following document apply.  
**ANSI/SIA DC-09-2013: Internet Protocol Event Reporting**  
**SIA Digital Communication Standard – Internet Protocol**  
**Event Reporting**

For further details, see the "ARC/ESCC reporting" chapter in the appendix.



### Danger

Please note that the time in the alarm panel must be set accurately so that the authorisation functions properly. Setting the time via an SNTP server is recommended here.


Click on the desired IP recipient.

The screenshot displays the 'ARC Reporting' configuration page. At the top, there are two dropdown menus: 'Call Mode' set to '\*Disabled' and 'Report Type' set to '\*Fast Format'. Below these are several buttons: 'Phone Book', 'Account Numbers', 'Fast Fmt Channels', 'Encryption' (which is highlighted in blue), and 'More...'. A table with two columns, 'Index' and 'Name', shows two entries: 'IP Recipient 1' and 'IP Recipient 2', both with 'None' in the 'Name' column. At the bottom of the main area are 'Cancel' and 'Submit' buttons. On the right side, there is a vertical sidebar with a 'Log out' button at the top, followed by a list of menu items: 'About', 'Status', 'Devices', 'Outputs', 'Partitions', 'System', 'Communications', 'Social Care', 'Test', 'View Log', and 'Keypad'.

## Configuration

Select the desired key length

To input the key, click on "Edit key"

Name/function	Explanation (checkbox)
Encryption length	None
Key length	128 bits
	192 bits
	256 bits
None	The messages are sent unencrypted
128 bits	 <p><b>Note</b> Enter the 32 hexadecimal characters as a key here. Hexadecimal characters are 0–9 and a–f</p>

Encryption Key:

0123	-	4567	-	89ab	-	cdef	-
fedc	-	ba98	-	7654	-	3210	

Submit

Cancel

192 bits



**Note**

Enter the 48 hexadecimal characters as a key here.  
Hexadecimal characters are 0–9 and a–f

Encryption Key:

0123	-	4567	-	89ab	-	cdef	-
fedc	-	ab98	-	7654	-	3210	-
0000	-	0000	-	0000	-	0000	-

Submit

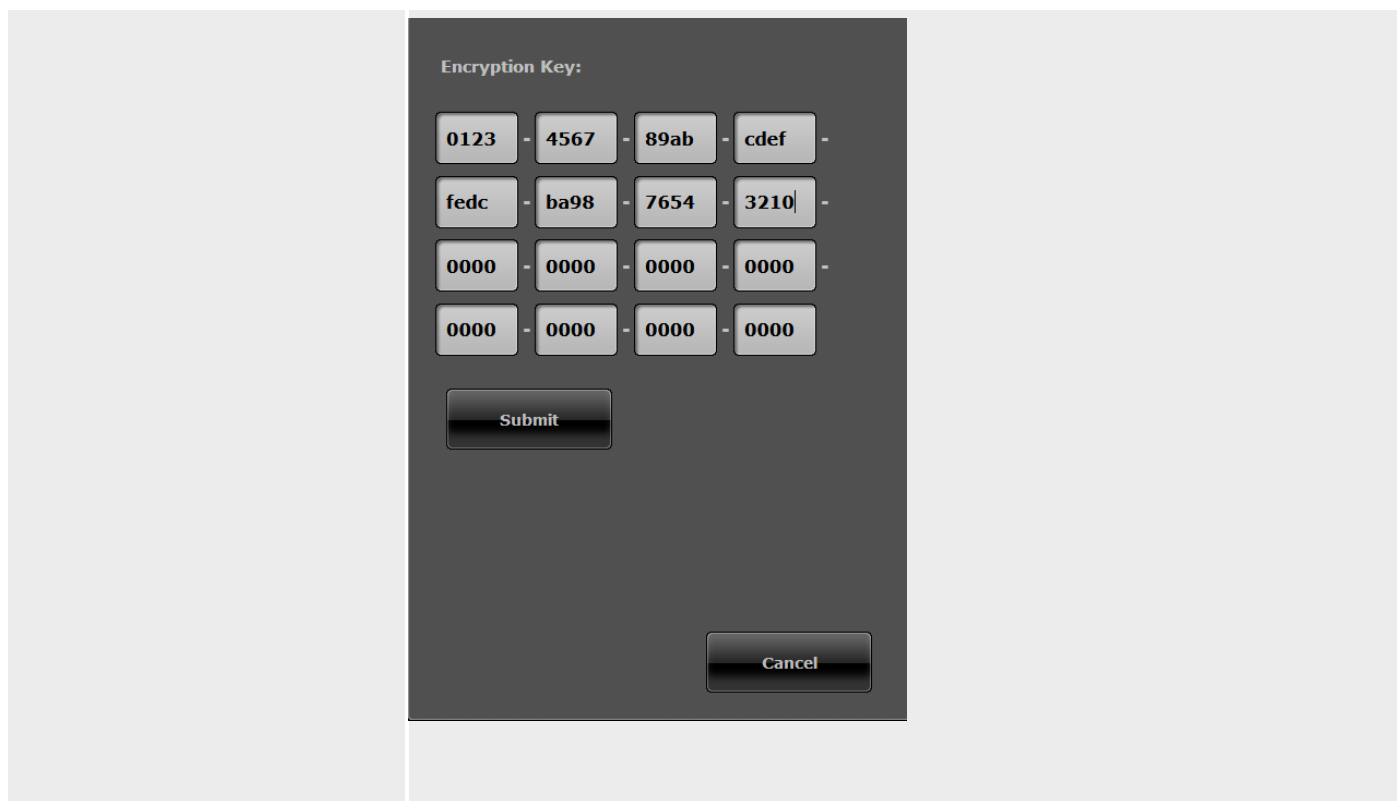
Cancel

256 bits



**Note**

Enter the 64 hexadecimal characters as a key here.  
Hexadecimal characters are 0–9 and a–f



On the **alarm panel** you will find the encryption settings under:

Installer Mode -> Communications -> ESCC Reporting -> Recipient -> IP Recipient 1/2

- Receiver
- IP Port Number
- Key length
  - None
  - 128 bit
  - 192 bit
  - 256 bits

Key



**Note**

The menu item does **not** appear when "None" is selected for the key length.

128 bit has been selected as the key length.

0000 0000 0000 0000

0000 0000 0000 0000



**Note**

Enter the 32 hexadecimal characters as a key here.  
Hexadecimal characters are 0–9 and a–f

192 bit has been selected as the key length.

0000 0000 0000 0000  
0000 0000 0000 0000  
0000 0000 0000 0000



**Note**

Enter the 48 hexadecimal characters as a key here.  
Hexadecimal characters are 0–9 and a–f

256 bit has been selected as the key length.

0000 0000 0000 0000  
0000 0000 0000 0000  
0000 0000 0000 0000  
0000 0000 0000 0000



**Note**

Enter the 64 hexadecimal characters as a key here.  
Hexadecimal characters are 0–9 and a–f



**ARC Reporting, More**

ABUS Log out

Communications | **ARC Reporting**

Call Mode: **\*Disabled** | Report Type: **\*Fast Format**

Phone Book | Account Numbers | Fast Fmt Channels | **More...**

Restorals  | Burg Comms Rearm

21CN Ack Time: **\*800ms** | Dynamic Test Call




Unset Comms  | Telecoms Priority





Cancel | Submit

- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- View Log
- Keypad

Name/function	Explanation (checkbox)
<b>Restorals</b>	<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"> <li>Type and time of the event taking place</li> <li>Event reset</li> </ul> <p>The event reset is called a "restoral".</p> <p><b>Enabled</b> The information about the event reset (restoral) is transmitted to the ARC.</p> <p><b>Deactivated</b> The information about the event reset (restoral) is not transmitted to the ARC.</p>
<b>21CN Ack Time</b>	<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. Use this option to set the wait time for the confirmation.</p> <p>Dropdown selection field for:</p> <ul style="list-style-type: none"> <li>400 ms</li> <li>600 ms</li> <li>800 ms</li> <li>1000 ms</li> <li>1200 ms</li> <li>500 ms</li> <li>700 ms</li> <li>900 ms</li> <li>1100 ms</li> </ul>

Name/function	Explanation (checkbox)
<b>Unset Comms</b>	<b>Enabled</b>

	<p>The alarm system transmits all status messages to the ARC, regardless of whether the system is armed or disarmed.</p> <p><b>Deactivated</b></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>
<p><b>Burg Comms Rearm</b></p>	<p>Only appears when "System → Confirmation → Confirmation Mode = Basic" and "Communications → Protocol = Fast Format")</p> <p><b>Enabled</b></p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Note: if a "Final Door" zone is triggered, channel 3 is activated at the end of the configured entry/exit time.</li> </ul> <p><b>Deactivated</b></p> <p>Channel 3 remains activated until a user or installer resets the system.</p>
<p><b>Dynamic Test Call</b></p>	<p><b>Enabled</b></p> <p>The dynamic test call is activated.</p> <p>The test call is started every 24 hours after the last transmission.</p> <p></p> <p><b>Note</b></p> <p>The advantage of the dynamic test call is that a test transmission is only made to the monitoring station if there was no transmission in the last 24 hours. If you have programmed an active/disarmed transmission, then it is possible that no test transmission will be made for several days if the system is activated or disarmed daily.</p> <p><b>Deactivated</b></p> <p>The dynamic test call is deactivated. The "Static Test Call" dropdown selection field appears.</p>
<p><b>Telecoms Priority</b></p>	<p>Set the order in which the communication methods should be used here.</p> <ul style="list-style-type: none"> <li>• Ethernet / IP      1, 2, 3 or No Mobile</li> <li>• PSTN                1, 2, 3 or No</li> <li>• GSM/mobile        1, 2, 3 or No</li> </ul> <p><b>Note:</b></p> <p>The alarm control panel automatically uses the IP-based protocol DC-09 if the alarm control panel uses Ethernet (LAN) as an outgoing communication path. In doing so, the data from traditional protocols are packed into IP packages and transferred.</p> <p>For details, see the "ARC/ESCC reporting protocols" appendix</p> <p><b>S/W &gt;=3.00.05</b></p> <p>Set the order in which the communication methods should be used here.</p> <ul style="list-style-type: none"> <li>• Ethernet / IP      1, 2, 3 or No Mobile</li> </ul> <p></p> <p><b>Note</b></p> <p>means data transfer according to the setting via IP gateway the "Mobile Setup" menu</p> <p></p>

	<p><b>Note</b> SW &gt;= 3.01.16 See also the information on ICMP Ping at "ABUS server" (Communication -&gt; Network -&gt; Network Setup)</p> <ul style="list-style-type: none"> <li>• PSTN 1, 2, 3 or No</li> <li>• Mobile 1, 2, 3 or No</li> </ul> <p> <b>Note</b> means classic voice transmission (also DTMF and FSK) or SMS transmission via a wireless mobile network.</p> <p> <b>Note</b> The display varies according to the setting via IP gateway the "IP Mobile Setup" menu.</p>
<p><b>Stat. Test Call</b> Only when "Dynamic Test Call" is deactivated</p>	<p><b>Dropdown selection field for:</b></p> <ul style="list-style-type: none"> <li>• Disabled</li> <li>• Daily</li> <li>• Weekly</li> <li>• Monthly</li> </ul> <p> <b>Note</b> For each of the three types of call - daily, weekly and monthly - the alarm panel adds a random minute value. This minute value lies between 0 and 16. The call can, therefore, occur up to 16 minutes after the hour you have entered. This should ensure that the ARC (ESCC) is not flooded with test calls from the system that all contain the same time.</p>
<p><b>SET THE HOUR</b> Only for "Static Test Call"</p> <ul style="list-style-type: none"> <li>• Daily</li> <li>• Weekly</li> <li>• Monthly</li> </ul>	<p>Input field for the time of the daily test call (hh:mm)</p> <p> <b>Note</b> Only full hours are possible.</p>

Name/function	Explanation (checkbox)
<p><b>SET THE DAY</b> Only for "Static Test Call"</p> <ul style="list-style-type: none"> <li>• Weekly</li> </ul>	<p><b>Dropdown selection field for:</b></p> <ul style="list-style-type: none"> <li>• Sunday</li> <li>• Monday</li> <li>• Tuesday</li> <li>• Wednesday</li> <li>• Thursday</li> </ul>

## Configuration

---

	<ul style="list-style-type: none"><li>• Friday</li><li>• Saturday</li></ul>
<b>SET THE DAY</b> Only for "Static Test Call" <ul style="list-style-type: none"><li>• Monthly</li></ul>	Input field for the day of the month on which the test call should be carried out (1–31)

**Emergency call**
Log out

ABUS
Communications | Social Care

Call Mode \*Disabled ▼

Telecoms Priority ▶

21CN Ack Time \*800ms ▼

Report Type \*Scancom ▼

Call Acknowledge

Phone Book

Account Numbers

Tel. Recipient 1 Keine

Tel. Recipient 2 Keine



Cancel

Submit

Log out

- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- View Log
- Keypad

Name/function	Explanation (checkbox)
<b>Call Mode</b>	Dropdown selection field for: <ul style="list-style-type: none"> <li>• Disabled</li> <li>• Single</li> <li>• Alternate</li> </ul> <div style="text-align: center; margin: 10px 0;"> </div> <p><b>Note</b></p> <p>The alarm panel does not send information. A connection is only established when an emergency call is actually sent, starting with a handshake. The information is then sent in accordance with the settings.</p>
<b>Log</b>	Dropdown selection field for: <ul style="list-style-type: none"> <li>• Scancom</li> <li>• Scanfast</li> <li>• Tunstall</li> </ul>
<b>Telecoms Priority</b>	<p><b>S/W &lt; 3.00.05</b></p> <p>Set the order in which the communication methods should be used here:</p> <ul style="list-style-type: none"> <li>• PSTN            1, 2 or No</li> <li>• GSM/mobile 1, 2 or No</li> </ul>

	<p><b>S/W &gt;=3.00.05</b> Set the order in which the communication methods should be used here.</p> <ul style="list-style-type: none"><li>• PSTN 1, 2, 3 or No</li><li>• Mobile 1, 2, 3 or No</li></ul> <p> <b>Note</b> means classic voice transmission (also DTMF and FSK) via a wireless mobile network.</p> <p> <b>Note</b> The display varies according to the setting via IP gateway the "IP Mobile Setup" menu.</p>
<b>21CN Ack Time</b>	<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. Use this option to set the wait time for the confirmation.</p> <p><b>Dropdown selection field for:</b></p> <ul style="list-style-type: none"><li>• 400 ms</li><li>• 500 ms</li><li>• 600 ms</li><li>• 700 ms</li><li>• 800 ms</li><li>• 900 ms</li><li>• 1000 ms</li><li>• 1100 ms</li><li>• 1200 ms</li></ul>
<b>Call Acknowledge</b>	<p><b>Enabled</b> A social care alarm transmission must be confirmed by the recipient by pressing DTMF button "5", otherwise the calls will be repeated.</p> <p><b>Deactivated</b> 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 Log out

Communications | **Social Care**

Call Mode: \*Disabled | Report Type: \*Scancom

Telecoms Priority: Call Acknowledge:

21CN Ack Time: \*800ms

Phone Book | Account Numbers

Tel. Recipient 1: Keine

Tel. Recipient 2: Keine

Cancel Submit

- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- View Log
- Keypad

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.



**Note**

SW >= 3.01.11

If the alarm panel was unable to reach the respective recipient during the first dialling attempt, the alarm panel will attempt to reach the respective recipient a maximum of three times.

SW < 3.01.11

The alarm panel attempts to reach the respective recipient max. 16 times.

## Social Care, Account Numbers

**ABUS**
Log out

Communications | Social Care

Call Mode: \*Disabled ▼

Telecoms Priority: ➔

21CN Ack Time: \*800ms ▼

Report Type: \*Scancom ▼

Call Acknowledge:

Phone Book

Account Numbers

Account No P1: 00000000

Account No P3: 00000000

Account No P2: 00000000

Account No P4: 00000000

Cancel

Submit

i+

About

🏠

Status

📄

Devices

➡

Outputs

🌀

Partitions

⚙️

System

☎️

Communications

🛏️

Social Care

📅

View Log

📞

Keypad

Name/function	Explanation (checkbox)
<b>Account No P#</b>	<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.</p> <p>When reporting a social care alarm, the account number can comprise up to 8 digits.</p> <p>For the <b>Scancom</b> and <b>Scanfast</b> log types, the alarm panel uses the last 4 to 6 digits of the saved account number.</p> <p>If you enter 4 digits, the alarm panel only uses these 4 digits.</p> <p>If you enter 5 digits, the alarm panel adds a leading zero in order to lengthen the number of digits to 6.</p> <p>For the <b>Tunstall</b> log type, the alarm panel adds leading zeros to lengthen shorter account numbers to 8 digits.</p>



**Voice dialler**

ABUS Log out

Communications | **Speech Dialler**

Enabled  Call Acknowledge

Telecoms Priority

---

Triggers

Message 1	Message 2
Message 3	Message 4

---

Destinations

Message 1	Message 2
Message 3	Message 4

- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- View Log
- Keypad

SW >=3.00.05

ABUS Log out

Communications | **Speech Dialler**





Enabled  Call Acknowledge



Telecoms Priority

Triggers

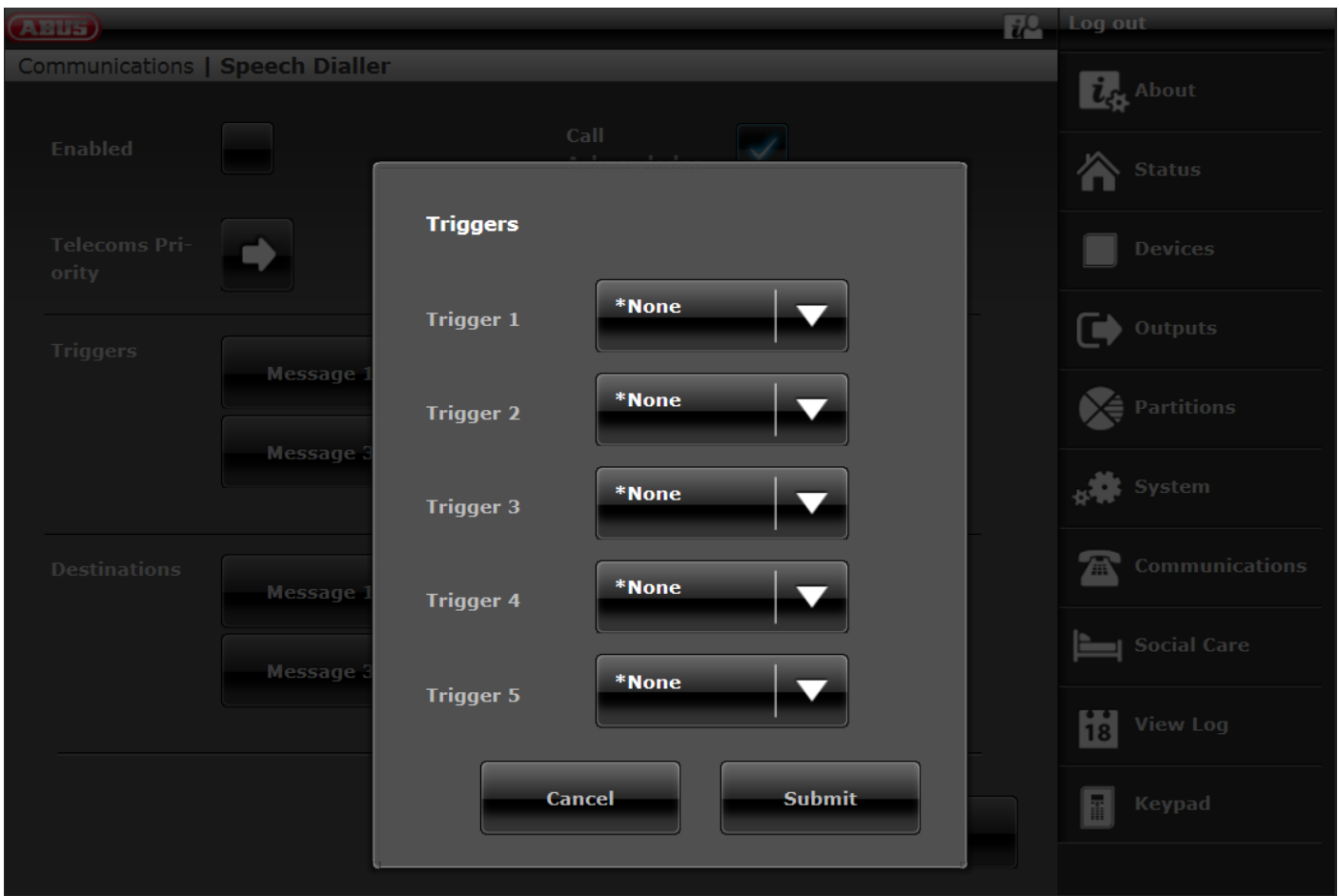
Message 1	Message 2
Message 3	Message 4


- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- Test
- View Log
- Keypad

Name/function	Explanation (checkbox)
<p><b>Enabled</b></p>	<p><b>Enabled</b> The speech dialler function is available.</p> <p><b>Deactivated</b> The speech dialler function is not available.</p> <p></p> <p><b>Note</b> The alarm panel does not send information. A connection is only established when a call is definitely made, starting with a handshake. The information is then sent in accordance with the settings as well as the recorded voice messages for the events.</p>
<p><b>Telecoms Priority</b></p>	<p>Set the order in which the communication methods should be used here.</p> <ul style="list-style-type: none"> <li>• Ethernet            1, 2, 3 or No</li> <li>• PSTN                1, 2, 3 or No</li> <li>• GSM/mobile        1, 2, 3 or No</li> </ul> <p><b>S/W &gt;=3.00.05</b> Set the order in which the communication methods should be used here.</p> <ul style="list-style-type: none"> <li>• Ethernet            1, 2, 3 or No</li> <li>• PSTN                1, 2, 3 or No</li> <li>• Mobile              1, 2, 3 or No</li> </ul> <p></p> <p><b>Note</b> means classic voice transmission (also DTMF and FSK) via a wireless mobile network.</p> <p></p> <p><b>Note</b> The display varies according to the setting via IP gateway the "IP Mobile Setup" menu</p>
<p><b>Call Acknowledge</b></p>	<p><b>Enabled</b> 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 the DTMF button "9": the calling sequence on the alarm panel is terminated.</p> <p></p> <p><b>Note</b> For VoIP, <b>RFC 2833 DTMF Detection</b> must also be activated.</p>

	<p><b>Deactivated</b> If the function is deactivated, the call is treated like a transmission when the called line is answered.</p>
<p><b>Messages</b></p>	<p>Select this item directly in the alarm panel and follow the instructions in the display.</p> <p><b>Home Message (approx. 12 sec.)</b> This message is displayed with every voice transmission. Here you should record the data for the location of the wireless alarm panel (name, street, building number, etc.)</p> <p><b>Message 1-4 (each approx. 8 sec.)</b> Recording the messages for the various events. There are four messages available. For example, record “fire alarm”, “intruder alarm”, ...</p> <p></p> <p><b>Note</b> At least one location message and one event message must be recorded. Do not forget to save the messages after recording.</p> <p></p> <p><b>Note</b> Note the settings during the test call:</p>

Speech Dialler, Triggers



Name/function	Explanation (checkbox)
Event	<p><b>Dropdown selection field for:</b></p> <ul style="list-style-type: none"> <li>• None</li> <li>• Intruder alarm</li> <li>• Panic alarm                             <ul style="list-style-type: none"> <li>○ Use of panic alarms and user threat code</li> </ul> </li> <li>• Fire</li> <li>• Medical Alarm</li> <li>• Social Care Alarm</li> <li>• Social Inactivity</li> <li>• Technical Alarm</li> <li>• Soak Test Fault</li> <li>• Mains Fault</li> <li>• Tamper Activated</li> <li>• Jamming</li> <li>• Test Call</li> </ul> <p> <b>Note</b> Note the settings during the test call:</p>

Speech Dialler, Destinations



Name/function	Explanation (checkbox)
Receiver	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.






**Note**


SW >= 3.01.11

If the alarm panel was unable to reach the respective recipient during the first dialling attempt, the alarm panel will attempt to reach the respective recipient a maximum of three times.

However, every recipient is attempted once via the available path before the alarm panel proceeds with the next attempt.

## Speech Dialler, Test Call

Name/function	Explanation (checkbox)
<p><b>Stat. Test Call</b></p>	<p>Static test call</p> <p>After clicking in a selection field, a pop-up window appears, where the desired rhythm can be selected.</p> <ul style="list-style-type: none"> <li>• Daily</li> <li>• Weekly</li> <li>• Monthly</li> </ul> <p> <b>Note</b></p> <p>For each of the three types of call - daily, weekly and monthly - the alarm panel adds a random minute value. This minute value lies between 0 and 16. The call can, therefore, occur up to 16 minutes after the hour you have entered. This should ensure that the recipient is not flooded with test calls from systems, which all contain the same time.</p> <p> <b>Note</b></p> <p>Note the settings during the event:</p> <p> <b>Note</b></p>

	It is important to record a "test call" voice message in order to differentiate clearly this test call from a normal alarm call.
<b>Hour</b> Input field for the time of the daily test call (format: h or hh) (0 – 23)	 <p><b>Note</b> Only full hours are possible.</p>
<b>Days</b> If "Stat. Test Call" <ul style="list-style-type: none"> <li>• Weekly</li> </ul>	<b>Dropdown selection field for:</b> <ul style="list-style-type: none"> <li>• Sunday</li> <li>• Monday</li> <li>• Tuesday</li> <li>• Wednesday</li> <li>• Thursday</li> <li>• Friday</li> <li>• Saturday</li> </ul>
<b>Days</b> If "Stat. Test Call" <ul style="list-style-type: none"> <li>• Monthly</li> </ul>	Input field for the day of the month on which the test call should be carried out. (1 - 31)

**SMS**
Log out

ABUS
Communications | SMS

Enabled

Telecoms Priority

Triggers
Destinations
Messages
PSTN SMS

Triggers

Message 1

Message 2

Message 3

Message 4

- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- View Log
- Keypad

Name/function	Explanation (checkbox)
<p><b>Enabled</b></p>	<p><b>Enabled</b> The SMS function is available.</p> <p><b>Deactivated</b> The SMS function is not available.</p> <div style="text-align: center; margin-top: 10px;"> </div> <p><b>Note</b> The alarm panel does not send information. A connection is only established when an SMS is actually sent, starting with a handshake. The information is then sent in accordance with the settings as well as the programmed texts and events.</p>
<p><b>Telecoms Priority</b></p>	<p><b>S/W &lt; 3.00.05</b> Set the order in which the communication methods should be used here.</p> <ul style="list-style-type: none"> <li>• PSTN                    1, 2, 3 or No</li> <li>• GSM/mobile           1, 2, 3 or No</li> </ul>



### S/W >=3.00.05

Set the order in which the communication methods should be used here.

- PSTN 1, 2, 3 or No
- Mobile 1, 2, 3 or No



#### Note

means classic SMS transmission via a wireless mobile network.



#### Note

The display varies according to the setting via IP gateway the "IP Mobile Setup" menu.

SMS, Triggers
i
Log out

Communications | SMS

Enabled 
Telecoms Priority

Triggers
Destinations
Messages
PSTN SMS

Triggers

Message 1

Message 2

Message 3

Message 4

Cancel
Submit

i About

🏠 Status

📱 Devices

➔ Outputs

🗺️ Partitions

⚙️ System

☎️ Communications

🛏️ Social Care

📅 View Log

📞 Keypad

Name/function	Explanation (checkbox)
<b>Message #</b>	<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"> <li>Tampers</li> <li>Alarms</li> <li>Set/Unset</li> <li>System</li> <li>Test Call</li> </ul> <div style="text-align: center; margin: 10px 0;"> <p><b>Note</b></p> <p>Note the settings during the test call:</p> </div> <p><b>Tampers</b> Comprises all types of tampering, including system, control panel, components, detectors, siren user code (code tampering) and other components. Examples: all tampering with the alarm panel, detectors, components, supervision (as tampering), jamming (as tampering)</p> <p><b>Alarms</b> Comprises all types of alarms, including 24-hour, fire, intruder, medical, care, test zone fault, zone alarm and zone follow. This also includes the re-setting of this alarm. See also details on the configuration of zone alarms and zone follow.</p> <p><b>Set/Unset</b></p>

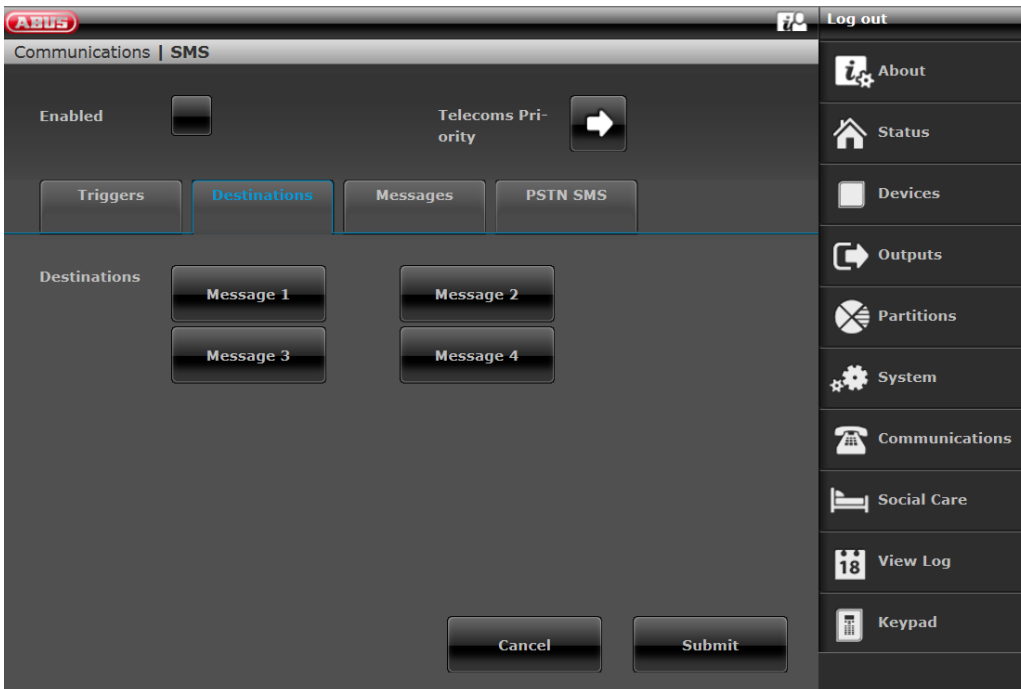
Comprises all types of activations, internal activations and deactivations of partitions via the alarm panel, the control panel, the additional door lock, the remote control, the app or via the other activation and deactivation components.

Examples: Partition x activated/deactivated

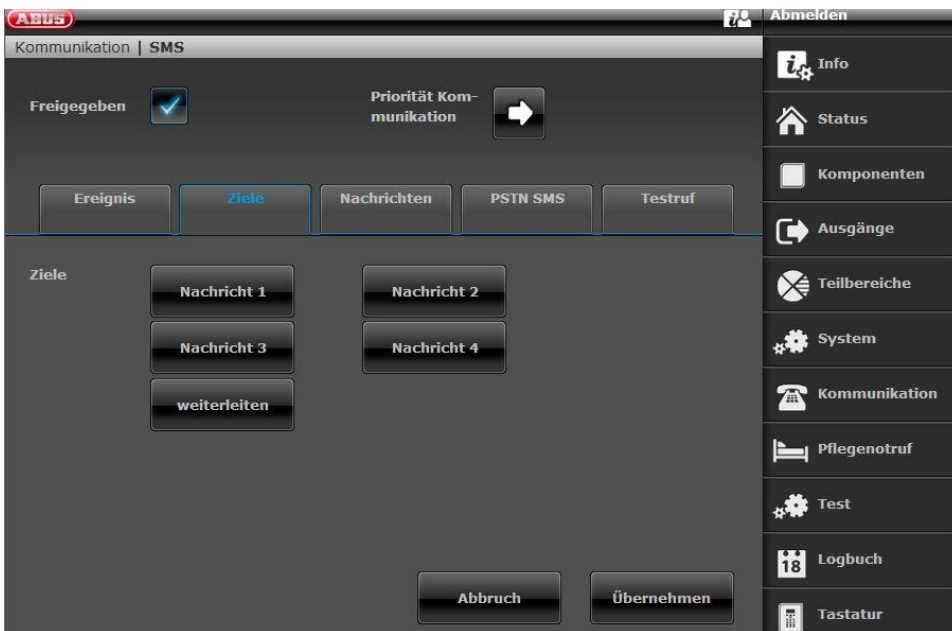
### System

Comprises all types of system events not related to alarms, tampering or activation/deactivation. This includes missing components, supervision (as a fault), jamming (as a fault), communication errors or faults, AC/DC PSU faults, a weak or missing system battery, a weak component battery and an Aux 12 V failure.

## SMS, Destinations



## SW >= 3.01.01



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.
Forwarding	<b>SW &gt;= 3.01.01</b> Allows configuration of the alarm panel so that the SMS messages received by the network operator (e.g. warning messages of low credit) are forwarded to <b>one</b> specific telephone number. If you select Forwarding, the contact list appears. Select a contact from the contact list and then one of the two telephone numbers specified for this contact.

## SMS, Destinations, Message X

The screenshot shows a configuration window for SMS destinations. A modal dialog is open, allowing selection of recipients for a specific message. The dialog contains eight rows, each labeled 'Tel. Recipient' followed by a number from 1 to 8. Each row has a checkbox labeled 'Keine'. At the bottom of the dialog are 'Cancel' and 'Submit' buttons. The background interface shows the 'SMS' configuration page with an 'Enabled' checkbox and a sidebar menu with options like 'About', 'Status', 'Devices', 'Outputs', 'Partitions', 'System', 'Communications', 'Social Care', 'View Log', and 'Keypad'.

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

**Note**

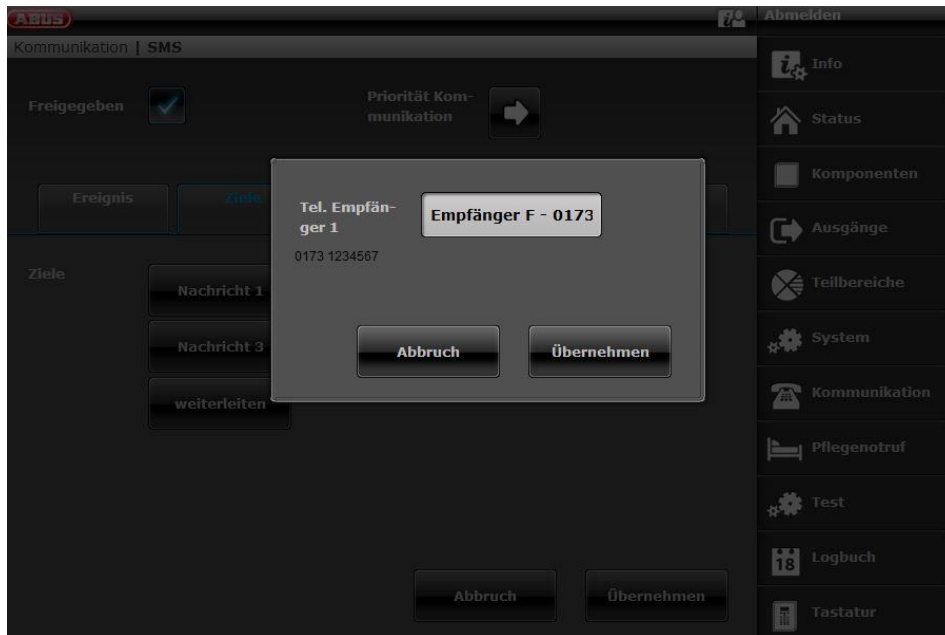
SW >= 3.01.11

If the alarm panel was unable to leave an SMS at the service centre for the respective recipient during the first dialling attempt, the alarm panel will attempt to reach the service centre for the respective recipient and leave an SMS a maximum of three times.

For every unsuccessful attempt via the first path, the alarm panel will attempt to reach the service centre for the respective recipient via the second path a maximum of three times.

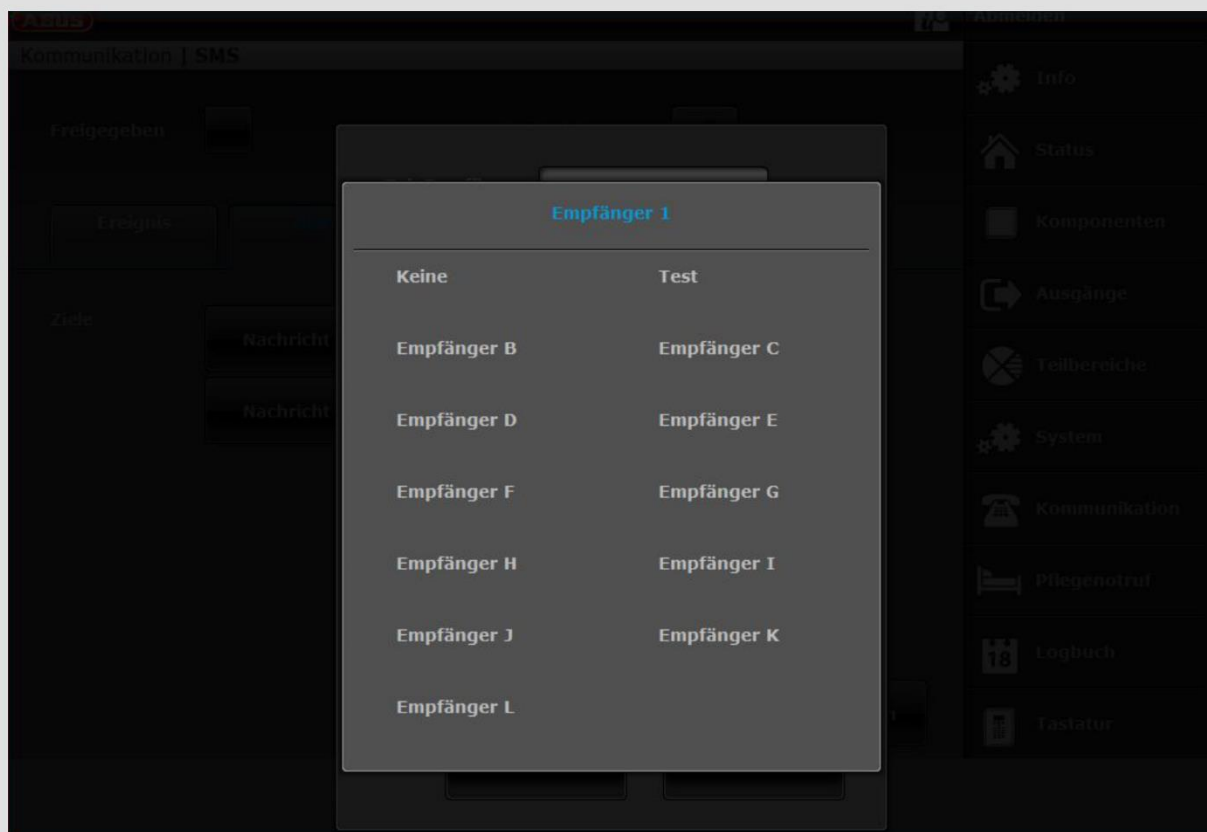
## SMS, Destinations, Forward

SW >= 3.01.01



Name/function	Explanation (checkbox)
Tel Recipient 1	Selection of a recipient for forwarding received SMS messages.

SMS, Destinations, Message, Telephone Recipients



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

**SMS, Messages**

ABUS
7
Log out

Communications | SMS

Enabled

Telecoms Priority

Triggers
Destinations
Messages
PSTN SMS

Home Message

Message 1       Message 2

Message 3       Message 4

- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- 18 View Log
- Keypad

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**
Log out

Communications | **SMS**

Enabled 
Telecoms Priority

Triggers
Destinations
Messages
PSTN SMS

Protocol

\*ETSI Protocol 1

TAP 8N1

TAP 7E1

UCP 8N1

UCP 7E1

\*ETSI Protocol 1

Service Centre Tel.

1470,17094009

Cancel
Submit

Log out

About

Status

Devices

Outputs

Partitions

System

Communications

Social Care

View Log

Keypad



**Note**  
 If you do not have an integrated wireless mobile 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 or first TAE socket and the wireless alarm panel must support the CLIP function.

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

## Configuration

---

Name/function	Explanation (checkbox)
<b>Service Centre Tel.</b>	<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> <b>Note</b> See also private branch exchange with outside line dialling in the chapter: Communication options – <b>mobile without outside line dialling</b></p> <p> <b>Note</b> To send SMS messages from the GSM/wireless mobile network (starting from the wireless mobile 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>
<b>Own Telephone No</b>	<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"><li>• UCP 8N1</li><li>• UCP 7E1</li></ul>

**SMS, test call**

ABUS Log out

Communications | SMS

Enabled  Telecoms Priority

Triggers Destinations Messages PSTN SMS **Test Call**

Static Test Call \*Monthly ▼ Hour

Day

Daily

---

Weekly

---

\*Monthly

About

Status

Devices

Outputs

Partitions

System



Communications

Social Care

Test


View Log

Keypad

Name/function	Explanation (checkbox)
<p><b>Stat. Test Call</b></p>	<p>Static test call</p> <p>After clicking in a selection field, a pop-up window appears, where the desired rhythm can be selected.</p> <ul style="list-style-type: none"> <li>• Daily</li> <li>• Weekly</li> <li>• Monthly</li> </ul> <p> <b>Note</b> For each of the three types of call - daily, weekly and monthly - the alarm panel adds a random minute value. This minute value lies between 0 and 16. The call can, therefore, occur up to 16 minutes after the hour you have entered. This should ensure that the recipient is not flooded with test calls from systems, which all contain the same time.</p> <p> <b>Note</b> Note the settings during the event.</p>

## Configuration

---

<b>Hour</b>	Input field for the time of the daily test call (format: h or hh) (0 – 23)
	 <b>Note</b> Only full hours are possible.
<b>Days</b> If "Stat. Test Call" • Weekly	<b>Dropdown selection field for:</b> <ul style="list-style-type: none"><li>• Sunday</li><li>• Monday</li><li>• Tuesday</li><li>• Wednesday</li><li>• Thursday</li><li>• Friday</li><li>• Saturday</li></ul>
<b>Days</b> If "Stat. Test Call" • Monthly	Input field for the day of the month on which the test call should be carried out. (1 - 31)

**Email**
Log out

ABUS
Communications | Email

Enabled

Telecoms Priority

Triggers

Destinations

Messages

Triggers

Message 1

Message 2

Message 3




Message 4

Cancel

Submit

- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- 18 View Log
- Keypad

Name/function	Explanation (checkbox)						
<p><b>Enabled</b></p>	<p><b>Enabled</b> The email function is available.</p> <p><b>Deactivated</b> The email function is not available.</p> <div style="text-align: center; margin: 10px 0;"> </div> <p><b>Note</b> The alarm panel does not send information. A connection is only established when an e-mail is definitely sent, starting with a handshake. The information is then sent in accordance with the settings (e.g. encrypted or unencrypted) as well as the programmed texts and events.</p>						
	<div style="text-align: center; margin: 10px 0;"> </div> <p><b>Note</b> The alarm panel can send photos from the TVIP41550 camera as an email attachment. If a wireless mobile module is in use, please note the following.</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%;"><b>Data connection</b></td> <td style="width: 50%;"><b>Sending images</b></td> </tr> <tr> <td>2G (GPRS)</td> <td>E-mail <b>without</b> photos in attachment</td> </tr> <tr> <td>4G (LTE)</td> <td>E-mail <b>with</b> photos in attachment</td> </tr> </table>	<b>Data connection</b>	<b>Sending images</b>	2G (GPRS)	E-mail <b>without</b> photos in attachment	4G (LTE)	E-mail <b>with</b> photos in attachment
<b>Data connection</b>	<b>Sending images</b>						
2G (GPRS)	E-mail <b>without</b> photos in attachment						
4G (LTE)	E-mail <b>with</b> photos in attachment						

	<p>In the GPRS network, the data rate is too low to transmit large volumes of data.</p>
<b>Telecoms Priority</b>	<p>Set the order in which the communication methods should be used here.</p> <ul style="list-style-type: none"><li>• Ethernet 1, 2, 3 or No</li></ul> <p><b>S/W &gt;=3.00.05</b></p> <p>Set the order in which the communication methods should be used here.</p> <ul style="list-style-type: none"><li>• Ethernet / IP 1, 2, 3 or No</li><li>• Mobile</li></ul> <p> <b>Note</b> means data transfer according to the setting via IP gateway the "IP Mobile Setup" menu</p> <p> <b>Note</b> SW &gt;= 3.01.16 See also the information on ICMP Ping at "ABUS server" (Communication -&gt; Network -&gt; Network Setup)</p> <p> <b>Note</b> The display varies according to the setting via IP gateway the "IP Mobile Setup" menu.</p>

**Email, Triggers**
Log out

Communications | Email
ABUS

Enabled 
Telecoms Priority

Triggers
Destinations
Messages

Triggers

Message 1

Message 2

Message 3

Message 4

Cancel
Submit

- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- View Log
- Keypad

Name/function	Explanation (checkbox)
<p><b>Message #</b></p>	<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"> <li>• Tampers</li> <li>• Alarms</li> <li>• Set/Unset</li> <li>• System</li> <li>• Test Call</li> </ul> <div style="text-align: center; margin: 10px 0;"> </div> <p><b>Note</b></p> <p>Note the settings during the test call:</p> <p><b>Tampers</b></p> <p>Comprises all types of tampering, including system, control panel, components, detectors, siren user code (code tampering) and other components. Examples: all tampering with the alarm panel, detectors, components, supervision (as tampering), jamming (as tampering)</p> <p><b>Alarms</b></p> <p>Comprises all types of alarms, including 24-hour, fire, intruder, medical, care, test zone fault, zone alarm and zone follow. This also includes the re-setting of this alarm. See also details on the configuration of zone alarms and zone follow.</p>

### Set/Unset

Comprises all types of activations, internal activations and deactivations of partitions via the alarm panel, the control panel, the additional door lock, the remote control, the app or via the other activation and deactivation components.

Examples: Partition x activated/deactivated

### System

Comprises all types of system events not related to alarms, tampering or activation/deactivation. This includes missing components, supervision (as a fault), jamming (as a fault), communication errors or faults, AC/DC PSU faults, a weak or missing system battery, a weak component battery and an Aux 12 V failure.



**Email, Destinations**

ABUS Log out

Communications | **Email**

Enabled  Telecoms Priority

Triggers **Destinations** Messages

Destinations

Message 1 Message 2

Message 3 Message 4

Cancel Submit

- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- View Log
- Keypad

Name/function	Explanation (checkbox)
<b>Message #</b>	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**
Log out

Communications | Email

Enabled

Telecoms Priority

Triggers
Destinations
Messages

Home Message

Message 1

Message 3

Message 2

Message 4

Cancel
Submit

About
Status

Devices
Outputs

Partitions
System

Communications
Social Care

View Log
Keypad

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

**Email, test call**

ABUS Log out

Communications | Email

Enabled  Telecoms Priority

Triggers Destinations Messages **Test Call**

Static Test Call \*Monthly ▼ Hour

Day

Daily

---

Weekly

---

**\*Monthly**

About

Status

Devices

Outputs

Partitions

System



Communications

Social Care

Test


View Log

Keypad

Name/function	Explanation (checkbox)
<p><b>Stat. Test Call</b></p>	<p>Static test call</p> <p>After clicking in a selection field, a pop-up window appears, where the desired rhythm can be selected.</p> <ul style="list-style-type: none"> <li>• Daily</li> <li>• Weekly</li> <li>• Monthly</li> </ul> <p> <b>Note</b></p> <p>For each of the three types of call - daily, weekly and monthly - the alarm panel adds a random minute value. This minute value lies between 0 and 16. The call can, therefore, occur up to 16 minutes after the hour you have entered. This should ensure that the recipient is not flooded with test calls from systems, which all contain the same time.</p> <p> <b>Note</b></p> <p>Note the settings during the event.</p>

## Configuration

---

<b>Hour</b>	Input field for the time of the daily test call (format: h or hh) (0 – 23)
	 <b>Note</b> Only full hours are possible.
<b>Days</b> If "Stat. Test Call" • Weekly	<b>Dropdown selection field for:</b> <ul style="list-style-type: none"><li>• Sunday</li><li>• Monday</li><li>• Tuesday</li><li>• Wednesday</li><li>• Thursday</li><li>• Friday</li><li>• Saturday</li></ul>
<b>Days</b> If "Stat. Test Call" • Monthly	Input field for the day of the month on which the test call should be carried out. (1 - 31)

**Communication options**

ABUS Log out

Communications | Reporting Options

Ethernet Line Fail Response	*Disabled	Ethernet Line Fail Delay	9
PSTN Line Fail Response	*Audible	PSTN Line Fail Delay	9
GSM Line Fail Response	*Audible	GSM Line Fail Delay	9
GSM Omit Digit	<input type="checkbox"/>	Call-out control	<input type="checkbox"/>
Call-in control	<input checked="" type="checkbox"/>		
Rings to Answer	*5 rings	Answer on 1 ring	<input type="checkbox"/>

About

Status

Devices

Outputs

Partitions


System



Communications


Social Care



View Log

Keypad

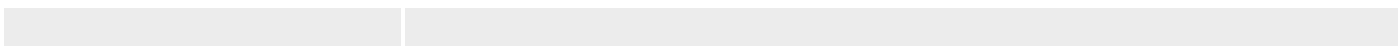
Name/function	Explanation (checkbox)
	<div style="text-align: center;">  </div> <p><b>Note</b> regarding line fail response</p> <p>Use this option to determine how the system should respond if the alarm panel registers a fault at a communication channel. You can configure various settings for Ethernet, PSTN and IP mobile / mobile.</p> <p><b>Audible</b> If the system is deactivated, the event is logged. Capable components will emit a brief audible sound every minute. Inputting a valid access code will silence the acoustic sounders and the display shows a communication channel fault. Despite the displayed communication channel fault, the system can still be activated again. If the system is then activated, the alarm panel logs the event but does not display a notification and does not emit an acoustic signal. The alarm panel cancels all siren delays (ARC/ESCC) programmed in the partition if the communication channel has a fault when the alarm is triggered. <b>Note:</b> ABUS recommends "Acoustic" for the communication channel fault.</p> <p><b>Silent</b> If the system is deactivated, the display shows a communication channel fault. The triangle appears on the bottom right of the display and the alarm panel logs the event. Despite the displayed communication channel fault, the system can still be activated again. If the system is then activated, the alarm panel does not display a notification and does not emit an acoustic signal, but it does log the event. The alarm panel cancels</p>

	<p>all siren delays (ARC/ESCC) programmed in the partition menu if the communication channel has a fault when the alarm is triggered.</p> <p><b>Disabled</b> The alarm panel does not monitor the communication channel.</p>
	<p></p> <p><b>Note</b> regarding line fault delay</p> <p>Use these options to determine how long the alarm panel should wait on one of its communication channels after finding a line fault before generating a warning, initiating communication and activating the line fault outputs. You can configure various settings for Ethernet, PSTN and IP mobile / mobile.</p> <p><b>Note:</b> It may take a few seconds for the alarm panel to detect a line fault. The actual delay between the occurrence of the line fault and the resulting warning is therefore a little longer than the value you have entered.</p>
<b>Ethernet Line Fail Response</b>	<p>Select how Secvest responds if a fault occurs at the Ethernet connection:</p> <ul style="list-style-type: none"> <li>• Disabled</li> <li>• Audible</li> <li>• Silent</li> </ul> <p></p> <p><b>Note</b> SW &gt;= 3.01.16 A WAN error is enforced if a line fault (Ethernet) occurs. This results in an immediate switch to the redundant IP transmission path (when using a wireless mobile module). A WAN test (Ping) is enforced as soon as a line fault (Ethernet) is rectified. This means the WAN test is carried out every 30 minutes or during the transition from line fault to OK. See also the information on ICMP Ping at "ABUS server" (Communication -&gt; Network -&gt; Network Setup)</p>
<b>Ethernet Line Fail Delay</b>	<p>Time in seconds until the alarm system responds to a fault at the Ethernet connection.</p> <p>Value range: 0 to 60 seconds</p>
<b>PSTN Line Fail Response</b>	<p>Select how Secvest responds if a fault occurs with the telephone connection:</p> <ul style="list-style-type: none"> <li>• Disabled</li> <li>• Audible</li> <li>• Silent</li> </ul>
<b>PSTN Line Fail Delay</b>	<p>Time in seconds until the alarm system responds to a fault in the telephone connection.</p> <p>Value range: 0 to 60 seconds</p>

<p><b>IP mobile / mobile Line Fail Response</b> (only when wireless mobile module is used)</p>	<p>Select how Secvest responds if a fault occurs with the wireless mobile connection:</p> <ul style="list-style-type: none"> <li>• Disabled</li> <li>• Audible</li> <li>• Silent</li> </ul>
<p><b>IP mobile / mobile Line Fail Delay</b> (only when wireless mobile module is used)</p>	<p>Time in seconds until the alarm system responds to a fault in the wireless mobile connection.</p> <p>Value range: 0 to 60 seconds</p>
<p><b>Mobile without outside dialling</b> (only when wireless mobile module is used)</p>	<p><b>Enabled</b></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 / wireless mobile connection.</p> <p>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> <p><b>Deactivated</b></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" and "Mobile Omit Digit=Activated" affects numbers to dial for:</p> <ul style="list-style-type: none"> <li>• ARC reporting</li> <li>• Emergency call</li> <li>• Voice dialler</li> </ul> <p></p> <p><b>Note</b></p> <p>SMS messages are normally sent only via GSM/wireless mobile. The normal destination numbers are saved in the phone book: Format of the telephone number: "0123 4567890". With a private branch exchange, the alarm panel is connected to an analogue extension <b>without automatic outside line dialling</b>. 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".</p>

	<p>See also notes in the Contacts chapter.</p> <p>For this purpose, contacts must be saved with two telephone numbers.</p>
<b>Call-out Control</b>	 <p><b>Note</b></p> <p>For more information on the key combinations on the telephone and the corresponding functions, see Chapter 11.4 "Operation via telephone" in the user manual.</p> <p><b>Enabled</b></p> <p>When this option is activated, the user can control the system remotely while answering a call from the alarm system.</p> <p><b>Deactivated</b></p> <p>When this option is deactivated, the user can still always use the commands for the speech dialler but not for the remote control.</p>
<b>Call-in Control</b>	 <p><b>Note</b></p> <p>For more information on the key combinations on the telephone and the corresponding functions, see Chapter 11.4 "Operation via telephone" in the user manual.</p> <p><b>Enabled</b></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><b>Deactivated</b></p> <p>When this option is deactivated, the user can no longer call the alarm system remotely.</p>
<b>Rings to Answer</b> (only when "Call-in control" is activated)	<p>Select when the wireless alarm panel answers a call.</p> <ul style="list-style-type: none"> <li>• 3 rings</li> <li>• 5 rings</li> <li>• 7 rings</li> <li>• 10 rings</li> <li>• 15 rings</li> <li>• 255 rings</li> </ul> <p><b>Note</b></p> <p>If the value is set to 255, the alarm panel never answers the call.</p>
<b>Answer after first ring</b> (only when "Call-in control" is activated)	<p><b>Enabled</b></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. 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><b>Deactivated</b></p> <p>If this function is deactivated, the "Rings to Answer" function takes over from the first call.</p>





## Contacts

ABUS Communications | Contacts

Recipient 1	Recipient 1	Recipient 2	Recipient 2
Recipient 3	Recipient 3	Recipient 4	Recipient 4
Recipient 5	Recipient 5	Recipient 6	Recipient 6
Recipient 7	Recipient 7	Recipient 8	Recipient 8
Recipient 9	Recipient 9	Recipient 10	Recipient 10
Recipient 11	Recipient 11	Recipient 12	Recipient 12

Cancel

- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- View Log
- Keypad

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

Click on a user in the recipient list to open their contact profile. Enter the corresponding details here.

S/W <2.00.00

ABUS Communications | Contacts

Name: Recipient 1

Telephone Number 1:

Telephone Number 2:

Email:

IP Address:

SIP User ID:

Cancel Submit

Cancel

- About
- Status
- Devices
- Outputs
- Partitions
- System
- Communications
- Social Care
- View Log
- Keypad

S/W &gt;=2.00.00

Name	<input type="text" value="Recipient I"/>				
Partitions	<input checked="" type="checkbox"/> 1	<input checked="" type="checkbox"/> 2	<input checked="" type="checkbox"/> 3	<input checked="" type="checkbox"/> 4	<input type="button" value="All Partitions"/>
Telephone Number 1	<input type="text"/>				
Telephone Number 2	<input type="text"/>				
Email	<input type="text"/>				
IP Address	<input type="text"/>				
SIP User ID	<input type="text"/>				
	<input type="button" value="Cancel"/>		<input type="button" value="Submit"/>		

**The recipient can be assigned to partitions.**

This stipulates that the recipient will only receive a message when an event occurs in the specified partition.

**Note**

This assignment of partitions is only applicable to voice diallers, text messages and email, and not for ARC/ESCC connection.

**Note**

Events not directly relating to a single partition (e.g. the double-key function on the alarm panel for fire, intrusion, medical emergency and care alarms) will be assigned to partition 1.

**Note**

Intrusion (remote control), intrusion (pendant), medical emergency (pendant) and care alarm (pendant).

Events triggered by these user-controlled components are transmitted to the recipient where the selected partition matches the partition authorisation for that user.



### Note

Wireless control panel

Double-key function for fire, intrusion, medical emergency and care alarms

Events triggered by these components are transmitted to the recipient where the selected partition matches the assignment of partitions for that control device.



### Note

#### SIP User (User) ID

Format

S/W  $\geq$ 2.00.00

Phone number

+49 (0)82071234567

ID, if the recipient has an account with the same SIP service provider

9876543

S/W  $<$ 2.00.00

Phone number

+4982071234567@sipgate.de

sipgate.de is the individual SIP service provider, as SIP server name

ID, if the recipient has an account with the same SIP service provider

9876543@sipgate.de



### Note

When using mobile SMS and PSTN SMS as well as private branch exchange with outside line dialling, two call numbers must be saved for the respective recipient.

See also private branch exchange with outside line dialling in the chapter:

Communication options – **mobile without outside line dialling**

S/W >=3.00.05

Name

Partitions  1  2  3  4

Speech/SMS/Email  Un-set  Set  Part Set

Telephone Number 1

Telephone Number 2

Email

IP Address


SIP User ID

Name/function	Explanation (checkbox)
<b>Voice/SMS/Email</b>	<p>Events are selected for and assigned to the speech dialler, the sending of SMS and the sending of emails.</p> <p>Events may come from the following groups:</p> <ul style="list-style-type: none"> <li>• Tampers</li> <li>• Alarms</li> <li>• Set/Unset</li> <li>• System</li> </ul> <p>The selected events are only transmitted to this contact when:</p> <ul style="list-style-type: none"> <li>• The event originates from one of the selected partitions</li> <li>• The partition has a selected status such as Disarmed and/or Armed and/or Indoor armed</li> <li>• The contact for these events is assigned as recipient</li> </ul>
<b>Deactivated</b>	<p><b>Yes</b> Events will be transmitted to this contact when the partition is disarmed</p> <p><b>No</b> Events will <b>not</b> be transmitted to this contact when the partition is disarmed</p>

## Configuration

<b>Activated</b>	<p><b>Yes</b> Events will be transmitted to this contact</p> <p><b>No</b> Events will <b>not</b> be transmitted to this contact</p>
<b>Part set</b>	<p><b>Yes</b> Events will be transmitted to this contact</p> <p><b>No</b> Events will <b>not</b> be transmitted to this contact</p>

<b>Example 1</b>	
<b>Partitions</b>	1=Yes, 2=Yes, 3=Yes, 4=Yes
<b>Voice/SMS/Email</b>	Disarmed=Yes, Armed=No, Part Set=No
<b>Event</b>	Fire in Partition 1
<b>Partition 1 is</b>	
<b>Deactivated</b>	No voice call, no SMS, no email to this contact
<b>Activated</b>	Voice call, SMS and email to this contact
<b>Part set</b>	No voice call, no SMS, no email to this contact

<b>Example 2</b>	
<b>Partitions</b>	1=Yes, 2=Yes, 3=Yes, 4=Yes
<b>Voice/SMS/Email</b>	Deactivated=Yes, Activated=No, Part Set=No
<b>Event</b>	Alarm panel has been opened (sabotaged).
<b>Partitions 1 and 2 are</b>	Note: Partitions 3 and 4 are <b>not</b> in use.
<b>Activated</b>	<b>Voice call, SMS and email to this contact!</b>
	 <p><b>Note</b> Normally, there should be no communication sent to this contact, because Armed is set to No. However, housing sabotage has been reported for all four partitions.     Partition 1: Housing open     Partition 2: Housing open     Partition 3: Housing open     Partition 4: Housing open Partitions 3 and 4 are <b>Disarmed</b> in this case, because they are not in use. Because Disarmed=Yes is communicated. The correct setting for this case is illustrated in Example 3.</p>

<b>Example 3</b>	
------------------	--

<b>Partitions</b>	1=Yes, 2=Yes, 3= <b>No</b> , 4= <b>No</b>
<b>Voice/SMS/Email</b>	Deactivated=Yes, Activated=No, Part Set=No
<b>Event</b>	Alarm panel has been opened (sabotaged).
<b>Partitions 1 and 2 are</b>	Note: Partitions 3 and 4 are <b>not</b> in use.
<b>Activated</b>	<b>No</b> voice call, <b>no</b> SMS, <b>no</b> email to this contact

**Emergency call**

**ABUS**
 **Log out**

**Social Care**

**Start Monitoring Hr**

**End Monitoring Hr**

**Monitoring Interval**

**Speech Volume**

**Log out**

**About**

**Status**

**Devices**

**Outputs**

**Partitions**

**System**

**Communications**

**Social Care**

**View Log**

**Keypad**

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





## Test

Select the corresponding function.  
Via web interface with S/W >=2.00.00.

An overview of the different functions can be found in the table below.



# Configuration

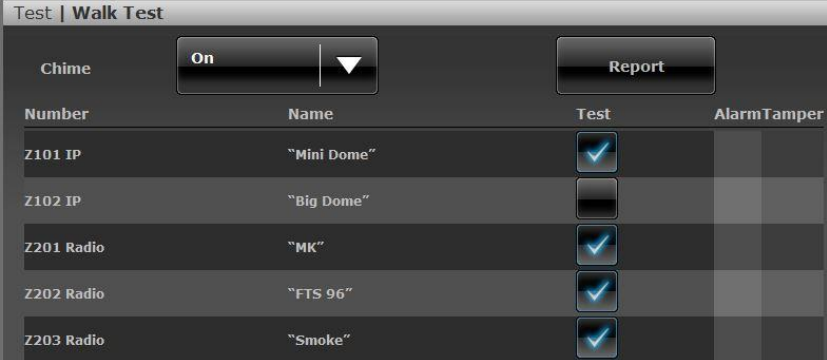
SW >= 3.01.01

The screenshot displays the ABUS configuration interface. At the top left, the 'ABUS' logo is visible. The main area is titled 'Test' and contains a grid of 20 buttons, each with an icon and a label: Walk Test, Keypad, External Sirens, Int.Sirens, Sounder Module, Loudspeakers, Control Devices, Door Locks, Signal Strengths, Outputs, Prox Tags, Remotes, Pendants, ARC Reporting, Social Care, Speech Dialler, SMS, Email, Zone Resistances, and Panel PSU. A single 'RF Repeaters' button is located below the grid. On the right side, there is a 'Log out' button and a vertical menu with the following items: About, Status, Devices, Outputs, Partitions, System, Communications, Social Care, Test, View Log, and Keypad.

S/W &gt;= 3.01.14

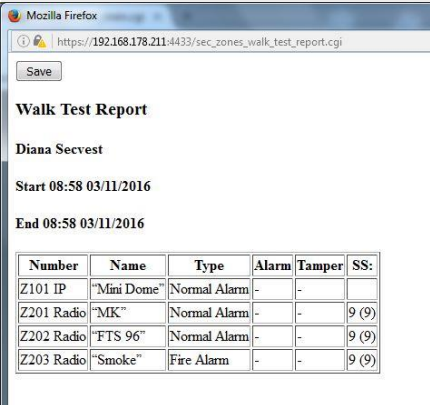
**Note**

Test call to external recipients. Please inform them in advance and let them know that it is just a test call.  
Test call e.g. receiving centre, language call, SMS, email.

Function	Meaning																														
<b>Walk Test</b>	<p><b>Bell</b></p> <ul style="list-style-type: none"> <li>On: An info tone sounds when a detector is operated.</li> <li>Off: No info tone sounds.</li> </ul> <p>All detectors belonging to the system can be tested here. The zones can be individually selected during test. Activate all detectors in the building one after the other. If a detector is triggered the alarm panel emits two signal tones The Alarm column will display whether a detector has detected an alarm. The tamper column will display whether a tamper contact has been triggered.</p>  <p>The screenshot shows a web interface titled "Test   Walk Test". It features a "Chime" dropdown menu set to "On" and a "Report" button. Below is a table with columns: Number, Name, Test, Alarm, and Tamper. The table contains five rows of detector information:</p> <table border="1"> <thead> <tr> <th>Number</th> <th>Name</th> <th>Test</th> <th>Alarm</th> <th>Tamper</th> </tr> </thead> <tbody> <tr> <td>Z101 IP</td> <td>"Mini Dome"</td> <td><input checked="" type="checkbox"/></td> <td></td> <td></td> </tr> <tr> <td>Z102 IP</td> <td>"Big Dome"</td> <td><input type="checkbox"/></td> <td></td> <td></td> </tr> <tr> <td>Z201 Radio</td> <td>"MK"</td> <td><input checked="" type="checkbox"/></td> <td></td> <td></td> </tr> <tr> <td>Z202 Radio</td> <td>"FTS 96"</td> <td><input checked="" type="checkbox"/></td> <td></td> <td></td> </tr> <tr> <td>Z203 Radio</td> <td>"Smoke"</td> <td><input checked="" type="checkbox"/></td> <td></td> <td></td> </tr> </tbody> </table>	Number	Name	Test	Alarm	Tamper	Z101 IP	"Mini Dome"	<input checked="" type="checkbox"/>			Z102 IP	"Big Dome"	<input type="checkbox"/>			Z201 Radio	"MK"	<input checked="" type="checkbox"/>			Z202 Radio	"FTS 96"	<input checked="" type="checkbox"/>			Z203 Radio	"Smoke"	<input checked="" type="checkbox"/>		
Number	Name	Test	Alarm	Tamper																											
Z101 IP	"Mini Dome"	<input checked="" type="checkbox"/>																													
Z102 IP	"Big Dome"	<input type="checkbox"/>																													
Z201 Radio	"MK"	<input checked="" type="checkbox"/>																													
Z202 Radio	"FTS 96"	<input checked="" type="checkbox"/>																													
Z203 Radio	"Smoke"	<input checked="" type="checkbox"/>																													

**Walk test (cont.)** **Report**

The test results can also be printed out and saved via the web interface.



The screenshot shows a Mozilla Firefox browser window displaying a "Walk Test Report" page. The report includes the following information:

- Start: 08:58 03/11/2016
- End: 08:58 03/11/2016

The report contains a table with the following data:

Number	Name	Type	Alarm	Tamper	SS:
Z101 IP	"Mini Dome"	Normal Alarm	-	-	
Z201 Radio	"MK"	Normal Alarm	-	-	9 (9)
Z202 Radio	"FTS 96"	Normal Alarm	-	-	9 (9)
Z203 Radio	"Smoke"	Fire Alarm	-	-	9 (9)

## Alarm panel

### System

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".

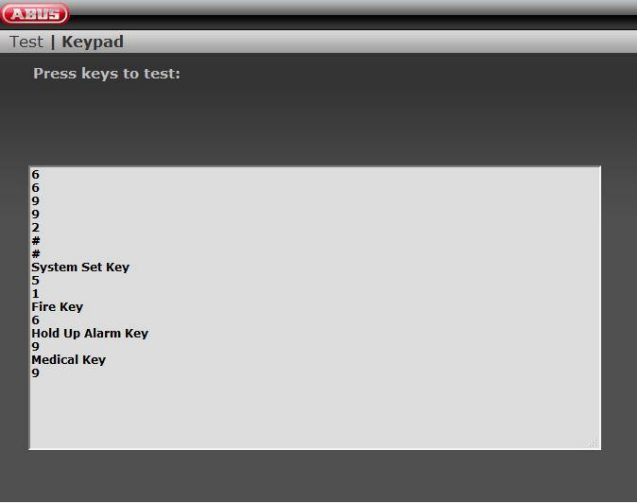


### Partitions

- Detectors from a specific partition can be tested here.
- Once the partitions are selected only the detectors in the selected partitions are displayed.

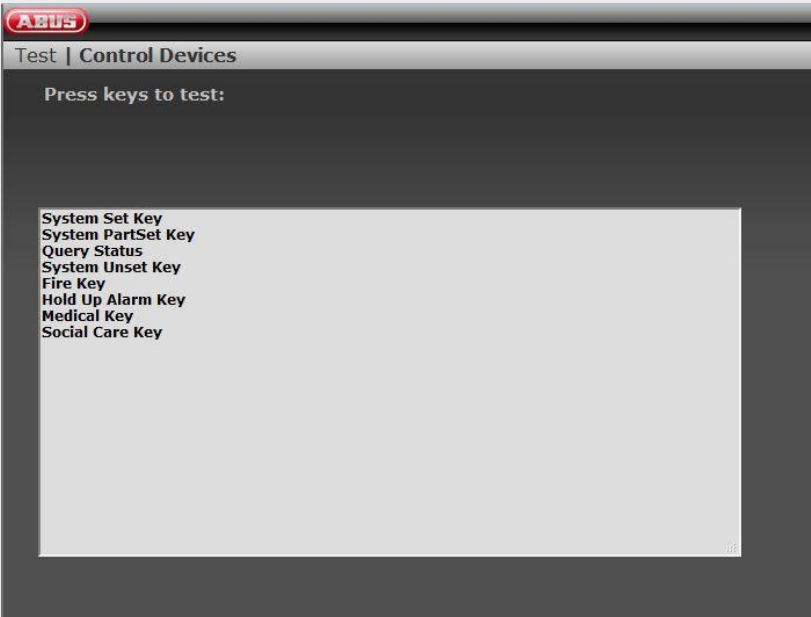
### Zones


- Selected detectors can be tested here.

A list of all detectors appears. Select the detectors to be tested with **Yes**.

Function	Meaning
<p><b>Keypad</b></p>	<p>Testing the keypad is possible both on the alarm panel and the web interface.            Press all buttons on the keypad one after the other.            The corresponding character or button function is shown on the display in response.            Press the dual keys (fire alarm, hold up alarm, medical emergency or social care alarm) at the same time to test them. The function of the key combination is shown on the display in response.</p>  <p>S/W &gt;= 2.01.08            Press the dual keys for the cleaning mode (left and right menu keys) simultaneously to test. The function of the key combination is shown on the display in response.</p>  <p><b>Note</b>            Cleaning mode will not be carried out. You can find instructions for cleaning mode in the user guide.</p>
<p><b>Sirens &amp; Sounders</b></p>	<p>Testing of sirens and sounders is carried out in the web interface in the same manner as on the alarm panel.</p> <p><b>Int.Sirens</b></p> <ul style="list-style-type: none"> <li>• The sounders on the alarm panel, info module, indoor siren and wireless control device are actuated.</li> </ul> <p><b>Ext. Radio Sirens</b></p> <ul style="list-style-type: none"> <li>• The sounders for the wireless external sirens are actuated.</li> </ul>  <p><b>Note</b>            For FUSG50100/1 (siren software 1.10.2)            If the housing of the external siren is <b>closed</b>, the strobe <b>and</b> the siren are switched on.            If the housing of the external siren is <b>open</b>, <b>only</b> the strobe is switched on.</p> <p><b>Sounder Module</b></p> <ul style="list-style-type: none"> <li>• The sounders for the external sirens are actuated. External siren in connection with the wireless universal module (WUM) as a "Sounder Module".</li> </ul> <p><b>Loudspeaker</b></p> <ul style="list-style-type: none"> <li>• Select "Play/Stop" to hear all existing messages in the system one after the other.</li> </ul>



Function	Meaning
<b>Wireless control panel</b>	<p>Testing of wireless control panels is carried out in the web interface in the same manner as on the alarm panel.</p> <p>Press the function buttons on the wireless control device one after the other.</p> <p>Wait 2 to 3 seconds between each button so that the control device can send each message.</p> <p>A corresponding letter appears on the display in response:</p> <p>A = "arm" button (closed lock)</p> <p>C = "internal arm" button (*)</p> <p>D= "query status" button (?)</p> <p>B = "disarm" button (open lock)</p> <p>On the <b>Web</b> you will also see:</p> <ul style="list-style-type: none"> <li>Arm system key</li> <li>Arm system internally key</li> <li>Status query</li> <li>Disarm system key</li> </ul> <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"> <li>• Press : 1234?</li> <li>• Displayed : 1234D (status query)</li> </ul> <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> <p>P = dual keys hold up</p> <p>M = dual keys medical emergency</p> <p>H = dual keys social care alarm</p> <p>On the <b>Web</b> you will also see:</p> <ul style="list-style-type: none"> <li>Fire key</li> <li>Intrusion key</li> <li>Medical emergency call key</li> <li>Social Care Key</li> </ul> <p>The lower "*" and "#" button on the control device cannot be tested.</p> 

Function	Meaning																				
<b>Door locks</b>	<p>Testing of door locks is carried out in the web interface in the same manner as on the alarm panel.</p> <p><b>Select the door lock to be tested.</b></p> <p>Operate the corresponding door lock.</p> <p>After unlocking, "Unlocked" appears on the display.</p> <p>After locking, "Locked" appears on the display.</p> <ul style="list-style-type: none"> <li>• Secvest key: press the button and then lock.</li> <li>• Additional door lock: do not press the button. Then lock.</li> </ul> <p><b>Note</b></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.</p>																				
<b>Signal Strengths</b>	<p>This option can be used to check the received signal strengths of all wireless components of the system.</p> <p></p> <p><b>Note</b></p> <p><b>To ensure good wireless communication, you must have a signal strength greater than 3. During the test, the reception power of the wireless alarm panel is reduced by 6 dB.</b> The Secvest wireless alarm panel is sensitive to approx. -110 dBm at a signal-to-noise ratio of 12 dB.</p> <p>The following level values apply for the signal strength display on the Secvest:</p> <table border="0"> <tr><td>0</td><td>&lt; -101 dBm</td></tr> <tr><td>1</td><td>&lt; -98 dBm</td></tr> <tr><td>2</td><td>&lt; -95 dBm</td></tr> <tr><td>3</td><td>&lt; -92 dBm</td></tr> <tr><td>4</td><td>&lt; -89 dBm</td></tr> <tr><td>5</td><td>&lt; -86 dBm</td></tr> <tr><td>6</td><td>&lt; -83 dBm</td></tr> <tr><td>7</td><td>&lt; -80 dBm</td></tr> <tr><td>8</td><td>&lt; -77 dBm</td></tr> <tr><td>9</td><td>≥ -77 dBm</td></tr> </table> <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>S/W &lt;2.00.00</p> <p>The signal strength of the repeated signal from the WAM is the same as that from each WAM.</p> <p>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.</p> <p>S/W ≥2.00.00</p> <p>The signal strength of the direct signal from each component is displayed in the right-hand column (WEB column direct).</p> <p>The signal strength of the repeated signal from the WAM or the RF repeater is displayed in the left-hand column (WEB column repeater).</p> <p><b>Resetting signal strengths to begin a new measurement.</b></p> <p>WEB</p> <p>Click on the line for the desired component and follow the instructions on the screen.</p> <p>Click on "Reset ALL" and follow the instructions on the screen. This will clear the recorded signal strengths for the entire list.</p>	0	< -101 dBm	1	< -98 dBm	2	< -95 dBm	3	< -92 dBm	4	< -89 dBm	5	< -86 dBm	6	< -83 dBm	7	< -80 dBm	8	< -77 dBm	9	≥ -77 dBm
0	< -101 dBm																				
1	< -98 dBm																				
2	< -95 dBm																				
3	< -92 dBm																				
4	< -89 dBm																				
5	< -86 dBm																				
6	< -83 dBm																				
7	< -80 dBm																				
8	< -77 dBm																				
9	≥ -77 dBm																				



Alarm panel

# key

Press this key to delete the recorded signal strengths for the selected component.

\* key

Press this key to delete the recorded signal strengths for the entire list.



**Note**

Deletion and updating can occur very quickly in the HyMo.

**Signal strengths (cont.)**

**Detectors**

The display shows the signal strength of each taught-in detector.

S/W <2.00.00 The zone names are displayed. To view the zone numbers, press the right menu key

**Wireless control panel**

The display shows the signal strength of each taught-in control device.

**External Sirens**

The display shows the signal strength of each taught-in wireless external siren.

**Indoor sounder**

The display shows the signal strength of each taught-in indoor sounder.

**WAM**

The display shows the signal strength of each taught-in WAM.

**Door locks**

The display shows the signal strength of each taught-in door lock.

**Hybrid module**

The display shows the signal strength of each taught-in hybrid module.

Here you can find 2 displays

**Signal on the alarm panel**

This is the signal strength of the hybrid module at the alarm panel.

**Signal on the HyMo**

This is the signal strength of the alarm panel at the hybrid module.



**Note**

Both signal strengths are approximately the same. However, the signal strengths “alarm panel -> HyMo” and “HyMo -> alarm panel” can deviate slightly from each other. The reasons for this are:

different antennas on the alarm panel and HyMo

different radio wave propagation characteristics in the different directions

The screenshot shows the 'Test | Signalstärken' (Test | Signal Strengths) section of the ABUS configuration software. It features a navigation bar with tabs for 'Funk Zonen', 'Funk Bedienteil', 'Außensirene', 'Innen-SG', 'UVM', 'Türschlösser', and 'Hybrid Module'. The 'Hybrid Module' tab is active, displaying a table with columns for 'Nummer', 'Name', 'Repeater', and 'Direkt'. The table is divided into two sections: 'Signal an der Zentrale:' and 'Signal am HyMo:'. Each section contains two rows for 'HyMo 1' and 'HyMo 2', showing signal strength values in parentheses. A 'ALLE zurücksetzen' (Reset all) button is located at the bottom right of the table area.

Nummer	Name	Repeater	Direkt
<b>Signal an der Zentrale:</b>			
HyMo 1	"HyMo 1"	9(9)	9(9)
HyMo 2	"HyMo 2"	9(9)	9(2)
<b>Signal am HyMo:</b>			
HyMo 1	"HyMo 1"	9(9)	9(9)
HyMo 2	"HyMo 2"	9(9)	9(9)

### RF repeater (only alarm panel)

The display shows the signal strength of each taught-in RF repeater.

Under RF repeater below you will find clarifications for the display on the WEB.

### RF repeater components (only alarm panel)

Under RF repeater below you will find clarifications for the display on the WEB.

The display shows the signal strength of each assigned component to each RF repeater on the RF repeater.

Under RF repeater below you will find clarifications for the display on the WEB.

#### Repeat alarm panel

You can find the signal strength of the received messages from the **alarm panel** on the repeater here.

#### Repeat detectors

You can find the signal strength of the received messages from the **detectors** on the repeater here.

#### Repeat wireless control panel

You can find the signal strength of the received messages from the **wireless control panel** on the repeater here.

#### Repeat indoor sounder

You can find the signal strengths of the received messages from the **indoor sounder** on the repeater here.

#### Repeat outdoor sirens

	<p>You can find the signal strength of the received messages from the <b>external sirens</b> on the repeater here.</p> <p><b>Repeat door locks</b> You can find the signal strength of the received messages from the <b>door locks</b> on the repeater here.</p> <p><b>Repeat HyMo</b> You can find the signal strength of the received messages from the <b>hybrid modules</b> on the repeater here.</p>
<b>Outputs</b>	<p><b>Radio Outputs</b></p> <ul style="list-style-type: none"> <li>• Use this option to check all configured radio outputs.</li> </ul> <p><b>Wired Outputs</b></p> <ul style="list-style-type: none"> <li>• Use this option to check all configured wired outputs.</li> </ul> <p><b>HyMo outputs</b></p> <ul style="list-style-type: none"> <li>• Use this option to check all configured HyMo wired outputs.</li> </ul> <p>After exiting the menu, all outputs switch back to their basic configured state.</p>
<b>Prox Tag</b>	<p>Testing of chip keys is carried out in the web interface in the same manner as on the alarm panel. Move the Prox Tag across the reader area at the bottom of the alarm panel (where the ABUS logo is). The following information appears on the display:</p> <ul style="list-style-type: none"> <li>• which user is assigned to this Prox Tag or</li> <li>• that the Prox Tag is not recognised by the alarm panel.</li> </ul>
<b>Remote controls</b>	<p>Testing of the remote control is carried out in the web interface in the same manner as on the alarm panel. Press a button on the remote control. The following information appears on the display:</p> <ul style="list-style-type: none"> <li>• the consecutive number of the remote control</li> <li>• a letter or character corresponding to the pressed key <ul style="list-style-type: none"> <li>A = "arm" key (closed lock)</li> <li>* = "internally arm" key or key for activating a "User Defined" output (*)</li> <li>? = "query status" key (?)</li> <li>D = "disarm" key (open lock)</li> </ul> </li> <li>• which user is assigned to this remote control</li> <li>• the function of the pressed button <ul style="list-style-type: none"> <li>- Set All</li> <li>- Prt Set All or Output On (Off or Toggle) xyz</li> <li>- Query Status</li> <li>- Unset All</li> </ul> </li> <li>• the received signal strength (RSSI)</li> </ul> <p><b>Example</b> Remote 001,D:User 002 Complete disarming RSSI: 9</p>

Function	Meaning
<b>Emergency buttons</b>	<p>Testing of the remote control is carried out in the web interface in the same manner as on the alarm panel.</p> <p>Press the button on a pendant.</p> <p>The following information appears on the display</p> <ul style="list-style-type: none"><li>• which user is assigned to this emergency button</li><li>• the function of this pendant<ul style="list-style-type: none"><li>HUA = hold up alarm</li><li>Medical = medical emergency</li><li>PFN alarm = social care alarm</li></ul></li><li>• the received signal strength (RSSI)</li></ul> <p><b>Example</b></p> <p>User: User 002</p> <p>Func: Medical</p> <p>RSSI: 9</p>
<b>ARC reporting</b>	<p>Testing of the ARC reporting function is carried out in the web interface in the same manner as on the alarm panel.</p> <p>ARC Reporting must be activated and the contact must be saved in the phone book.</p> <p>Installer Mode-&gt;Communications-&gt;ARC Reporting -&gt;Call Mode -&gt;Single (or Alternate)</p> <p>A list of the available connected transmission paths can be seen:</p> <p><b>Ethernet, Ethernet / IP Mobile</b></p> <ul style="list-style-type: none"><li>• When this is selected, the 2 possible configured recipients (IP Recipient 1, IP Recipient 2) are displayed with their contact names as stored in the phone book.</li><li>• Scroll to the desired contact. Press the "Select" or "Start" key in the web interface.</li><li>• The alarm panel sends a test call to this recipient.</li><li>• The event (or trigger) "Test" is sent according to the set protocol.</li></ul> <p><b>PSTN</b></p> <ul style="list-style-type: none"><li>• When this is selected, the 2 possible configured recipients (Tel Recipient 1, Tel Recipient 2) are displayed with their contact names as stored in the phone book.</li><li>• Scroll to the desired contact. Press the "Select" or "Start" key in the web interface.</li><li>• The alarm panel sends a test call to this recipient.</li><li>• The event (or trigger) "Test" is sent according to the set protocol.</li></ul> <p><b>GSM / Mobile</b></p> <ul style="list-style-type: none"><li>• When this is selected, the 2 possible configured recipients (Tel Recipient 1, Tel Recipient 2) are displayed with their contact names as stored in the phone book.</li><li>• Scroll to the desired contact. Press the "Select" or "Start" key in the web interface.</li><li>• The alarm panel sends a test call to this recipient.</li><li>• The event (or trigger) "Test" is sent according to the set protocol.</li></ul> <p>During the test call a series of progress messages appear on the display.</p> <p>If the test call was not successful, the display shows a brief message with the cause of the error.</p>

Function	Meaning
<b>Emergency call</b>	<p>Testing of the nursing emergency call function is carried out in the web interface in the same manner as on the alarm panel.</p> <p>Nursing emergency call must be activated and the contact must be saved in the phone book.            Installer Mode-&gt;Communications-&gt;ARC Reporting -&gt;Call Mode -&gt;Single (or Alternate)</p> <p>A list of the available connected transmission paths can be seen:</p> <p><b>PSTN</b></p> <ul style="list-style-type: none"> <li>• When this is selected, the 2 possible configured recipients (Tel Recipient 1, Tel Recipient 2) are displayed with their contact names as stored in the phone book.</li> <li>• Scroll to the desired contact. Press the "Select" or "Start" key in the web interface.</li> <li>• The alarm panel sends a test call to this recipient.</li> <li>• The event (or trigger) "Test" is sent according to the set protocol.</li> </ul> <p><b>GSM / Mobile</b></p> <ul style="list-style-type: none"> <li>• When this is selected, the 2 possible configured recipients (Tel Recipient 1, Tel Recipient 2) are displayed with their contact names as stored in the phone book.</li> <li>• Scroll to the desired contact. Press the "Select" or "Start" key in the web interface.</li> <li>• The alarm panel sends a test call to this recipient.</li> <li>• The event (or trigger) "Test" is sent according to the set protocol.</li> </ul> <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>

Function	Meaning
<b>Voice dialler</b>	<p>Speech Dialler must be activated. Installer Mode-&gt;Communications-&gt;Speech Dialler-&gt;Call Mode-&gt;Enabled</p> <p>A list of the available connected transmission paths can be seen:</p> <p><b>Ethernet</b></p> <ul style="list-style-type: none"><li>• Once this has been selected, enter a valid SIP User ID.</li><li>• e.g. +498207123456789@sipgate.de</li><li>• Press the "OK" button.</li><li>• 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".</li></ul> <p><b>S/W &gt;=2.00.00</b></p> <ul style="list-style-type: none"><li>• When this is selected, the configured recipients are displayed with their contact names as stored in the phone book.</li><li>• Scroll to the desired contact. Press the "Select" or "Start" key in the web interface.</li><li>• The alarm panel sends a test call to this recipient.</li></ul> <p><b>PSTN</b></p> <ul style="list-style-type: none"><li>• When this is selected, enter a number to dial.</li><li>• Press the "OK" button.</li><li>• 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".</li></ul> <p><b>S/W &gt;=2.00.00</b></p> <ul style="list-style-type: none"><li>• When this is selected, the configured recipients are displayed with their contact names as stored in the phone book.</li><li>• Scroll to the desired contact. Press the "Select" or "Start" key in the web interface.</li><li>• The alarm panel sends a test call to this recipient.</li></ul> <p><b>GSM / Mobile</b></p> <ul style="list-style-type: none"><li>• When this is selected, enter a number to dial.</li><li>• Press the "OK" button.</li><li>• 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".</li></ul> <p><b>S/W &gt;=2.00.00</b></p> <ul style="list-style-type: none"><li>• When this is selected, the configured recipients are displayed with their contact names as stored in the phone book.</li><li>• Scroll to the desired contact. Press the "Select" or "Start" key in the web interface.</li><li>• The alarm panel sends a test call to this recipient.</li></ul> <p>If "Call Acknowledge" is activated:</p> <ul style="list-style-type: none"><li>• The recipient can acknowledge and end the call with 5 or 9 respectively if the following is set: Installer Mode-&gt;Communications-&gt;Speech Dialler-&gt;Call Acknowledge -&gt;Enabled.</li><li>• During the test call a series of progress messages appear on the display.</li></ul> <p>If the test call was not successful, the display shows a brief message with the cause of the error.</p>
<b>SMS</b>	<p>Text messages must be activated and the contact must be saved in the phone book. Installer Mode-&gt;Communications-&gt;SMS-&gt;Call Mode-&gt;Enabled</p> <p>A list of the available connected transmission paths can be seen:</p> <p><b>PSTN</b></p>

- When this is selected, the possible configured recipients are displayed with their contact names as stored in the phone book.
- Scroll to the desired contact. Press the "Select" or "Start" key in the web interface.
- The alarm panel sends a test text message to this recipient.

**GSM / Mobile**

- When this is selected, the possible configured recipients are displayed with their contact names as stored in the phone book.
- Scroll to the desired contact. Press the "Select" or "Start" key in the web interface.
- The alarm panel sends a test text message to this recipient.
- 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.

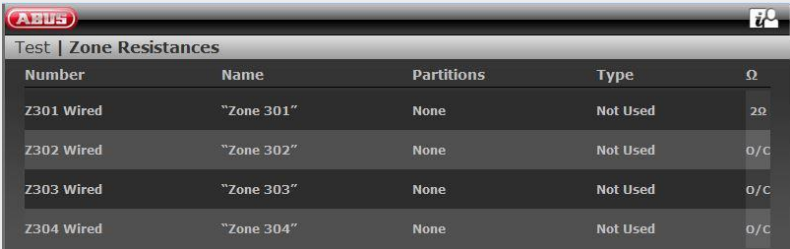

**Email**

Email must be activated and the contact must be saved in the phone book.  
Installer Mode->Communications->Email->Call Mode->Enabled

A list of the available connected transmission paths can be seen (on WBI only):

**Ethernet, Ethernet / IP Mobile**

- When this is selected, the possible configured recipients are displayed with their contact names as stored in the phone book.
  - Scroll to the desired contact. Press the "Select" or "Start" key in the web interface.
  - The alarm panel sends an email to this recipient.
  - 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
  - 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
<b>Zone Resistances</b>	<p>The current resistances for the wired zones (alarm panel and hybrid module) are displayed here.</p> <p><b>Display on the alarm panel:</b></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"> <li>• Alarm contact open/closed</li> <li>• Tamper contact open/closed</li> <li>• Short circuits</li> <li>• Open (isolated circuits)</li> </ul> <p>0k00 means 0 ohms or NC</p>  <p> <b>Note</b></p> <p>“4-wire CC” wiring type</p> <p><b>Alarm panel</b></p> <p>The display switches between the resistance of the alarm loop (A) and the resistance of the tamper loop (S).</p> <p><b>WBI</b></p> <p>Here the field shows both values simultaneously, the resistance of the alarm loop (A) and the resistance of the tamper loop (S).</p> <p><b>Example for a "2-wire FSL 2K2/4K7" zone</b></p> <ul style="list-style-type: none"> <li>• Alarm contact closed (standby) 2k18</li> <li>• Alarm contact open 6k89</li> <li>• Alarm contact open and series resistor bridged 4k68</li> <li>• Short circuit in line to detector 0k00</li> <li>• Line disconnection NO</li> </ul>
<b>Panel PSU</b>	<p>Here you can find information about the voltage values of the power supply. The display is identical on the alarm panel and the web interface.</p> <p><b>Ext. DC voltage in</b></p> <ul style="list-style-type: none"> <li>• The voltage value of the external DC power source</li> </ul> <p><b>Panel Battery 1</b></p> <ul style="list-style-type: none"> <li>• The voltage value of the first battery</li> </ul> <p><b>Panel Battery 2</b></p> <ul style="list-style-type: none"> <li>• The voltage value of the second battery</li> </ul> <p><b>Aux. Voltage Out</b></p> <ul style="list-style-type: none"> <li>• The voltage value at the terminal clamp 0 V/12 V AUX</li> </ul> <p><b>Example</b> (battery 2 is not connected in this example)</p>



- Ext. DC voltage in 14.1 volt
- Panel Battery 1 8.3 volt
- Panel Battery 2 0.1 volt
- Aux. Voltage Out 13.9 volts

**HyMo PSU** Here you can see the voltage value of the external DC power source at the terminal connection 0 V / 12 V IN of the hybrid module.

WBI:

Nummer	Name	Teilbereiche	Lautsprecher Teilbereiche	DC Spannung
HyMo 1	"HyMo 1"	3	1-4	13.6V
HyMo 2	"HyMo 2"	1	1-4	13.7V

Contains additional information including

**Number**

the internal number within the alarm panel software

**Name**

the unique name selected for this hybrid module

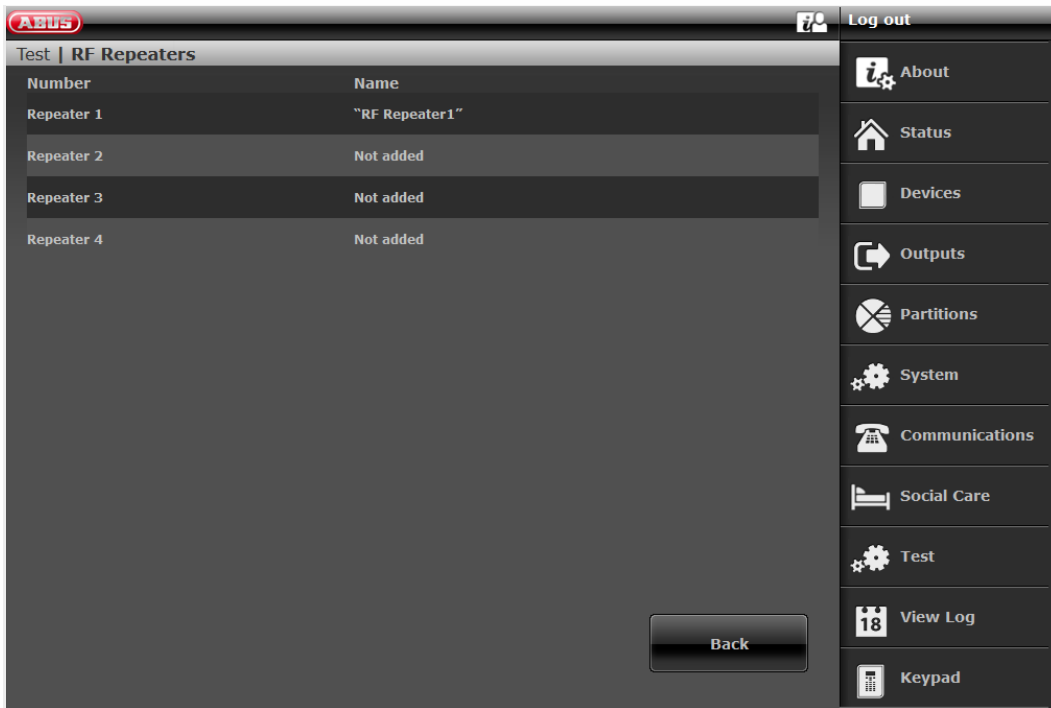
**Partitions**

the numbers of the partitions to which the hybrid module is assigned

**Loudspeaker partitions**

the partitions for which the optionally connected loudspeaker should provide a signal

**RF re-peater** Here you can find information about the signal strength of the components on the repeater. This is the signal strength on the repeater of the received notifications from the components. The display is identical on the alarm panel and the web interface

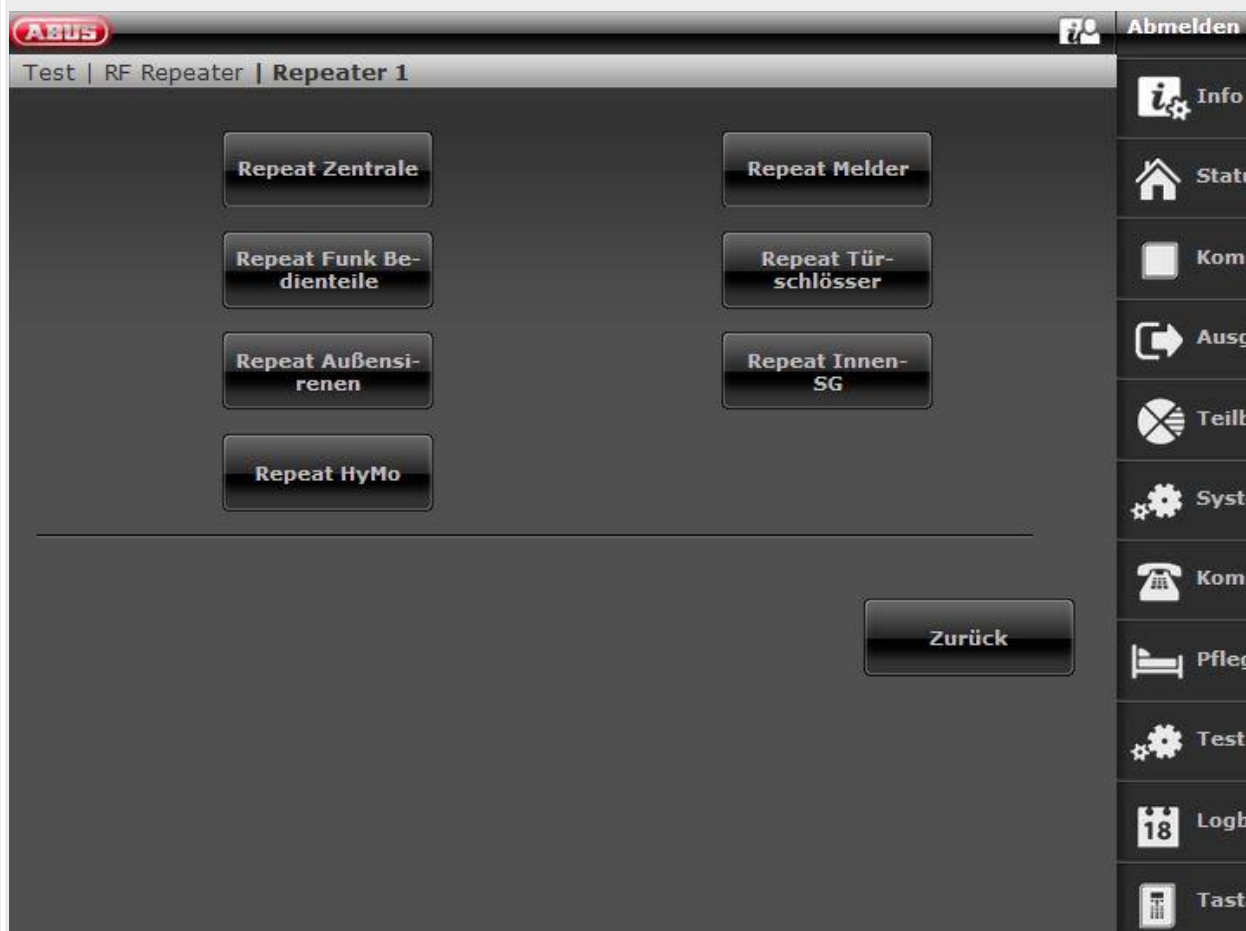


Click on the line of the desired repeater. The following display then appears:

S/W < v3.01.14



S/W &gt;= v3.01.14



Click on the desired component type. Details on the signal strength display can be found above under Test -> Signal Strengths.

### Repeat alarm panel

Here you can find 2 displays

#### RF repeater

This is the signal strength of the repeater to the alarm panel.

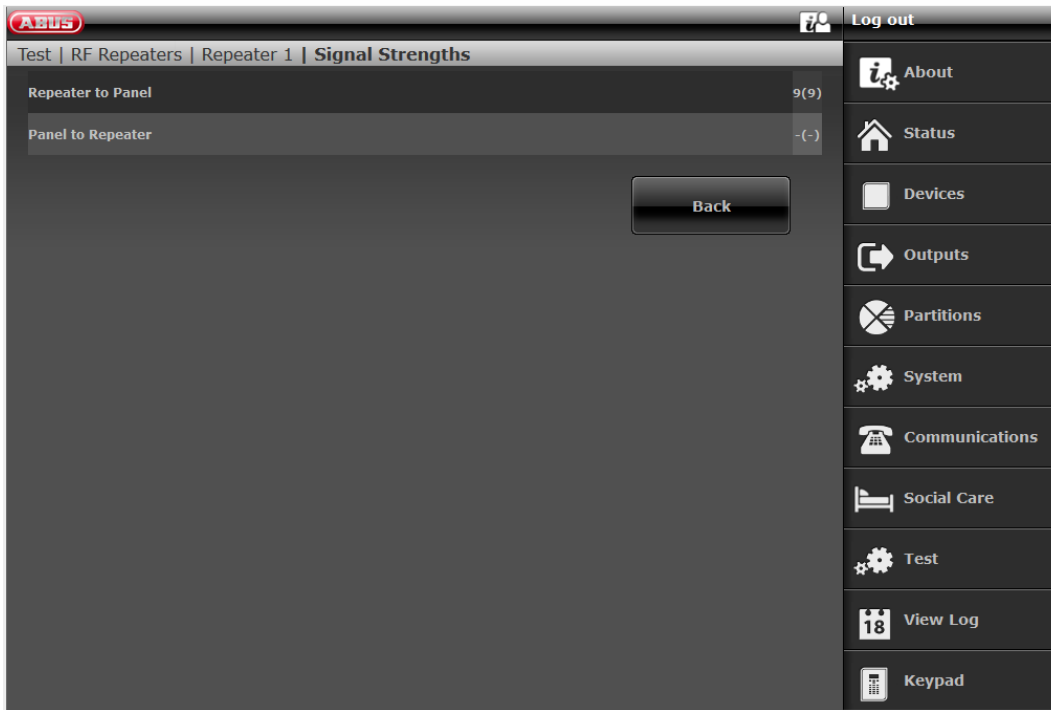
#### Repeat alarm panel

This is the signal strength of the alarm panel on the repeater.



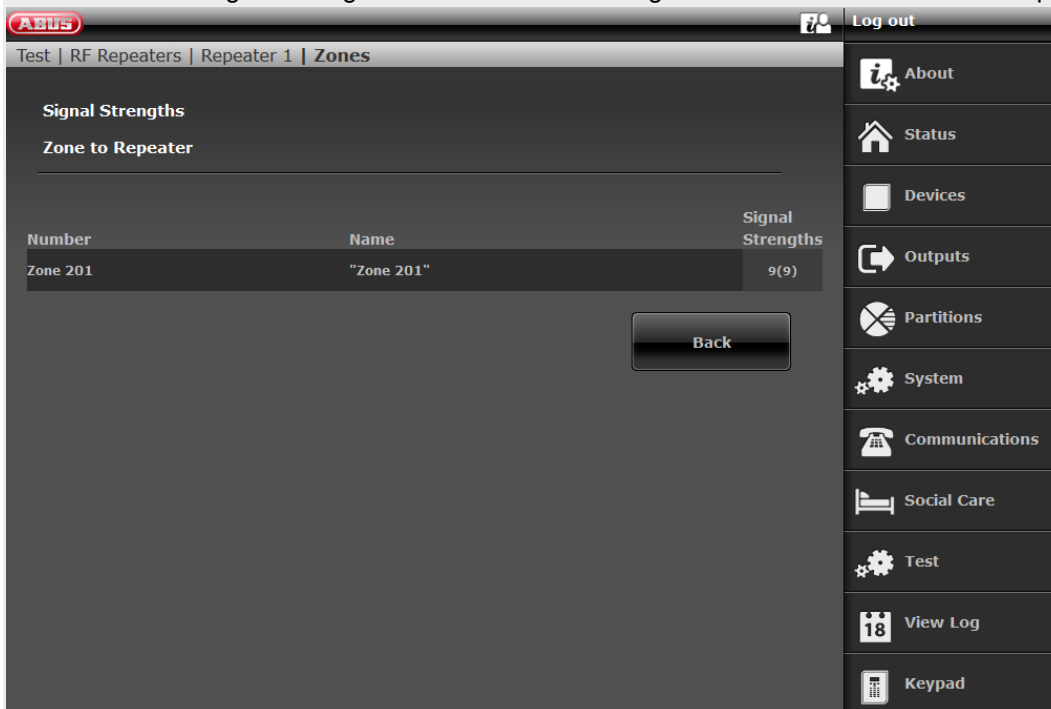
### Note

Both signal strengths are approximately the same. However, the signal strengths "alarm panel -> repeater" and "repeater -> alarm panel" can deviate slightly from each other. The reasons for this are:  
 different antennas on the alarm panel and repeater  
 different radio wave propagation characteristics in the different directions



## Repeat detectors

You can find the signal strength of the received messages from the **detectors** on the repeater here.



## Repeat wireless control panel

You can find the signal strength of the received messages from the **wireless control panel** on the repeater here.

## Repeat door locks

You can find the signal strength of the received messages from the **door locks** on the repeater here.

## Repeat outdoor sirens

You can find the signal strength of the received messages from the **external sirens** on the repeater here.

### **Repeat indoor sounder**


You can find the signal strengths of the received messages from the **indoor sounders** on the repeater here.

### **Repeat HyMo**

You can find the signal strength of the received messages from the **hybrid modules** on the repeater here.

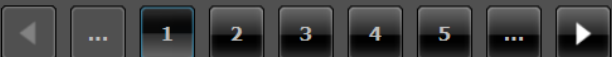
## Log











S/W <= v2.01.08

**ABUS**  Log out

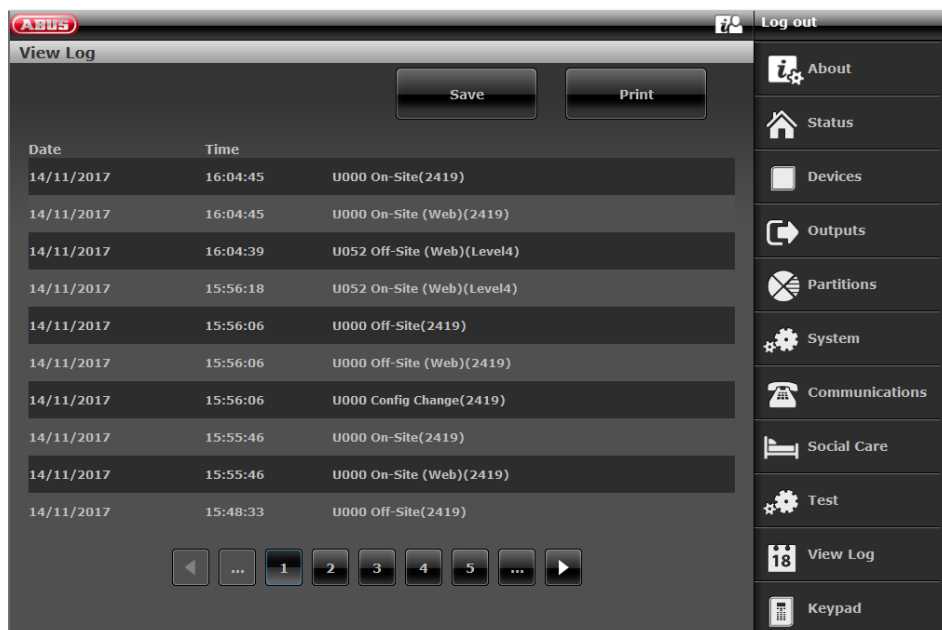
### View Log

Date	Time	
03/01/2014	19:21:23	U000 On-Site(9999)
03/01/2014	19:21:23	U000 On-Site (Web)(9999)
03/01/2014	19:20:31	U000 Off-Site(9999)
03/01/2014	19:20:31	U000 Off-Site (Web)(9999)
03/01/2014	19:02:15	U000 On-Site(9999)
03/01/2014	19:02:15	U000 On-Site (Web)(9999)
01/01/2014	01:21:48	U000 Off-Site(9999)
01/01/2014	01:21:48	U000 Off-Site (Web)(9999)
01/01/2014	01:15:16	U000 On-Site(9999)
01/01/2014	01:15:16	U000 On-Site (Web)(9999)



-  About
-  Status
-  Devices
-  Outputs
-  Partitions
-  System
-  Communications
-  Social Care
-  View Log
-  Keypad

S/W >= v3.00.03



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 (FIFO principle: first in, first out).

**You can find an overview of the possible log entries in the appendix.**

**"Save" button (S/W >= v3.00.03)**

To save the log book, click the "Save" button. The standard Windows "Open/Save" dialog appears. Either select "Open with" or "Save file".

The standard file name is "log.csv".



**Note**

To open and edit a "log.csv", it is best to use Excel. To convert the ".csv" file (comma separated values) into an ".xlsx" file, proceed as follows:

Select row 5/column A to row x/column A. Click on **Text in columns** in the **Data** tab in the **Data-tools** group.

Follow the instructions in the text conversion wizard to specify how the text will be divided into columns. Save as ".xlsx" You will now have three columns for better searching and data readability.

**"Print" button (S/W >= v3.00.03)**

To print the log book, click on the "Print" button. The standard Windows "Print" dialog appears. Select your desired printer.



**Note**

Which printers appear will depend on the printers installed on the computer. E.g. "Real" paper printer, or "PDF printer" such as PDF-Xchange, Freepdf.



**Note**

When saving or printing, all of the saved entries from the currently selected page to the last page are exported. Example:

## Configuration

---

The log book currently has 51 pages, each with 10 rows. You have selected page 41. When saving or printing, the contents of pages 41 to 51 will now be exported. You will then receive these 100 saved entries, i.e. 100 rows, in the respective file.

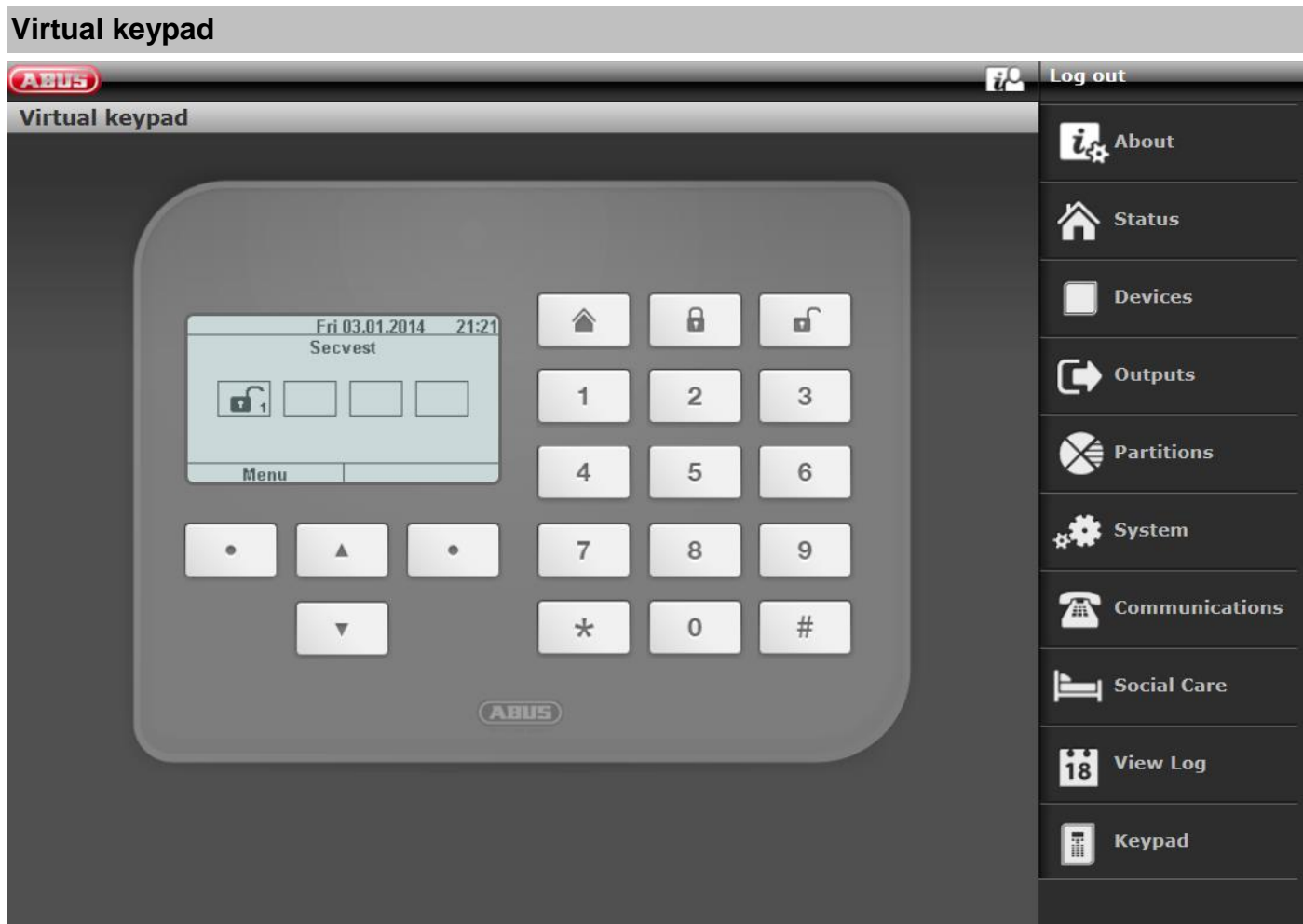
```
08/11/2018,10:45:19,Ben 000 Log in(2925)
08/11/2018,10:45:19,Ben000 Log in (Web)(2925)
08/11/2018,10:45:09,Ben 000 Log out(2925)
...
...
...
```

**The first 4 rows contain information about the alarm panel. The next rows mirror the content of the log book.**

### Example:

```
Secvest-ABUS, (display text)
Secvest 3.01.11,
Alarm panel time 11:39, date: 08/11/2018,
The system is configured as: Partitions,
```





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

Product name	Secvest
Product description	Wireless alarm system
Manufacturer	ABUS Security-Center GmbH & Co. KG Linker Kreuthweg 5 86444 Affing GERMANY
Environmental class	II (EN 50131-1 + A1:2009 Section 7, EN 50131-3:2009 Section 7)
Protection class, IP protection class	IP30 (internal spaces, in its installed state) IP = international protection or ingress protection 3 = Protection from foreign objects: protected against solid foreign objects with a diameter of > 2.5 mm, Protection from contact: protected against access with a tool and wires Ø >2.5 mm 0 = Protection from water: no protection
Operating temperature	0 °C to 40 °C
Storage temperature	0 °C to 40 °C
Humidity, maximum	Non-condensing average relative humidity 75%
Housing material	ABS
Dimensions (W x H x D)	205 x 285 x 48 mm
Weight	1453 g (excluding batteries) 1543 g (including one battery) 90 g one battery
General	This product must be installed, serviced and maintained by a qualified service engineer. External cleaning work can be carried out by the user.

#### Capacity

Zones	
IP zones	3 6 (S/W 1.01.00 and later) for the ABUS camera models specified see the appendix to the instructions for installers entitled "Compatible equipment"
Wireless Zones	48
Wired Zones	4 (2-wire FSL/DEOL or 2-wire CC) 2 (4-wire CC)
Wireless control panels	8
External Sirens	
Wireless sirens	4
Wired sirens	1
Indoor sounder	4
Info modules/internal sirens	∞
WAM	8
Door locks	8
RF repeater	4

Number of components per repeater	10 Remote controls and emergency transmitters (intrusion, medical emergency, care alarm) are always repeated.
Outputs	
IP Outputs	0
Radio Outputs	32
Wired Outputs	4
Combination outputs	10
Partitions	Four (each with internal arming)
User	50
User names	50 (plus installer name)
User Codes	50 (plus installer code)
Proximity tags (chip keys)	50 (one per user)
Remote controls	50 (one or several per user)
Panic alarm transmitter	50 (one per user)
Medical emergency call transmitter	50 (one per user)
Nursing emergency call transmitter	50 (one per user)
Telephone book	12 contacts Name Partitions 1-4 Voice/SMS/Email – Deactivated, Activated, Part Set 2 telephone nos 1 email 1 IP address 1 VoIP/SIP ID
Time schedules active/inactive:	160 events 20 exceptions
Logbook capacity	Up to 600 events 500 mandatory events 100 non-mandatory events Stored in EEPROM storage (non-volatile memory – NVM) retained for at least ten years without electricity. The whole log book stores its records for at least ten years without electricity. Note: The logbook is protected and cannot be deleted by an installer, administrator or ordinary user.
Internal clock	1 Crystal controlled and time synchronisation via a time server (SNTP time synchronisation) Accuracy if the alarm panel does not use time synchronisation via a time server: ± 5 minutes over a year @ 20°C nominal temperature < ± 10 minutes over a year @ 20°C nominal temperature according to EN 50131-1 Section 8.10
Loudspeaker	1
Microphone	1
Voice messages	33 voice messages for each language installed on the alarm panel  5 messages recorded by the user (Installer mode voice dialler) 12 second site message 8 seconds for each message 1–4

## Appendix

	<p>1 memo message (user menu) 30 seconds</p> <p>58/56 zone names (user menu) 2 seconds for each zone 6 IP zones 48 wireless zones 4/2 wired zones</p>
Internal Siren	<p>1 (integrated piezo sounder) Sound pressure level &gt; 96 dB(A) @ 1 m</p>
Communication modules, plug-in	1
Ports	<p>1x Ethernet 1x a/b 1x USB 1x SD card</p>
Backup batteries	2
Display	3.5", effective area 84 mm x 45 mm, 240 x 128 pixel monochrome (greyscale) LCD, white backlighting

### Protection and security


Security level	<p>Level 2 (EN 50131-1 + A1:2009 Section 6, EN 50131-3:2009 Section 6)</p>
Environmental class	<p>II (EN 50131-1 + A1:2009)</p>
Tamper protection (detection/protection)	<p>Type B (EN 50131-3:2009 Section 8.7)</p>
Wireless components, differentiation	16,777,214 ( $2^{24} - 2$ ) different IDs per component type
Wireless supervision	Configurable
Access codes	<p>There is no default installer code. There is no default administrator code. S/W &lt;=1.01.00 It is absolutely essential to change the default code (administrator user code: 1234 or 123456) during installation.</p>
Quantity of access codes	50 plus one installer
Access code differentiation	<p>10,000 code variants with 4-digit codes (0000–9999) The digits of the code are numbers between 0 and 9. <math>10^4 = 10 \times 10 \times 10 \times 10 = 10,000</math> (combinatorial variation)</p> <p>1,000,000 code variants with 6-digit codes (000000–999999) The digits of the code are numbers between 0 and 9. <math>10^6 = 10 \times 10 \times 10 \times 10 \times 10 \times 10 = 1,000,000</math> (combinatorial variation)</p>
Quantity of proximity tags (chip keys)	50
Proximity tag differentiation	4,294,967,296 ( $2^{32}$ , $2^{32}$ )
Temporary authorisation for user access	There is no facility for providing temporary access (e.g. PIN code or proximity keyfob which is only valid for a limited time or a specified quantity).

Locking access/locking codes	Keyboard is locked for 5 minutes after 3 incorrect codes in succession. Keyboard is locked for 5 minutes after 3 incorrect proximity keyfobs in succession.														
Mechanical keys															
Control panels															
Wireless key switch	FUBE50061, FUBE50060, FU8165														
Mechanical key differentiation	30,000														
Door locks															
Additional door lock	FUFT5001x-2x, 7010E 7025E														
Mechanical key differentiation	30,000														
Secvest Key	FUSK53030-58080, FUBE5XXXX														
Mechanical key differentiation	789.024														
Web user name length	12 characters														
Web user name differentiation	<p><math>88^{12}</math> (215,671,155,821,681,003,462,656, <math>88^{12}</math>, &gt;1,000,000) All characters can be alphanumeric symbols or special symbols.</p> <table border="1"> <tr> <td>A-Z</td> <td>26</td> </tr> <tr> <td>a-z</td> <td>26</td> </tr> <tr> <td>0-9</td> <td>10</td> </tr> <tr> <td>Space apostrophe ():.!&amp;@+_*#</td> <td>14</td> </tr> <tr> <td>Æ Å Ä Ø Ö Ü (upper case)</td> <td>6</td> </tr> <tr> <td>Æ Å Ä Ø Ö Ü (lower case)</td> <td>6</td> </tr> <tr> <td></td> <td>88 <math>\Sigma</math></td> </tr> </table>	A-Z	26	a-z	26	0-9	10	Space apostrophe ():.!&@+_*#	14	Æ Å Ä Ø Ö Ü (upper case)	6	Æ Å Ä Ø Ö Ü (lower case)	6		88 $\Sigma$
A-Z	26														
a-z	26														
0-9	10														
Space apostrophe ():.!&@+_*#	14														
Æ Å Ä Ø Ö Ü (upper case)	6														
Æ Å Ä Ø Ö Ü (lower case)	6														
	88 $\Sigma$														
Web encryption	<p>HTTPS TLS 1.2 &lt; 2.0.0: Signature algorithm: SHA1 &gt;= 2.0.0: Signature algorithm: SHA256 (SHA 2) &gt; 3.01.01: mbedTLS library V2.6.0</p>														
Electromagnetic compatibility EMC – immunity	Complies with EN 50130-4														
Electromagnetic compatibility EMC – interference	Complies with EN 61000-6-3														
Electrical safety	Complies with EN60950-1														

## Appendix

### Power supply

Type of power supply	Type A with reference to EN 50131-1:2006+A1:2009 Section 9 and EN 50131-6:2008+A1:2014 Section 4.1 Secvest has an integrated power supply unit (Type A). This power supply unit supplies different internal voltages to the circuit board to supply power to the circuitry. This power supply unit supplies 13.8 V with a maximum of 600 mA at the 0 V/12 V AUX output.
Normal voltage/frequency	110 V/230 V AC, 50/60 Hz, (85-265 V AC, 50/60 Hz) 13.8 V DC (13.0–14.5 V DC)
Power consumption, maximum	I AC MAX: 430mA rms @ 85 V AC 190mA rms @ 230VAC 170 mA rms @ 265 V AC
Power consumption, nominal	6.9 W 6.9 W x 24 x 365 = 60 kWh per year  55 mA rms @ 230 V AC specified with 200 mA aux load and fully charged batteries 300 mA @ 13.8 V
External DC input fault triggered at	12.5 V OK at 12.7 V
External PSU	13.0–14.5 V DC, at least 1.7 A
Power consumption, typical	Alarm panel standby: 100 mA Backlighting off Backlighting: High: 100 mA Medium: 40 mA Low: 15 mA  Internal siren sounding alarm at maximum volume: +70 mA GSM/mobile standby: +15 mA @ 12 V DC GSM/mobile active: +240 mA @ 12 VDC Battery charging current per battery: 220 mA
Backup power supply	
Rechargeable battery	Polymer lithium ion, 7.4 V
Capacity	2500 mAh, 18.5 Wh
Minimum running time in emergency power mode (standby time)	More than 12 hours More than 24 hours with optional second battery
Maximum recharging time	Less than 72 hours with reference to EN 50131-1:2006+A1:2009 Section 9 Table 24
Maximum time to recharge the battery to 80%	24 hours)
Lower threshold value of the battery	7.2 V "Flat battery" fault at <7.2 V
Deep discharge protection at	6 +/- 0.2 V
Aux power supply output	I max. 700 mA (main pcba issue < 7) I max. 600mA (main pcba issue >= 7)  Running on the mains (85–265 V AC, 50/60 Hz) 13.9 V max, idle 13.4 V min, full load (@ 600 mA)

	<p>Running on DC input @13.0V</p> <p>12.8 V max, idle 12.2 V min, full load (@ 600 mA)</p> <p>@13.8V</p> <p>13.6 V max, idle 13.0 V min, full load (@ 600 mA)</p> <p>@14.5V</p> <p>14.3 V max, idle 13.7 V min, full load (@ 600 mA)</p> <p></p> <p><b>Note</b> This output is <b>not</b> buffered by the battery in case of power failure. The output voltage during a power failure is directly 0 V.</p>
Aux power supply output fault triggered at	11.5V OK from 12.0 V
Surge protection trip voltage	Not given for grade 2
PSU monitoring	<p>Monitoring covers AC and external DC faults.</p> <p>It notifies the alarm panel if the AC or external DC power supply is disrupted or fails. The alarm panel will continue running on the batteries but the alarm panel and user are informed.</p> <p>Monitoring covers battery under voltage.</p> <p>If the battery is flat, the alarm panel and user are informed and the alarm panel gives a warning.</p>

## Fuses

Mains fuse (AC in)	Miniature fuse (micro fuse) removable
Name	T1AL250V
Characteristic	T = slow blow
Operating current	1 A
Breaking capacity	L = low
Operating voltage	250 V
Design	Glass tube 5x20 mm

## Appendix

### Wireless signal transmission





Operating frequency	868.6625 MHz
	In accordance with: EN 50131-5-3 Grade 2 EN 300 220-1 V.2.1.1 EN 300 220-2 V.2.1.1 EN 300 220-3 V.1.1.1
	Frequency band reserved for applications in the security zone.
Modulation	FM
Bandwidth	+/- 10 kHz Narrow band, 25 kHz channel separation
Transmission power	Max. 10 mW
Sensitivity	approx. -110dBm
Signal-to-noise ratio	12 dB
Antenna	Integrated duplex antenna technology
Range	Indoors: approximately 30 m depending on environmental factors Outdoors: approximately 100 m
Special features	Individual identification Supervision monitoring Jamming detection

### RFID proximity keyfob reader

System	Mifare Classic
Operating frequency	13.56 MHz
Transmission power	max. 55 mW
	In accordance with: EN 300 330-2
Special features	Individual identification



## Connections

L  N	Mains connection 110 V/230 V AC, 50/60 Hz, (85-265 V AC, 50/60 Hz) L – line, single phase (black or brown)  – protective earth (yellow/green) N – neutral (blue)
- DC IN + 13.8 V	External PSU input 13.8 V DC, external PSU at least 1.7 A See Power supply section for more details
0 V 12 V AUX	Voltage output 13.8 V DC up to 700 mA, main pcba issue < 7 up to 600 mA, main pcba issue >= 7  Maximum output residual ripple (ripple voltage): 0.2 Vp-p Aux output fault triggered at 11.5 V, ok from 12.0 V See Power supply section for more details   <b>Note</b> This output is <b>not</b> buffered by the battery in case of power failure. The output voltage during a power failure is directly 0 V.
+BATT1 ,+BATT2	Battery polymer lithium ion, 7.4 V, 2500 mAh
OP 301, OP 302	Relay output Potential-free changeover contact NO/C/NC Max. contact capacity: 500 mA @ 24 V AC rms or 30 V DC
OP 303, OP 304	Transistor output Open-drain Max. contact capacity: 500 mA @ 13.8 V DC   <b>Note</b> These outputs will drop to 0 V during power failures
TR	A negative tamper input The input is switched to the inactive low state (ground potential) by the connected siren. The threshold voltages are > 4 V for active and < 3.6 V for inactive.
TRB	A negative fault input The input is switched to the inactive low state (ground potential) by the connected siren. The threshold voltages are > 4 V for active and < 3.6 V for inactive.
10/100 LAN	Ethernet/LAN Cat5e patch cable, RJ45 male Connector at each end, suitable for 10/100Base-T
USB TYPE-B	USB Mini-B connector for alarm panel USB-A connector for PC Max. length 3 m
A B	Interface for analogue telephone connection to the public telephone network, a private branch exchange or an integrated access device (IAD [router] e.g. Vodafone Easybox xyz or FRITZ!Box vwxy) Approved for telecommunications in accordance with TBR-21/CTR21 (ETSI ES203021) > 18 V

## Appendix

	REN rating 1 PSTN data rates up to 1200 bps (V.22)
Micro SD	Secure Digital Memory Card Micro SD 11 mm x 15 mm x 1.0 mm 4 GB Micro SDHC
Z301, Z302, Z303, Z304	Wired Zones 2-wire FSL 2K2/4K7 2-wire FSL 1K/1K 2-wire FSL 2K2/2K2 2-wire FSL 4K7/4K7 2-wire CC
Z301A/Z301T, Z302A/Z302T	Wired Zones 4-wire CC

Resistance ranges specified for idle, alarm and tamper states (in Ohms).

Resistances immediately by the screw terminals.

Recommended cable resistance: must be less than 100 Ohms.

	2-wire FSL 2K2/4K7	2-wire FSL 1K/1K	2-wire FSL 2K2/2K2	2-wire FSL 4K7/4K7
O/C tampering	8281-∞	2401-∞	5281-∞	11281-∞
Alarm	4081-8280	1401-2400	3081-5280	6581-11280
Idle	1760-4080	800-1400	1760-3080	3760-6580
S/C tampering	0-1759	0-799	0-1759	0-3759

	4-wire CC	2-wire CC
Open/alarm/tampering	1001-∞	1001-∞
Closed/idle	0-1000	0-1000

## Communication

<b>Communication channels</b>									
a/b interface	Interface for analogue telephone connection to the public telephone network, a private branch exchange or an integrated access device (IAD)								
Ethernet	10/100 LAN								
GSM/GPRS (2G)	Plug-in module, optional FUMO50000 FUMO50001 Quad-band GSM: 850/900/1800/1900 MHz								
GSM/GPRS (2G) LTE (4G)	Plug-in module, optional ESMO50000 2G GSM: 900 and 1800 MHz 4G LTE: B3 (1800 MHz), B8 (900 MHz), B20 (800 MHz)								
<b>Communication methods</b>									
Web server	Web access, app and ABUS server								
ARC/ESCC reporting									
Receiver	2 Tel, 2 IP								
Protocols	DTMF-based Fast Format, Contact ID FSK-based SIA 1, SIA 2, Ex SIA 3, Ex SIA 3 V2, Ex SIA 3 V3 SMS-based CID in SMS IP <b>Compatible with "SIA IP Reporting (TCP-2013)"</b>  DC-09 (SIA-IP), with Fast Format, Contact ID, SIA <table border="1"> <thead> <tr> <th>Protocol</th> <th>Token</th> </tr> </thead> <tbody> <tr> <td>FF</td> <td>"SCN-S8"</td> </tr> <tr> <td>CID</td> <td>"ADM-CID"</td> </tr> <tr> <td>SIA 1, SIA 2, SIA 3, Ex SIA 3, Ex SIA 3 V2, Ex SIA 3 V3</td> <td>"SIA-DCS"</td> </tr> </tbody> </table> <p>TCP, only unencrypted (S/W&lt;=3.00.03), unencrypted and encrypted (S/W&gt;=3.00.03) Note: For details, see the appendix entitled "<b>ARC (ESCC) reporting protocol formats</b>"</p>	Protocol	Token	FF	"SCN-S8"	CID	"ADM-CID"	SIA 1, SIA 2, SIA 3, Ex SIA 3, Ex SIA 3 V2, Ex SIA 3 V3	"SIA-DCS"
Protocol	Token								
FF	"SCN-S8"								
CID	"ADM-CID"								
SIA 1, SIA 2, SIA 3, Ex SIA 3, Ex SIA 3 V2, Ex SIA 3 V3	"SIA-DCS"								
<b>Emergency call</b>									
Receiver	2 Tel								
Protocols	DTMF-based Scancom, Scanfast, Tunstall								
<b>Voice dialler</b>									
Receiver	8 Tel or VoIP/SIP ID								
DTMF detection VoIP/SIP Acknowledgement	RFC 2833								
Codec VoIP/SIP	PCM G711 A law (RTP AV Profile 8) ITU-T G.711 PCM A-Law audio 64 kbit/s Reference RFC 3551								

## Appendix

SMS	
Receiver	8
PSTN SMS protocols	TAP 8N1 TAP 7E1 UCP 8N1 UCP 7E1 ETSI Protocol 1
Email	
Receiver	8
Remote control by telephone	Yes
ATS Alarm transmission system Categories and classifications ATS (Alarm Transmission System) categories, SPT (Supervised Premises Transceiver) clas- sification	The alarm panel contains an integrated SP2 (ATS2) communica- tor to fulfil the requirements of EN 50131 for security level 2. The alarm transmission system is compliant with EN 50136- 1:2012 as an SP2 (ATS2) communicator. The alarm panel supports options A, B and C for grade 2 as given in Table 10 in EN 50131-1:2006+A1:2009
Classification of transmission time	D2 -> SP2
Transmission time, maximum values	M2 -> SP2
Classification of notification time	T2 -> SP2
Classification of availability	A0 (no requirement)-> SP2 (optional) There is no method for achieving compliance with EN 50136- 1:2012, 6.7.3 (non-availability of the alarm transmission system) because A0, no requirement.
Security to prevent removal	S0 (no measures) -> SP2 (optional) There is no method for achieving compliance with EN50136- 1:2012, 6.7.2 (redundancy) because S0, no measures
Information security	I0 (no measures) -> SP2 (optional) There is no method for achieving compliance with EN 50136- 1:2012, 6.8.3 (information security) because I0, no measures.
Monitoring a/b, Ethernet and GSM/wireless mobile	See the Communication options chapter in the Installer manual. Installer mode -> Communication -> Comm. options -> Comm. path fault response Ethernet, PSTN (a/b), GSM/mobile Installer mode -> Communication -> Comm. options -> Comm. path fault delay Ethernet, PSTN (a/b), GSM/mobile
Handshaking procedure	Mode/procedure: Transfer (EN 50136-2:2013 Section 6, Operation)

## SW &gt;= 3.00.06

Function	PSTN	Ethernet LAN	2G GSM, GPRS	4G LTE
mobile communication module, mobile radio module, cellular module, mobile service module, cellular module or connection	a/b	LAN	ESMO50000 FUMO50001 FUMO50000	ESMO50000
AES/NSL reporting (DTMF and FSK-based)	yes	no	yes	no
AES/NSL reporting (IP-based, e.g.DC-09)	no	yes	yes	yes
Emergency call (DTMF-based)	yes	no	yes	no
Voice dialler (analogue)	yes	no	yes	2G fall back
Voice dialler (VoIP/SIP)	no	yes	no	no
Voice dialler (VoLTE)	no	no	no	no
2-way communication	yes	yes	yes	2G fall back
Remote Control by Phone	yes	no	yes	2G fall back
SMS	yes	no	yes	Yes If the network operator supports it
E-mail (with photos)	no	yes	no	yes
E-mail (without photos)	no	yes	yes	yes
Web server	no	yes	no	no
DynDNS ABUS Server	no	yes	no	no
SNTP (time synchronisation)	no	yes	yes	yes
IP camera	no	yes	no	no
Smartphone app	no	yes	no	no
Push messages	no	yes	yes	yes

## Other

Configuration	Web browser via the integrated web server or directly on the alarm panel

### EU Directives

RED: 2014/53/EU  
EMC: 2014/30/EU  
RoHS: 2011/65/EU  
WEEE: 2012/19/EU  
ErP: 2009/125/EU  
Low voltage: 2014/35/EU  
General safety: 2001/95/EG

### Declarations of compliance for the FUA50000, FUA50500, FUA50010, FUA50510, FUA50100, FUA50600, FUA50110 and FUA50610 Secvest wireless alarm panel systems.

Standards with which the alarm panel claims compliance.

Certification body: **Telefication B.V.**

EN 50131-1:2006+A1:2009  
EN 50131-3:2009  
EN 50131-5-3:2005+A1:2008  
EN 50131-6:2008+A1:2014  
EN 50131-10:2014  
EN 50136-2:2013

Certification body: **ANPI**

INCERT TO31 2014 edition

Security level: Level 2

Environmental class: Class II

If the alarm panel has been installed correctly, the Secvest will be compliant with EN 50131 Grade 2.

The Secvest is compliant with EN 50131-1 and EN 50130-5 environmental class II.

Power supply is compliant with EN 50131-1:2006+A1 2009 Section 9 and EN 50131-6:2008+A1:2014 if the alarm panel has been installed correctly.

The alarm transmission system (ATS) is compliant with EN 50136-1:2012 as an SP2 communicator.

At Grade 2 the integrated SP2 communicator provides a compliant communicator for the Secvest on the condition that

- a) it is installed as specified in the installation instructions
- b) the connected PSTN, LAN and GSM/wireless mobile work normally,
- c) the alarm receiving centre has the right equipment.

The wireless mobile module (for Types see Technical Data -> Communication) can be used as an optional communicator for Grade 2.

S/W >3.00.06

	Option 1	Variant 2
TE Primary Network Interface	Communicator	mobile communication module, mobile radio module, cellular module, mobile service module, cellular module

TE Replacement Network Interface	mobile communication module, mobile radio module, cellular module, mobile service module, cellular module	Communicator
----------------------------------	---	--------------

The alarm panel supports options A, B and C for grade 2 as given in Table 10 in EN 50131-1:2006+A1:2009

If the installer selects a non-compliant configuration the compliance label must be removed or corrected.

Third party verification of compliance was carried out by ANPI and Telefication B.V.



**Compatible equipment**

**Radio devices**

Name	Article no	Note
<b>Detectors</b>		
Opening detector CC (brown)	FUMK50000B	
Opening detector CC (white)	FUMK50000W	
Opening detector FSL (brown)	FUMK50010B	
Opening detector FSL (white)	FUMK50010W	
Additional door lock with rotary knob 7010 E (brown)	FUFT50010B	
Additional door lock with rotary knob 7010 E (silver)	FUFT50010S	
Additional door lock with rotary knob 7010 E (white)	FUFT50010W	
Additional door lock with rotary knob 7010 E (brown)	FUFT50011B	
Additional door lock with rotary knob 7010 E (silver)	FUFT50011S	
Additional door lock with rotary knob 7010 E (white)	FUFT50011W	
Additional door lock with inner cylinder 7025 E (brown)	FUFT50020B	
Additional door lock with inner cylinder 7025 E (silver)	FUFT50020S	
Additional door lock with inner cylinder 7025 E (white)	FUFT50020W	
Additional door lock with inner cylinder 7025 E (brown)	FUFT50021B	
Additional door lock with inner cylinder 7025 E (silver)	FUFT50021S	
Additional door lock with inner cylinder 7025 E (white)	FUFT50021W	
Mini opening detector (brown)	FUMK50020B	
Mini opening detector (silver)	FUMK50020S	
Mini opening detector (white)	FUMK50020W	
Narrow opening detector (white)	FUMK50030W	
Narrow opening detector (white)	FUMK50031W	
Window lock FTS 96 E – AL0089 (brown)	FUFT50000B	
Window lock FTS 96 E – AL0089 (white)	FUFT50000W	
Window lock FTS 96 E – AL0125 (brown)	FUFT50001B	
Window lock FTS 96 E – AL0125 (white)	FUFT50001W	
Window lock FTS 96 E – AL0145 (brown)	FUFT50002B	
Window lock FTS 96 E – AL0145 (white)	FUFT50002W	
Upgrade kit for FTS 96 (brown)	FUFT50008B	
Upgrade kit for FTS 96 (white)	FUFT50008W	
Window handle FG 350 E (brown)	FUFT50040B	
Window handle FG 350 E (silver)	FUFT50040S	
Window handle FG 350 E (white)	FUFT50040W	
Window bar lock FOS 550 E – AL0089 (brown)	FUFT50030B	
Window bar lock FOS 550 E – AL0089 (white)	FUFT50030W	
Window bar lock FOS 550 E – AL0125 (brown)	FUFT50031B	
Window bar lock FOS 550 E – AL0125 (white)	FUFT50031W	
Window bar lock FOS 550 E – AL0145 (brown)	FUFT50032B	
Window bar lock FOS 550 E – AL0145 (white)	FUFT50032W	
Upgrade kit for FOS 550 E – AL0089 (brown)	FUFT50036B	
Upgrade kit for FOS 550 E – AL0089 (white)	FUFT50036W	
Upgrade kit for FOS 550 E – AL0125 (brown)	FUFT50037B	
Upgrade kit for FOS 550 E – AL0125 (white)	FUFT50037W	
Upgrade kit for FOS 550 E – AL0145 (brown)	FUFT50038B	
Upgrade kit for FOS 550 E – AL0145 (white)	FUFT50038W	
Window handle lock FO 400 E – AL0089 (brown)	FUFT50050B	
Window handle lock FO 400 E – AL0089 (white)	FUFT50050W	
Window handle lock FO 400 E – AL0125 (brown)	FUFT50051B	



Window handle lock FO 400 E – AL0125 (white)	FUFT50051W	
Upgrade kit for FO 400	FUFT50058	
PIR motion sensor	FUBW50000	
Motion detector (PET)	FUBW50010	
Outdoor motion detector	FUBW50020 FUBW50021 FUBW50022	
Smoke alarm	FURM50000	
Glass breakage detector	FUGB50000	
Shock detector	FUEM50000	
Flood detector	FUWM50000	
Panic alarm button	FUAT50010	Hold up detector
Fire alarm button	FUAT50020	
<b>Control panels</b>		
Control panel	FUBE50000	Activate/deactivate (arming/disarming)
Control panel with RC	FUBE50001	Activate/deactivate (arming/disarming) S/W >= V2.00.06
Key switch	FUBE50060	Activate/deactivate (arming/disarming)
Key switch with RC	FUBE50061	Activate/deactivate (arming/disarming) S/W >= V2.00.06
<b>External Sirens</b>		
Outdoor siren	FUSG50000	
Outdoor siren	FUSG50100	Sirens S/W 1.8 Note: Cannot be repeated.
Outdoor siren	FUSG50101	Sirens S/W >= 1.10
<b>Indoor sounder</b>		
Indoor sounder	FUSG50110	S/W >=3.00.05
<b>Info modules/internal sirens</b>		
Information module	FUMO50030	
Indoor siren	FUSG50010	
<b>WAM</b>		
Wireless universal module (WUM)	FUMO50020	
<b>Door locks</b>		
Additional door lock with rotary knob 7010 E (brown)	FUFT50010B	Activate/deactivate (arming/disarming)
Additional door lock with rotary knob 7010 E (silver)	FUFT50010S	Activate/deactivate (arming/disarming)
Additional door lock with rotary knob 7010 E (white)	FUFT50010W	Activate/deactivate (arming/disarming)
Additional door lock with rotary knob 7010 E (brown) with RC	FUFT50011B	Activate/deactivate (arming/disarming) S/W >= V2.00.06

## Appendix

Additional door lock with rotary knob 7010 E (silver) with RC	FUFT50011S	Activate/deactivate (arming/disarming) S/W >= V2.00.06
Additional door lock with rotary knob 7010 E (white) with RC	FUFT50011W	Activate/deactivate (arming/disarming) S/W >= V2.00.06
Additional door lock with inner cylinder 7025 E (brown)	FUFT50020B	Activate/deactivate (arming/disarming)
Additional door lock with inner cylinder 7025 E (silver)	FUFT50020S	Activate/deactivate (arming/disarming)
Additional door lock with inner cylinder 7025 E (white)	FUFT50020W	Activate/deactivate (arming/disarming)
Additional door lock with inner cylinder 7025 E (brown) with RC	FUFT50021B	Activate/deactivate (arming/disarming) S/W >= V2.00.06
Additional door lock with inner cylinder 7025 E (silver) with RC	FUFT50021S	Activate/deactivate (arming/disarming) S/W >= V2.00.06
Additional door lock with inner cylinder 7025 E (white) with RC	FUFT50021W	Activate/deactivate (arming/disarming) S/W >= V2.00.06
Secvest key	FUSK5xxxx	Activate/deactivate (arming/disarming)
Secvest key with RC	FUKE53030-58080	Activate/deactivate (arming/disarming) S/W >= V2.00.06
<b>RF repeater</b>		
Repeater module Secvest	FUMO50010	S/W >= V2.01.08
<b>Hybrid Module</b>		
Secvest hybrid module	FUMO50110	S/W >= V3.01.14
<b>Outputs</b>		
Socket	FUHA50010	
<b>Prox Tag</b>		
Proximity keyfob	FUBE50020	Activate/deactivate (arming/disarming)
<b>Remote controls</b>		
Remote control	FUBE50010 FUBE50011 FUBE50012 FUBE50013	Activate/deactivate (arming/disarming)
Remote control with RC	FUBE50014 FUBE50015	Activate/deactivate (arming/disarming) S/W >= V2.00.06
<b>Hold up pendant</b>		
Emergency buttons	FUAT50000	Panic alarm button:
<b>Medical emergency call transmitter</b>		
Emergency buttons	FUAT50000	

---

<b>Nursing emergency call transmitter</b>		
Emergency buttons	FUAT50000	
<b>Test devices</b>		
Test box	FU3801	

## Appendix

### Wired components, accessories

Name	Article no	Note
<b>Camera TVIP41550</b>		
PIR network camera	TVIP41550	
<b>IP cameras</b>		
Internal IP Dome IR 3MPx	IPCA33500	S/W >= V1.01.00
IP Boxtype 2 MPx (1080p, 3 x WDR)	IPCA52010	
Universal IP Boxtype 3MPx	IPCA53000	S/W >= V1.01.00
IP Boxtype 8 MPx (4K, 3 x WDR)	IPCA58000	
IP Tube 2 MPx (1080p, 3–9 mm, 3 x WDR)	IPCA62510	
IP Tube 2 MPx (1080p, 5–50 mm, 3 x WDR)	IPCA62515	
Outdoor IP Tube IR Ultra Low-Light 1080p	IPCA62520	S/W >= V1.01.00
Outdoor IP Tube IR 3MPx	IPCA63500	S/W >= V1.01.00
Outdoor IP Tube IR 6MPx	IPCA66500	S/W >= V1.01.00
IP Tube 8 MPx (4K, 4.3–8.6 mm, 3 x WDR)	IPCA68500	
IP Dome 2 MPx (1080p, 3–9 mm, 3 x WDR)	IPCA72510	
IP Dome 2 MPx (1080p, 5–50 m, 3 x WDR)	IPCA72515	
Outdoor IP Dome IR Ultra Low-Light 1080p	IPCA72520	S/W >= V1.01.00
Outdoor IP Dome IR 3MPx	IPCA73500	S/W >= V1.01.00
Outdoor IP Dome IR 6MPx	IPCA76500	S/W >= V1.01.00
IP Dome 8 MPx (4K, 4.3–8.6 mm, 3 x WDR)	IPCA78500	
Outdoor IP Mini Dome IR 1080p	IPCB42500 IPCB42501	S/W >= V1.01.00
IP Mini Dome 2 MPx (1080p, 2.8 mm)	IPCB42510A	
IP Mini Dome 2 MPx (1080p, 4 mm)	IPCB42510B	
IP Mini Dome 2 MPx (1080p, 6 mm)	IPCB42510C	
IP Mini Dome Wi-Fi 2 MPx (1080p, 2.8 mm)	IPCB42515A	
Outdoor IP Mini Dome IR Wi-Fi 1080p	IPCB42550 IPCB42551	S/W >= V1.01.00
IP Mini Dome 4 MPx (2.8 mm)	IPCB44510A	
IP Mini Dome 4 MPx (4 mm)	IPCB44510B	
IP Mini Dome 4 MPx (6 mm)	IPCB44510C	
Universal IP Mini Tube IR 1080p	IPCB62500	S/W >= V1.01.00
IP Mini Tube 2 MPx (1080p, 2.8 mm)	IPCB62510A	
IP Mini Tube 2 MPx (1080p, 4 mm)	IPCB62510B	
IP Mini Tube 2 MPx (1080p, 6 mm)	IPCB62510C	
IP Tube 2 MPx (1080p, 2.8–12 mm)	IPCB62520	
IP Mini Tube 4 MPx (2.8 mm)	IPCB64510A	
IP Mini Tube 4 MPx (4 mm)	IPCB64510B	
IP Mini Tube 4 MPx (6 mm)	IPCB64510C	
IP Tube 4 MPx (2.8–12 mm)	IPCB64520	
IP Mini Tube 8 MPx (4K, 2.8 mm)	IPCB68510A	
IP Mini Tube 8 MPx (4K, 4 mm)	IPCB68510B	
IP Mini Tube 8 MPx (4K, 6 mm)	IPCB68510C	
IP Tube 8 MPx (4K, 2.8–12 mm)	IPCB68520	

Universal IP Dome IR 720p	IPCB71500	S/W >= V1.01.00
Universal IP Dome IR 1080p	IPCB72500 IPCB72501	S/W >= V1.01.00
IP Dome 2 MPx (1080p, 2.8 mm)	IPCB72515A	
IP Dome 2 MPx (1080p, 2.8–12 mm)	IPCB72520	
IP Dome 4 MPx (4 mm)	IPCB74515B	
IP Dome 4 MPx (2.8–12 mm)	IPCB74520	
IP Dome 8 MPx (4K, 2.8 mm)	IPCB78515A	
IP Dome 8 MPx (4K, 2.8–12 mm)	IPCB78520	
Dual Flex Encoder	IPCS10020	
Ultra-Low-Light IP Tube IR 1080p	IPCS62520	S/W >= V1.01.00
Ultra-Low-Light IP Dome IR 1080p	IPCS72520	S/W >= V1.01.00
IP PTZ 2 MPx (1080p, 20x)	IPCS82500	
IP PTZ 2 MPx (1080p, 23x, Ultra Low-Light)	IPCS82520	
IP PTZ 3 MPx (36x)	IPCS83500	
IP Mini PTZ 4 MPx (4x)	IPCS84510	
IP Video Surveillance 2 MPx Wi-Fi Indoor Compact Camera	TVIP11560 TVIP11561	
Wi-Fi HD 720p Pan/Tilt Indoor Camera	TVIP21560	
IR HD 720p Network Outdoor Dome Camera	TVIP41500	
Wi-Fi HD 720p outdoor dome camera	TVIP41560	
Wi-Fi HD 720p PTZ Dome Camera	TVIP41660	
ABUS IP Video Surveillance 2 MPx Wi-Fi Mini Dome Camera	TVIP42560	
WDR Day/Night HD 1080p Network Camera	TVIP52502	
IR HD 720p Network Outdoor Camera	TVIP61500	
IR HD 720p WLAN Network Outdoor Camera	TVIP61550	
Wi-Fi HD 720p Outdoor Camera	TVIP61560	
ABUS IP Video Surveillance 2 MPx Wi-Fi Mini Tube Camera	TVIP62560	
Day/Night PTZ 720p Network Dome Camera	TVIP81000	
Day/Night PTZ 720p Network Outdoor Dome Camera	TVIP81100	
Day/Night PTZ 1080p Network Dome Camera	TVIP82000	
Day/Night PTZ 1080p Network Outdoor Dome Camera	TVIP82100	
Fisheye HD 1080p Network Indoor Camera	TVIP82900	
IP Fisheye 3 MPx	TVIP83900	
Outdoor Hemispheric IP Dome 6 MPx	TVIP86900	
<b>Communication devices</b>		
Wireless mobile module	FUMO50000	
Wireless mobile module	FUMO50001	S/W >= V1.01.00
Wireless mobile module	ESMO50000	S/W >= V3.00.05
Mobile antenna	AZ6310W	
SIM card		Standard SIM 1.8 V/3.0 V

## Appendix

		Micro SIM FUMO50001 ESMO50000
WiFi adapter	FUMO50040	Ethernet <-> WiFi
<b>External PSU</b>		
Power supply unit 13.8 V/1.7 A	AZZU10000 AZZU10030 FU3819	
High power supply unit 13.8 V/2 A	TVAC35500	
High power supply unit 13.8 V/3 A	TVAC35510	
High power supply unit 13.8 V/5 A	TVAC35520	
<b>Backup power supply</b>		
Backup battery 7.4 V/2500 mAh	FUBT50000	
<b>SD card</b>		
Micro SD 4 GB storage card	TVAC40970	4 GB Micro SDHC
<b>Touch Cover</b>		
Individual Secvest Touch Cover	FUZU50000	S/W >= 2.01.08

Wired components that fulfil the electrical specification of the corresponding connections (zones, outputs, inputs).

## Software for operation, control and communication

Name	Article no	Note
<b>Browser</b>		
IE8		IE7 and older are NOT compatible
Firefox		
Chrome		
Safari		
<b>App</b>		
Secvest APP (iOS)	APP50000	Version 2.3.1 2.1.1 2.1.0 2.0.1 1.3.5 1.3.1 1.2.5 1.2.2 1.1.7 1.1.2 iOS 10 or later iPhone, iPad, iPod touch
Secvest APP (Android)	APP50200	Version 2.3.1 2.1.1 2.1.0 2.0.1 1.3.40 1.3.38 1.3.1 1.2.1 1.1.6 Android 5.0 (Lollipop) or later
<b>Update S/W</b>		
Secvest Update Utility		Version 1.02.05 or later

### HW default values/factory defaults

In the default settings, a jumper is connected between the TR (tamper return) connection and 0 V as well as the TRB (trouble) connection and 0 V.

This means there is no fault indication (tamper/fault) if no wired sounder is connected.



## SW default values/factory defaults



## Note

The Secvest alarm control panel meets the requirements of EN50131 if the default values are retained while taking the note into account. If you change these settings, the installation may no longer be compliant. If the Secvest alarm control panel is no longer compliant with EN30131, you must remove all markings suggesting it is compliant.

## Installer Mode

MENU option	Default settings Default values	Comments
<b>1. COMPONENTS</b>		
<b>Detectors</b>		
<b>IP zones</b>		
Add/Del Detectors		
Zone 1nn		Zone 101 to 103 Zone 101 to 106 (S/W 1.01.00 and later)
Device Type	IPCx Range	
Trigger Mode	External	
Trigger Events	No	Only appears if Trigger Mode = "External" or "Int. + Ext."
Camera Action	Videos No Pictures Yes	Appears for IPCx range only
Trigger Partitions	Partition 1 Yes Partition 2 Yes Partition 3 Yes Partition 4 Yes All partitions Yes	Only appears if Trigger Mode = "External" or "Int. + Ext."
IP address	Empty	
HTTP Port Internal	80	
HTTP Port External	Empty	
RTSP Port Internal	554	
RTSP Port External	Empty	
User name	Empty	
Password	Empty	
Reaction time	20 s	Range of 1 s to 99 s
<b>Edit Zones</b>		
Name	Zone 10x	Zone 101 to 103 Zone 101 to 106 (S/W 1.01.00 and later)
Type	Not used	

## Appendix

Partitions	None	Only appears if the zone type is not set to "Not Used".	
Attributes	None	Only appears if the zone was given a type that was not "Not Used". Some attributes are only available for certain zone types.	
	Part Set		Off
	Chime		Off
	Soak Test		Off
	Activity Mon.		Off
	Force Set Omit		Off
	Dis. Sabotage		Off
	Omittable		Off
	Inverted		Off
Supervision	On		
Delete All			
<b>Wireless Zones</b>			
Add/Del Detectors			
Zone 2nn		Zone 201 to 248	
Edit Zones			
Name	Zone 2xy	Zone 201 to 248	
Type	Not used		
Partitions	None	Only appears if the zone type is not set to "Not Used".	
Attributes	None	Only appears if the zone was given a type that was not "Not Used". Some attributes are only available for certain zone types.	
	Part Set		Off
	Chime		Off
	Soak Test		Off
	Activity Mon.		Off
	Force Set Omit		Off
	Dis. Sabotage		Off
	Omittable		Off
	Supervision S/W >=3.01.16		On
Delete All			
<b>Wired Zones</b>			
Edit Zones			
Name	Zone 30x	Zone 301 to 304	
Type	Not used		
Partitions	None	Only appears if the zone type is not set to "Not Used".	
Attributes	None	Only appears if the zone was given a type that was not "Not Used". Some attributes are only available for certain zone types.	
	Part Set		Off
	Chime		Off
	Soak Test		Off
	Activity Mon.		Off
	Force Set Omit		Off
	Dis. Sabotage		Off
	Omittable		Off
Inverted	Off		
Delete All			

<b>HyMo zones</b>																		
Edit Zones																		
Name	Zone 40x	Zone 401 to 420																
Type	Not used																	
Partitions	None	Only appears if the zone type is not set to "Not Used".																
Attributes	None	Only appears if the zone was given a type that was not "Not Used". Some attributes are only available for certain zone types.																
	<table border="1"> <tr> <td>Part Set</td> <td>Off</td> </tr> <tr> <td>Chime</td> <td>Off</td> </tr> <tr> <td>Soak Test</td> <td>Off</td> </tr> <tr> <td>Activity Mon.</td> <td>Off</td> </tr> <tr> <td>Force Set Omit</td> <td>Off</td> </tr> <tr> <td>Dis. Sabotage</td> <td>Off</td> </tr> <tr> <td>Omittable</td> <td>Off</td> </tr> <tr> <td>Inverted</td> <td>Off</td> </tr> </table>	Part Set	Off	Chime	Off	Soak Test	Off	Activity Mon.	Off	Force Set Omit	Off	Dis. Sabotage	Off	Omittable	Off	Inverted	Off	
Part Set	Off																	
Chime	Off																	
Soak Test	Off																	
Activity Mon.	Off																	
Force Set Omit	Off																	
Dis. Sabotage	Off																	
Omittable	Off																	
Inverted	Off																	
Delete All																		
<b>Wireless control panel</b>																		
Add/Del Ctrl Dev																		
Ctrl Dev 0n		Ctrl Dev 01 to 08																
Edit Ctrl Device																		
Name	Ctrl Dev 0x	Ctrl Dev 01 to 08																
Partitions	Partition 1-4: Yes All partitions: Yes																	
Button C	Part set																	
Instant Set	Yes																	
Delete All																		
<b>External Sirens</b>																		
<b>Wireless sirens</b>																		
Add/Del Siren																		
Wireless Siren 0n		Wireless Siren 01 to 04																
Edit Siren																		
Name	Wireless Siren 0n	Wireless Siren 01 to 04																
Partitions	Partition 1-4: Yes All partitions: Yes																	
Delete All																		
<b>Wired Sirens</b>																		
Wired SRN 01																		
Name	Wired SRN 01																	
<b>Indoor sounder</b>																		
Add/delete																		
Indoor sounder 0n		Indoor sounder 01 to 04																
Edit																		
Name	Indoor sounder 0n	Indoor sounder 01 to 04																
Partitions	Partition 1: Yes Partition 2-4: No																	

## Appendix

	All partitions: No	
Delete All		
<b>Indoor sirens/Info module</b>		
Add Panel		
Updates	Disabled	
Ready-to-Set LED	Disabled	
<b>WAM</b>		
Add/Del WAM		
WAM On		WAM 01 to 08
Edit WAM		
Name	UVM 0x	WAM 01 to 08
Mode		
Delete All		
<b>Door locks</b>		
Add/Del Door Lock		
Door Lock On		Door Lock 01 to 08
Edit Door Lock		
Name	Door Lock 0x	Door Lock 01 to 08
Partitions	Partition 1-4: Yes All partitions: Yes	
Disabled after breaking and entering	Yes	S/W >= 3.01.16
Delete All		
<b>RF repeater</b>		
Add/delete RF repeater		
RF repeater1 to 4		RF repeater1 to 4
Edit Door Lock		
Name	RF repeater1 to 4	RF repeater1 to 4
Repeat alarm panel	No	
Repeat detectors	No	After a repeater has been added, all taught-in detectors of the alarm panel will appear.
Repeat wireless control panel	No	After a repeater has been added, all taught-in wireless control panels of the alarm panel will appear.
Repeat indoor sounder	No	After a repeater has been added, all taught-in indoor sounders for the alarm panel will appear.
Repeat outdoor sirens	No	After a repeater has been added, all taught-in external sirens of the alarm panel will appear.
Repeat door locks	No	After a repeater has been added, all taught-in door locks of the alarm panel will appear.

Repeat HyMo	No	After a repeater has been added, all taught-in hybrid modules for the alarm panel will appear.
Delete All		
<b>Hybrid module</b>		
Add/delete		
HyMo n		Hybrid module 1 to 2
Edit		
Name	HyMo x	Hybrid module 1 to 2
Partitions	Partition 1-4: Yes All partitions: Yes	
Wired Zone Type	2-wire FSL 2K2/4K7	
Loudspeaker options		
Partitions	Partition 1-4: Yes All partitions: Yes	
Delete All		
<b>2. OUTPUTS</b>		
<b>Radio Outputs</b>		
Add Outputs		
Output 2nn		Output 201 to 232
Edit Outputs		
Name	Output 2nn	Output 201 to 232
Type	Not used	
Polarity	Normal	
Partitions	Partition 1-4: Yes All partitions: Yes	
Delete All		
<b>Wired Outputs</b>		
Edit Outputs		
Name	Output 3nn	Output 301 to 304
Type	Not used	
Polarity	Normal	
Partitions	Partition 1-4: Yes All partitions: Yes	
Delete All		
<b>HyMo outputs</b>		
Edit Outputs		
Name	Output 40n	Output 401 to 408
Type	Not used	
Polarity	Normal	
Partitions	Partition 1-4: Yes All partitions: Yes	
Delete All		

## Appendix

<b>Combination outputs</b>		
Combination outputs 1–10		
Mode	One (OR)	
Inputs 1–10	Not used	
<b>3. PARTITIONS</b>		
<b>Partition 1-4</b>		
Name	Partition n	Partition 1 to 4
Complete arming		
Output Mode	Timed Set	
Exit Time	40 seconds	Only appears if the "Timed Set" or "Silent Set" Output Mode is set.
Settle Time	15 Seconds	Only appears if the "Final Door Set", "Lock Set" or "Cancel Exit Delay" Output Mode is set.
Entry Time	40 seconds	To fulfil EN50131-1 Clause 8.3.8.2, maximum of 45 s
Alarm Response	Siren + Comms	Internal alarm included
Siren delay	0 minutes	
Ext. Siren Time	15 minutes 3 minutes when country = Germany	To fulfil EN 50131-1 Clause 8.6, minimum 90 s, maximum 15 min.
Strobe on Set	Off	This setting is required to fulfil EN 50131.
Strobe on Unset	Off	
Beep on Set	Off	This setting is required to fulfil EN 50131.
Beep on Unset	Off	
Int. Siren Time	Endless	
Part set		
Output Mode	Instant Set	
Exit Time	40 seconds	Only appears if the "Timed Set" or "Silent Set" Output Mode is set.
Settle Time	15 Seconds	Only appears if the "Final Door Set", "Lock Set" or "Cancel Exit Delay" Output Mode is set
Entry Time	40 seconds	To fulfil EN50131-1 Clause 8.3.8.2, maximum of 45 s
Alarm Response	Siren	Internal alarm included This setting is required to fulfil EN 50131.
Siren delay	0 minutes	
Ext. Siren Time	15 minutes 3 minutes when country = Germany	To fulfil EN 50131-1 Clause 8.6, minimum 90 s, maximum 15 min.
Pt.Set Final Exit	Final Door	
Pt.Set Entry Route	Entry Route	
Strobe on Set	Off	This setting is required to fulfil EN 50131.

Strobe on Unset	Off	
Beep on Set	Off	This setting is required to fulfil EN 50131.
Beep on Unset	Off	
Int. Siren Time	Endless	
Deactivated		S/W >=2.00.00
Alarm Response	Siren + Comms	Internal alarm included
Siren delay	0 minutes	
Ext. Siren Time	15 minutes 3 minutes when country = Germany	To fulfil EN 50131-1 Clause 8.6, minimum 90 s, maximum 15 min.
Int. Siren Time	Endless	
Panic response:	Silent (S/W >=2.00.00) Acoustic (S/W < 2.00.00)	
Full set link	Partition 2-4: No All partitions: No	Partition 1 is a common partition.
<b>4. SYSTEM</b>		
<b>General</b>		
Language	English	This value depends on how you answer the language question during initial commissioning.
Display Text	Secvest	
Restore defaults		
Default settings		
Country defaults		Only appears as part of the factory-default process.
Mains Fault		
A/C Fault Reporting	On	This setting is required to fulfil EN 50131.
A/C Fail delay	0 minutes	This setting is required to fulfil EN 50131.
Ext. notification DC fault	On	This setting is required to fulfil EN 50131.
Ext. delay DC fault	0 minutes	This setting is required to fulfil EN 50131.
<b>Installer details</b>		
Installer Name		This value depends on how you answer the "Access Code Length" and "New Installer Code" questions during initial commissioning.
Installer Code		This value depends on how you answer the "Access Code Length" and "New Installer Code" questions during initial commissioning.
Installer Tel No		
<b>User access</b>		
Record Memo	Yes	

## Appendix

Dual Key Function	No	
Social Care Key	No	
Omit All	Yes	
Quick Set	No	This setting is required to fulfil EN 50131.
Quick Omit	No	
User Code Req'd	Yes	This setting is required to fulfil EN 50131. EN 50131-1, Section 8.3.1 (with reference to EN 50131-3, Section 8.3.1)
2 Way Replies	Yes	
Remote Inst. Set	Yes	
Duress Enable	No	Switch to Yes for Duress Code use
<b>User Reset</b>		
Zone Alarms	Yes	This option only appears if the confirmation mode is set to "Basic".
Zone Tamper	Yes	For INCERT detection, set to NO.
System Tamper	No	For INCERT detection, set to NO.
<b>Confirmation</b>		
Confirmation mode		
Basic	Default for systems apart from the UK	This value depends on how you answer the "Country defaults" question during initial commissioning.
DD243		
BS8243	Default for UK systems if the UK is chosen as the country.	This value depends on how you answer the "Country defaults" question during initial commissioning.
Confirmation time		
	30 minutes	Visible for DD243 or BS8243. Can be set to between 1 and 60 minutes. Ensure that only one value of 30 minutes or more is compliant with DD243 or BS8243.
After Entry	1 Zone	Visible for DD243 or BS8243. The default setting is changed to 2 zones if the confirmation mode = DD243.
Entry Keypad Lock	Off	Visible for DD243 or BS8243.
Sounder On	Unconfirm	Visible for DD243, BS8243 and Basic.
Siren On	Unconfirm	Visible for DD243, BS8243 and Basic.
Unconfirmed Reset	User	Visible for DD243 or BS8243.
Confirmed Reset	Installer	Visible for DD243 or BS8243.
Hold Up Alarm confirmation time	8 hours	Only visible for BS8243. Must be between 8 and 20 hours to be compliant with BS8243:2010.
Tamp as Tamp-Only	Enabled	Visible for BS8243.
<b>Hardware</b>		
Wired Zone Type	2-wire FSL 2K2/4K7	This value depends on how you answer the "Wired Zone Type" question during initial commissioning.
RF Siren Options	Siren + Strobe	



Battery 2	Disabled	
SD Card		
GSM/mobile antenna	Internal	
<b>Security</b>		
Supervision	Fault Tamper when country = UK	"TAMPER" for UK to fulfil PD6662:2010
Jamming	Fault Tamper when country = UK	"TAMPER" for UK to fulfil PD6662:2010
Level4 updates	Disabled	
Tamper Omit	Disabled	This setting is required to fulfil EN 50131.
Force Set	Off	If Force Set is enabled, the system is not compliant with EN 50131.
Remote Unset Full Set	Always	
Remote Unset Part Set	Always	
Ctrl Device Unset Full Set	Always	
Ctrl Device Unset Part Set	Always	
Auto Rearm	Never	This setting is required to fulfil EN 50131. Only appears if the confirmation mode is set to "Basic".
Silence Alerts	User Code	
Abort time	120 seconds	
Siren Delay (Ben)	0 minutes	
Entry Alarm Delay	Enabled	This setting is required to fulfil EN 50131-1 8.3.8.2.
Broadcast Panel Status	No	
<b>Panel upgrade</b>		"V3.00.03 – Installed"
<b>Checking for an upgrade?</b>		Once the selection has been made, the alarm panel automatically checks whether a new software ver- sion is available on the ABUS FTP server.
<b>Backup/restore</b>		
Backing up config to the SD card		
Loading config from SD card		"Secvest—04-12-2017-0932.cfg"
<b>Report</b>		Only on web interface
<b>5. COMMUNICATION</b>		
<b>Network</b>		
Network Setup		
Web server	Enabled	
DHCP	On	
IP address	Empty	This option will only be displayed, S/W >=2.00.00 DHCP=off
IP Port Number	80	S/W <2.00.00

## Appendix

Internal HTTP port	80	
Internal HTTPS port	4433	
IP Subnet Mask	Empty	This option will only be displayed, S/W <2.00.00 if an IP address is entered. S/W >=2.00.00 DHCP=off
Gateway IP address	Empty	This option will only be displayed, S/W <2.00.00 if an IP address is entered. S/W >=2.00.00 DHCP=off
DNS primary IP address	Empty	This option will only be displayed, S/W <2.00.00 if an IP address is entered. S/W >=2.00.00 DHCP=off
DYNDNS ABUS Server		
Status	Enabled	
User name	Empty	
Password	Empty	
External Port	443	S/W <2.00.00
External HTTPS port	4433	
IP Mobile Setup		S/W >=3.01.01 This option is only displayed if a wireless mobile module is installed.
APN	Empty	
User name	Empty	
Password	Empty	
IP Gateway	Ethernet	
Email Setup		
Server Name	Empty	
Server IP port number	587	
Account	Empty	
User name	Empty	
Password	Empty	
SSL	Disabled	
VoIP Dialler Setup		
SIP Test Call		
Called SIP User ID	Empty	
Start Test		
SIP Server Name	Empty	S/W <2.00.00
SIP domain name	Empty	
SIP proxy	Empty	
SIP user ID	Empty	
SIP User Password	Empty	
SIP Port	5060	
RTP Port	10000	
RFC 2833 DTMF Detection	Enabled	
SIP Dialler Enable	Enabled	

ARC reporting			
Call Mode	Single	"Single" or "Alternate" setting is required to be compliant with EN 50131.	
Log	Fast Format		
Telecoms Priority	Ethernet 2 PSTN 1		
Receiver	None		
Encryption	None		
Account Numbers	Account number for partition 1: 000000 Account No P 2: 000000 Account No P 3: 000000 Account No P 4: 000000	One account number per partition	
Fast Format channels	Channel 1: Fire Channel 2: Panic alarm Channel 3: Intruder alarm Channel 4: Open/Close Channel 5: Zone Omit (System) Channel 6: Tamper Channel 7: Confirmed Alarm Channel 8: General Fault	Only appears if protocol = Fast Format	
CID/SIA Events	Fire	Yes	Notes: 1. Appears if protocol = CID or SIA. 2. This setting is required to fulfil EN 50131.
	Panic alarm	Yes	
	Medical Alarm	Yes	
	Intruder alarm	Yes	
	Technical Alarm	No	
	Tampers	Yes	
	Set/Unset	Yes See Note 2	
	Part set	Yes See Note 2	
	Reset	Yes See Note 2	
	Exit Timeout	Yes	
	Omit	Yes	
	Key Box	No	
	RF Supervision	Yes	
	RF Jamming	Yes See Note 2	
	RF Battery/PSU	Yes See Note 2	
	Panel Battery	Yes See Note 2	
	Mains Fault	Yes See Note 2	
	Faults	Yes See Note 2	
Installer Mode	Yes See Note 2		
User Code Chnge	Yes		
Time/Date Re-set	No		
Camera supervision	No		

## Appendix

Restorals	Enabled	
Burg Comms Rearm	Enabled	Only appears if protocol = Fast Format AND if confirmation mode = "Basic"
21CN Ack Time	800 ms	Only appears if protocol = Fast Format.
Send Tamp As Burg	Disabled	Only appears if protocol = CID or SIA.
Dynamic Test Call	Enabled	Only appears if Static Test Call disabled
Stat. Test Call	Disabled	Only appears if Dynamic Test Call disabled. To be compliant with EN 50131, either the static or dynamic test call must be enabled.
Unset Comms	Enabled	
<b>Emergency call</b>		
Call Mode	Disabled	
Protocol	Scancom	
Telecoms Priority	PSTN 1	
Receiver	None	
Account Numbers	Account number for partition 1: 000000 Account No P 2: 000000 Account No P 3: 000000 Account No P 4: 000000	One account number per partition
Call Acknowledge	Enabled	
21CN Ack Time	800 ms	Only appears if protocol = Scancom or Scanfast
<b>Voice dialler</b>		
Call Mode	Disabled	
Telecoms Priority	Ethernet 2 PSTN 1	
Messages	None	
Event	None	
Message 1	Event 1: None Event 2: None Event 3: None Event 4: None Event 5: None	
Message 2	Event 1: None Event 2: None Event 3: None Event 4: None Event 5: None	
Message 3	Event 1: None Event 2: None Event 3: None Event 4: None Event 5: None	
Message 4	Event 1: None Event 2: None	

	Event 3: None Event 4: None Event 5: None	
Destinations	None	
Call Acknowledge	Enabled	
Stat. Test Call	Month, day: 1, hour: 12:00	
<b>SMS</b>		
Call Mode	Disabled	
Telecoms Priority	PSTN 1	
Messages	Empty	
Event	None	
PSTN SMS		
Protocol	ETSI Protocol 1	
Service Centre Tel.	1470,17094009	BT
Own Telephone No	Empty	Only appears if protocol = UCP
Destinations	None	
Stat. Test Call	Month, day: 1, hour: 12:00	
<b>Email</b>		
Call Mode	Disabled	
Telecoms Priority	Ethernet 1	
Messages	Empty	
Event	None	
Destinations	None	
Stat. Test Call	Month, day: 1, hour: 12:00	
<b>Communication Options</b>		
Line Fail Response	Ethernet = Audible PSTN = Audible IP mobile / mobile = Audible	
Line Fail Delay	Ethernet = 9 seconds PSTN = 9 seconds IP mobile / mobile = 9 seconds	This setting is required to fulfil EN 50131. IP mobile only visible if a wireless mobile module is installed.  Value range: 0 to 60 seconds
Remote Control by Phone		
Call-out control	Off	
Call-in control	Off	
Rings to Answer	5 rings	Only appears if Call-in control = on
Answer after first ring	Off	Only appears if Call-in control = on
GSM/mobile without outside dialling	No	Only appears when a wireless mobile module is installed.
<b>Contacts</b>		
Recipient A-L		
Name	Recipient A-L	
Partitions	1-4	S/W >= 2.00.00

## Appendix

Voice /SMS/Email	Deactivated: Yes Activated: Yes Part set: Yes	SW >= 3.01.01
Tel. no 1	Empty	
Tel No 2	Empty	
Email	Empty	
IP address	Empty	
SIP user ID	Empty	
<b>6. EMERGENCY CALL</b>		
<b>Start Monitoring Hr</b>	08:00 (hh:mm)	
<b>End Monitoring Hr</b>	20:00 (hh:mm)	
<b>Monitoring Interval</b>	4 hours	
<b>Volume</b>	Alarm control panel – medium, web – 5	
<b>7. TEST</b>		
<b>Walk Test</b>	No Zones in use	
<b>Keypad</b>		
<b>Sirens &amp; Sounders</b>		
Int.Sirens	Off	
Ext. Wireless sirens	No Devices!	
Sounder Module	No Devices!	
Loudspeaker	Stopped	
<b>Wireless control panel</b>		
<b>Door locks</b>	No Devices!	
<b>Signal Strengths</b>		
Detectors	No detectors	
Wireless control panel	No Devices!	
External Sirens	No Devices!	
Indoor sounder	No Devices!	
WAM	No Devices!	
Door locks	No Devices!	
Hybrid module	No Devices!	
RF repeater	No Devices!	
RF repeater components	No Devices!	
<b>Outputs</b>		
Radio Outputs	No Outputs Available	
Wired Outputs	No Outputs Available	
<b>Prox Tag</b>	No Prox Tags learnt	
<b>Remote controls</b>	No Remotes Learnt	
<b>Emergency buttons</b>	No Pendants Learnt	
<b>ARC reporting</b>		
Ethernet	No Recipients!	
PSTN	No Recipients!	

GSM/mobile	No Recipients!	Only appears when a wireless mobile module is installed.
<b>Voice dialler</b>	Comms not enabled	
<b>SMS</b>	Comms not enabled	
<b>Email</b>	Comms not enabled	
<b>Zone Resistances</b>	No Zones in use	
<b>Panel PSU</b>		
Ext. DC voltage in	e.g. 14.2 volts	Voltage value only appears if an external PSU is connected.
Panel Battery 1	e.g. 8.3 volts	
Panel Battery 2	e.g. 0.1 volts	
Aux. Voltage Out	e.g. 13.9 volts	
<b>HyMo PSU</b>		
	No Devices!	
<b>8. LOG</b>		
<b>All Events</b>		
<b>Mandatory Events</b>		
<b>Non-Mand. Events</b>		
Save		Only available on the WEB interface
Print		Only available on the WEB interface
<b>9. INFO</b>		
<b>Alarm panel</b>		
Version		Shows S/W version, S/N, Part No. and Language.
Customisation		Shows code for customer-specific alarm control panel adjustment.
<b>Communication</b>		
PSTN		
GSM/mobile		Only appears when a wireless mobile module is installed.
Network		Shows mobile network provider and SS (signal strength)
IMEI		
Subscriber Number		
IMSI		
Version	e.g. 13.210.11.07.00	Modem firmware from wireless mobile module
Reset		
<b>Ethernet</b>		
IP address		
IP Subnet Mask		
Gateway IP address		
DNS primary IP address		

## Appendix

---

MAC address		
IP Link Status		
<b>Hybrid module</b>		
	No Devices!	



## User menu

MENU option	Default settings Default values	Comments
<b>1. USER</b>		
<b>Add User</b>		Only visible to the administrator
<b>Edit User</b>		
"User 001"		Cannot be deleted
Name		This value depends on how you answer the "Access Code Length" and "Administrator Code" questions during initial start-up.
Type	Administrator	
Partitions	1-4	
Code		This value depends on how you answer the "Access Code Length" and "Administrator Code" questions during initial start-up.
Prox Tag	None	
Remote control	None	
Panic alarm	None	
Medical emergency call transmitter	None	
Nursing emergency call transmitter	None	
<b>Delete User</b>		Only visible to the administrator
<b>2. VOICE MEMO</b>		
<b>Recording</b>		Maximum recording time = 30 s
<b>Playback</b>	None	
<b>Delete Message</b>		
<b>3. OMIT ZONES</b>		
	No Zones Omittable	
<b>4. OUTPUTS ON/OFF</b>		Only appears if the installer has set the outputs to "User Defined".
<b>5. CONFIGURATION</b>		
<b>Functions</b>		<b>Keypad front</b>
Bell	On	
Voice message	On	
Activity monitor	Off	
Display contrast	100%	

## Appendix

Backlighting brightness	High	
LCD backlighting	On	
Backlighting for menu keys	Off	
Backlighting for arm keys	Off	
Backlighting for number keys	Off	
Zone name announcement		Maximum recording time = 2 seconds for each zone
Enabled	Off	
IP zones	Recording Playback:       None Delete Message	Zone 101 to 106
Wireless Zones	Recording Playback:       None Delete Message	Zone 201 to 248
Wired Zones	Recording Playback:       None Delete Message	Zone 301 to 304
Restart Panel		Only visible to the administrator and if: <ul style="list-style-type: none"> <li>• No communication is taking place at the time</li> <li>• Alarm control panel is unset.</li> </ul>
Keypad tones	On	SW >= 2.01.08
<b>Functions</b>		<b>Touch Cover, SW &gt;= 2.01.08</b>
Bell	On	
Voice message	On	
Activity monitor	Off	
Display contrast	100%	
Backlighting brightness	High	
Backlighting	When active	
Zone name announcement		Maximum recording time = 2 seconds for each zone
Enabled	Off	
IP zones	Recording Playback:       None Delete Message	Zone 101 to 106
Wireless Zones	Recording Playback:       None Delete Message	Zone 201 to 248
Wired Zones	Recording Playback:       None Delete Message	Zone 301 to 304
Restart Panel		Only visible to the administrator and if: <ul style="list-style-type: none"> <li>• No communication is taking place at the time</li> <li>• Alarm control panel is unset.</li> </ul>
Keypad tones	On	
Dynamic backlighting	On	

Cleaning mode	On	
<b>Date &amp; time</b>		Only visible to the administrator
SNTP Time sync.		
SNTP Time sync.	Off	
Manual mode		
Set date	01/01/2015	
Set time	00:00 (hh:mm)	
SUMMER/WINTER	Automatic	
<b>Edit Outputs</b>		Only visible to the administrator and only appears if the installer has set the outputs to "User Defined".
<b>Remote controls</b>	None	Only visible to the administrator
<b>Volume Settings</b>		Only visible to the administrator
Operator Sounds	5	
Info tones:	5	
Alarm tones:	10	
Speech Volume	50%	
Message Volume	33%	
<b>Web Access</b>	Enabled	Only visible to the administrator
<b>Level4 updates</b>	Disabled	Only visible to the administrator
<b>Time schedules active/inactive:</b>		Only visible to the administrator
Enabled	No	
Week Planner		Events: 160 Exceptions: 20
<b>Push notification</b>	None	
<b>6. CONTACTS</b>		Only visible to the administrator
<b>Recipient A-L</b>		
Name	Recipient A-L	
Tel No 1	Empty	
Tel. no 2	Empty	
Email	Empty	
IP address	Empty	
SIP User ID	Empty	
<b>7. TEST</b>		Only visible to the administrator
<b>Walk Test</b>	No Zones in use	
<b>Sirens &amp; Sounders</b>		
Int.Sirens	Off	
Ext. Wireless sirens	No Devices!	
Sounder Module	No Devices!	
Loudspeaker	Stopped	
<b>Door locks</b>	No Devices!	
<b>Outputs</b>	No Outputs Available	

## Appendix

<b>Prox Tag</b>	No Prox Tags learnt	
<b>Remote controls</b>	No Remotes Learnt	
<b>Emergency buttons</b>	No Pendants Learnt	
<b>Telephone call</b>	Empty	
<b>8. LOG</b>		
<b>9. INFO</b>		Only visible to the administrator
<b>Alarm panel</b>		
Version		Shows S/W version, S/N, Part No. and Language.
<b>Communication</b>		
PSTN		
GSM/mobile		Only appears when a wireless mobile module is installed.
Network		Shows mobile network provider and SS (signal strength)
IMEI		
Subscriber Number		
IMSI		
Version	e.g. 13.210.11.07.00	Modem firmware from wireless mobile module
Reset		
<b>Ethernet</b>		
IP address		
IP Subnet Mask		
Gateway IP address		
DNS primary IP address		
MAC address		
IP Link Status		

## Start Wizard

LANGUAGE

UPGRADE PANEL APPLICATION

COUNTRY DEFAULTS

Set date

Set time

SUMMER/WINTER TIME

Automatic (default setting)

Manual

A/C FAULT NOTIFICATION

OFF

ON (default setting)

EXT DC FAULT NOTIFICATION

OFF

ON (default setting)

BATTERY 2

WIRED ZONE TYPE

WEB SERVER

Disabled

Released (default setting)

DHCP

Off

If OFF is selected

IP ADDRESS

IP SUBNET MASK

GATEWAY IP ADDRESS

DNS PRIMARY IP ADDRESS

On

(default setting)

INTERNAL HTTP PORT

OVERVIEW

CALL MODE (ARC/ REPORTING)

Disabled

Single

(Standard setting due to the requirements of EN 50131)

Alternate

ACCESS CODE LENGTH

### Note

You can delete all users with the help of the this menu.

For further information, please refer to the instructions under System -> Security-> 6 digit user code.

INSTALLER CODE

CONFIRMATION OF INSTALLER CODE

ADMIN USER CODE

CONFIRMATION OF ADMIN USER CODE

LOGIN

Information on the display:

"Please check whether new software is available."

Information on the display:

For using secure codes.

Information on the display:

Certificate creation



Standby display (with date and time)

### Acoustic signal tones

The alarm panel is able to generate a wide range of acoustic signal tones. On components such as the control panel, indoor siren/info module, indoor sounder and loudspeaker on the hybrid module, these are similar to the alarm tones, info tones and operating sounds of the wireless alarm panel.

The following table shows an overview of the signal tones and their group assignment.

Signal tones	Meaning
Alarm tones:	Breaking and entering/intrusion
	Fire
	Medical alarm
	Emergency call
Info tones:	Chime
	Exit tone E.g.: Long continuous beep (beeeeeeeeeeeep): During the exit delay time. All zones closed, the alarm panel is activated after the delay time has expired.
	Exit tone in the event of a fault E.g.: Interrupted beeps (beep...beep...beep): A zone was opened during the exit delay time. It must be closed before the delay time expires.
	Entry tone E.g.: Interrupted beeps (beep...beep...beep): During the entry delay time.
	Emergency call warning, inactivity warning
Operator Sounds	Acknowledgement/confirmation E.g.: Double deep (beep, beep): The alarm panel has been successfully activated.
	Error E.g.: Short beep (beep): System fault, the alarm panel cannot be activated

 Note	The volume of the signal tones can be configured separately for each group.  User menu -> Configuration -> Volume Settings Operator tones 0-10 Info tones 0-10 Alarm tones 0-10
 Note	These volume settings also affect the volume of the alarm panel <b>and</b> the indoor sounder <b>and</b> the loudspeaker on the hybrid module.

### Repairs and maintenance

#### Maintenance by the installer

The alarm control panel should be checked once a year. During every inspection:

- Check the Secvest for visible signs of damage on the housing or the front cover.
- Check the condition of the housing-tampering switch and the wall-tampering switch (wall-removal contact)
- Check the condition of the backup battery
- Check the cabling for visible signs of damage or wear
- Check the keypad for visible signs of damage
- Test the function of all keys on the keypad
- Clean the keypad surface, the display and the housing
  - When cleaning the surface, use a soft, dry cloth.
  - Do not use any water, solvents or cleaning agents.
- Check the signal strength and the battery condition of all detectors, control panels, external sirens, indoor sirens, indoor sounders, WAMs, door locks, hybrid modules, remote controls, hold up pendants, medical pendants and care pendants.
- Replace the batteries when recommended by the manufacturer
- Test every component.
- Carefully clean the lenses on all PIR detectors and cameras using a soft, clean, dry cloth.
- Do not use any water, solvents or cleaning agents.
- Carry out a walk test on all detectors.
- Test all external sounders
- Test the communication.
- EN 50131-7 "Alarm systems – intrusion and hold up alarms – part 7: application rules" must also be taken into consideration.

Use the test function in Installer mode -> Test

It is not necessary to check any calibrations or adjustments.

#### Maintenance by the user

The administrator uses the test function in User menu -> Test

- Clean the sounder
  - When cleaning the surface, use a soft, dry cloth.
  - Do not use any water, solvents or cleaning agents.
- The user does not need to carry out any other maintenance work.



## S/W upgrade



### Note

SW >=3.00.03

There are four ways to perform a software upgrade.

- Software upgrade with new files that are saved on the SD card.
- Software upgrade with new files that are saved on the PC.
- Software upgrade with new files that are stored on the FTP server.
- SW upgrade with the Secvest update utility



### Note

#### Software update from 3.01.14 to 3.01.17

#### Software update from earlier versions to 3.01.17

- The Secvest wireless alarm system may return to factory settings upon updating to V3.01.17.
- It is therefore **essential** to **save** the alarm control panel **configuration** in advance. After completing the update, the configuration (inc. all component IDs) can be restored.
- The language file must be updated BEFORE updating the application file.
- "Level 4 user" authorisation level for SW updates
  - It is no longer possible to run SW updates via the Installer menu of the web server.
  - Approval for "Level 4 User" must be granted in the User and Installer menu.
  - The user code for "Level 4 User" will be issued following approval.
- PUSH settings could be lost during an update and must be checked and tested.

#### Registering on the ABUS server

- If the Secvest wireless alarm system is used in conjunction with the ABUS server, it may need to be manually deleted in the Abus server account.
  - You can use the trace function to check. With X = 4 = "HTTPS Client", you can see the communication log between the alarm panel and the ABUS server. If "MAC already in use" appears there, then the alarm panel must be deleted from the ABUS server account. The alarm panel can then register itself again.
- The registration occurs automatically on the ABUS server after restoring the configuration within a maximum of 30 minutes.

#### Browsing history

- Please delete the cache (browsing history) to ensure that the newest JavaScript, CSS and image files are loaded from the alarm panel.

### Waiting period – Access to the web server after restart

- Wait at least three minutes after restarting the alarm panel before you access the alarm panel web server.
- During the first access, the https certificate and other safety features are "exchanged" during this period.

### Saving and restoring the configuration



#### Important

**As part of a comprehensive update, the Secvest wireless alarm system is reset to the factory defaults.**

It is therefore essential to save the alarm control panel configuration in advance:

1. "Installation mode"
2. "System"
3. "Backup/restore"
4. "Backup"

After completing the update, the configuration (inc. all component IDs) can be restored:

5. "Installation mode"
6. "System"
7. "Backup/restore"
8. "Load Configuration"



#### Note

You can tell an update process is running from the following 3 processes on the alarm panel.

- 1)
  - Menu keys light up
  - Arm/disarm keys flash
  - Number keys are dark
4.
  - Menu keys light up
  - Arm/disarm keys are dark
  - Number keys flash
- 3)
  - Menu keys are dark
  - Arm/disarm keys start flashing again to show that the upgrade process is almost finished.
  - Number keys are dark

The first point of the start wizard appears (language selection).



#### Important

Wait until this process is fully complete. The power supply must not be disconnected during the upgrade process under any circumstances. This could lead to a complete crash/failure of the software.

If a touch front is installed, no keys light up during this process.

**Important**

Wait until something appears again on the display. The power supply must not be disconnected during the upgrade process under any circumstances. This could lead to a complete crash/failure of the software.

**Software file set for V3.01.17**

Software Title	Software Version	Software File name	File size on data storage device
			PC display of the operating system
Core	V3_01_17	13410164_FUAA50XXX_App_V3_01_17.bin	2880 KB
		<b>File size in bytes</b> GUI display: 2.949.120	
<b>Languages</b>			
German	V1_42	13404974_FUAA50XXX_Deutsch_V1_42.Ing	2347 KB
English	V1_35	13404973_FUAA50XXX_English_V1_35.Ing	1864 KB
Dutch	V1_17	13404976_FUAA50XXX_Nederlands_V1_17.Ing	2281 KB
French	V1_17	13404975_FUAA50XXX_Francais_V1_17.Ing	2328 KB
Italian	V1_16	13404978_FUAA50XXX_Italiano_V1_16.Ing	2521 KB
Danish	V1_19	13404977_FUAA50XXX_Dansk_V1_19.Ing	1791 KB
Swedish	V1_13	13405100_FUAA50XXX_Svenska_V1_13.Ing	2346 KB
Spanish	V1_13	13404979_FUAA50XXX_Espanol_V1_13.Ing	2379 KB
Polish	V1_13	13405101_FUAA50XXX_Polski_V1_13.Ing	2177 KB
Russian	V1_10	13405102_FUAA50XXX_Pycck_V1_10.Ing	2534 KB
<b>Confidence Test</b>			
ConfTest	V1_03	12551477_FUAA50XXX_ConfTest_V1_03.Ing	32 KB
<b>Auxiliary programs Accessories</b>			
Setup Secvest Update Utility 32	V1.02.05	Setup Secvest Update Utility 1_02_05 (32 bit).msi	
Setup Secvest Update Utility 64	V1.02.05	Setup Secvest Update Utility 1_02_05 (64 bit).msi	
Bootloader	V1_00_00	12526869_FUAA50XXX_Boot_V1_00_00.bin	42

### Software upgrade with new files from the SD card

Alarm panel

Installer Mode -> System -> General -> Language

Installer Mode -> System -> Upgrade alarm panel



#### Note

The language file must be updated BEFORE updating the application file.

Which language file version is compatible with which application file version can be found in the corresponding release note "Secvest\_Software\_Release\_Notes\_Va\_bc\_de\_yyyy\_mm\_dd".

Example

Installer Mode -> System -> Upgrade alarm panel

UPGRADE PANEL APPLICATION		
V3.01.14	Installed	
V1.01.00	10/02/2016	(2293760)
V2.00.00	04/10/2016	(2621440)
V2.00.06	06/03/2017	(2621440)
V2.01.08	15/06/2017	(2686976)
V3.00.04	12/12/2017	(2883584)
V3.01.01	10/05/2018	(2883584)
V3.01.11	17/10/2018	(2883584)
V3.01.14	11/03/2019	(2949120)
V3.01.16	25/11/2019	(2949120)

## Software upgrade with new files on the PC



### Important

#### Saving and restoring the configuration

**As part of a comprehensive update, the Secvest wireless alarm system is reset to the factory defaults.**

It is therefore essential to save the alarm control panel configuration in advance:

1. "Installer Mode" web server
2. "System"
3. "Backup/restore"
4. "Backup"

After completing the update, the configuration (inc. all component IDs) can be restored:

5. "Installer Mode" web server
6. "System"
7. "Backup/restore"
8. "Load Configuration"



### Important

#### SW >= 3.00.06, saving and restoring the configuration

Before the alarm panel starts the upgrade, the configuration files and the SSL certificate are saved automatically on the internal flash drive. The new software is then installed, and the alarm panel restarted. At this point, the factory settings are used first, but the alarm panel then automatically reproduces the configuration files and the SSL certificate from the flash drive (as if the configuration had been saved/reproduced manually). This means that the Start Wizard is not used, the SSL certificate is not regenerated and, more importantly, that the installer does not have to go to the site in order to respond to the command prompt of the Start Wizard.



### Important

Changes have been made to the following menus as part of S/W 2.00.00

- VoIP Dialler Setup
- Contacts -> SIP User ID
- Outputs -> Type "User defined"
- ARC/ESCC reporting -> IP port

Please check these menus after carrying out the configuration and adjust the settings accordingly.

#### Level4 updates

##### Preparation:

Adding new "Level 4 user"

Alarm panel

Installer Mode -> System -> Security -> Level4 Updates -> Enabled

## Appendix

Or  
WBI  
Installer Mode -> System -> Security Settings -> Level4 Updates -> Enabled (activated, ticked)

If this option is activated, a new Level 4 code must be entered. This is only the case if this Level 4 code was never programmed to begin with (as delivered or since the last reset to the factory defaults). This Level 4 code has the same number of digits as the Installer code or the User code.

Enter a "New Level 4 code" and "Confirm Level 4 code" (enter the code again to confirm it).  
A new user is added automatically. See "User" menu.

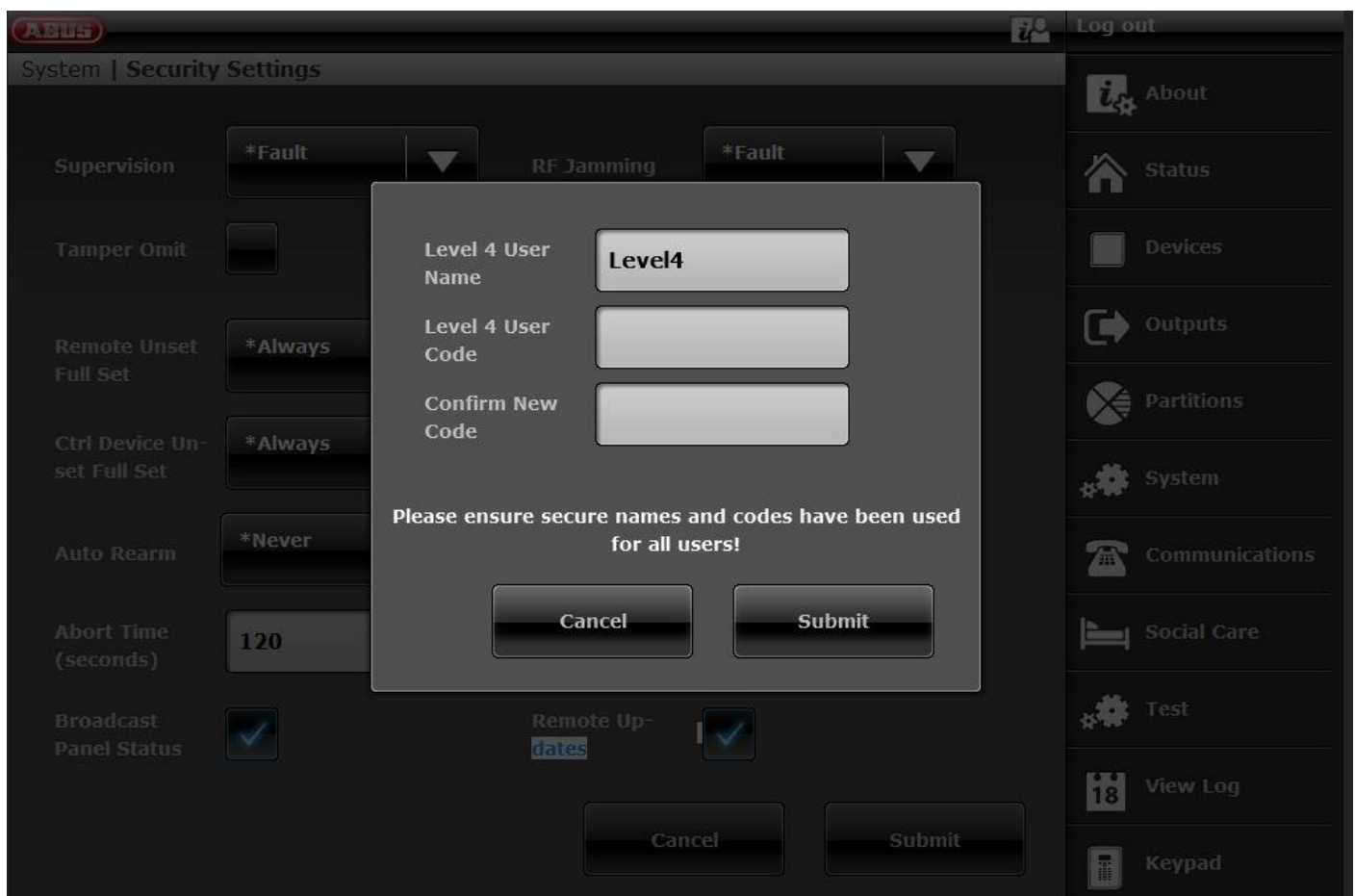
Name: "Level4"

Note:

For security reasons, you should change the "Level4" default name of the Level 4 user.

Note:

Further details can be found under the menu explanations in the corresponding instruction manuals.



### Starting the "Remote Update" procedure:

Ensure that

Alarm panel  
Installer Mode -> System -> Security -> Level4 Updates -> Enabled  
User Menu -> Configuration -> Level4 Updates -> Enabled  
Or  
WBI  
Installer Mode -> System -> Security Settings -> Level4 Updates -> Enabled (activated, ticked)

User Menu -> Configuration -> Security Settings -> Level4 Updates -> Enabled (activated, ticked)

Provided both "Remote Update" options are enabled, a Level 4 user will only be shown 3 menu options if they log in to the web server using their Level 4 User Name and Level 4 User Code:

- Level 4 User Details for amendment
  - Level 4 User Name
  - Level 4 User Code

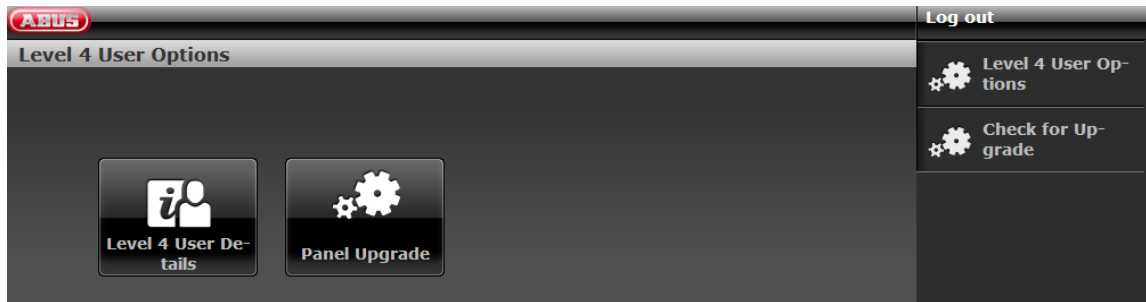
and

- Panel upgrade

These options are not displayed if you log in as an Installer.



SW >= 3.00.03

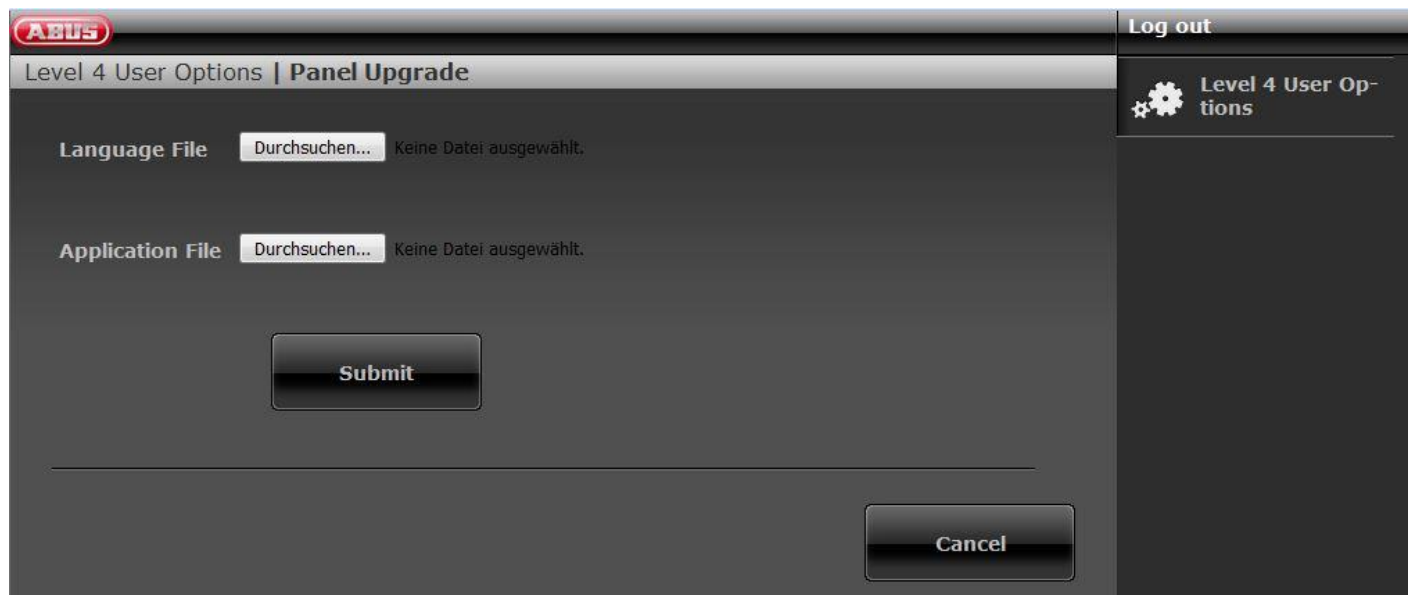


**Note**

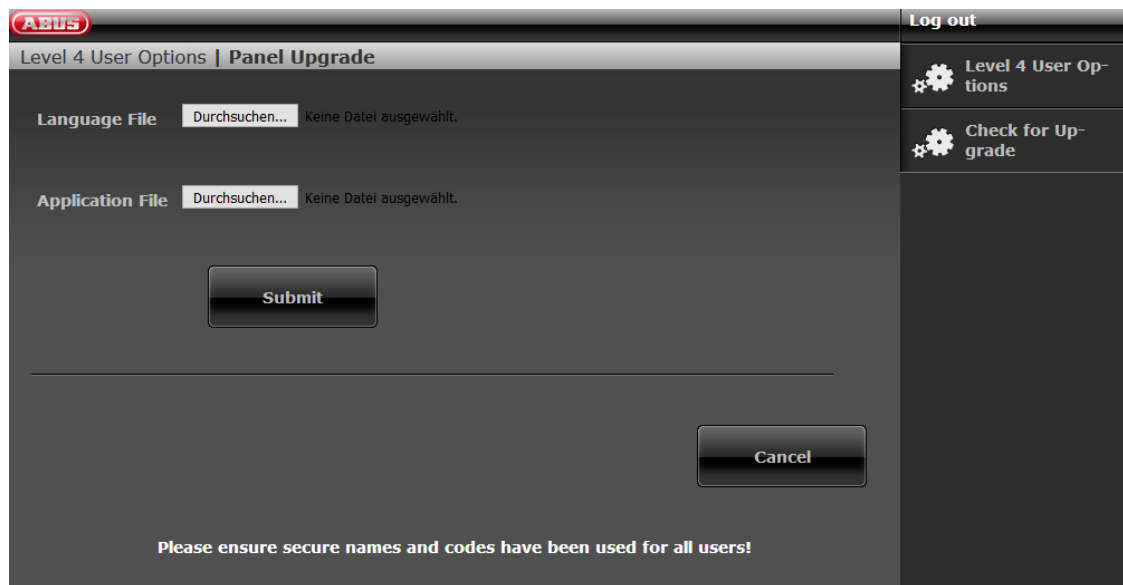


Click on this symbol to generate a PDF version of the "Release notes" file.

Click "Panel Upgrade"



SW >= 3.00.03



### Important

Please ensure that you only load

- a language file that is compatible with the existing application file or
- a application file that is compatible with the existing language file or
- a language file and an application file that are compatible with one another

Please consult the corresponding release notes when doing so.

Select a "Language file"



Click the "**Browse**" button to enter the path and file name of the language file that should be loaded.  
Click the "**Submit**" button to import the selected file into the wireless alarm system.

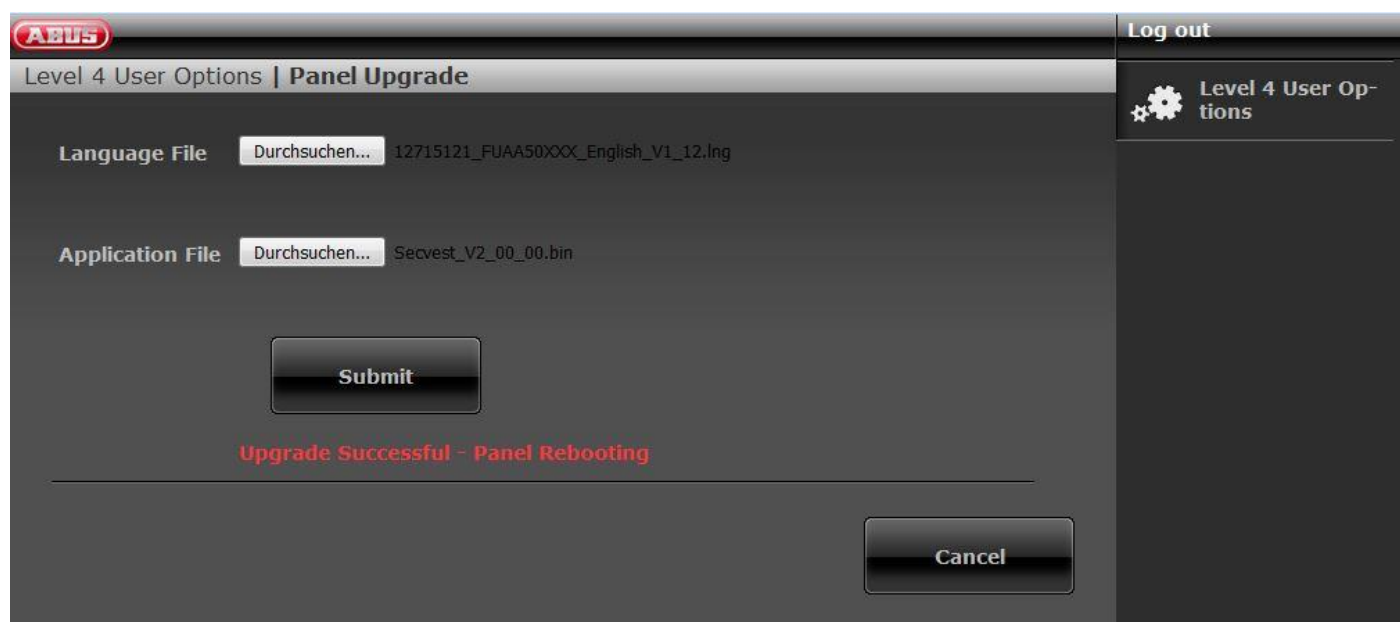
Select an "Application file"

Click the "**Browse**" button to enter the path and file name of the application file that should be loaded.  
Click the "**Submit**" button to import the selected file into the wireless alarm system.

You can also do both at the same time.

Select a "Language file".  
Select an "Application file".  
Click "Submit".

Once the download is complete, the alarm control panel will check the configuration number of the current S/W against the configuration number of the downloaded S/W. If these numbers match, the alarm control panel automatically re-starts and installs the new S/W.



If they do not match, the web server warns the user that the alarm control panel will restart, their configuration will be lost and the Installer on Site will need to come to reconfigure the alarm control panel (the alarm control panel remains in "Start assistant").

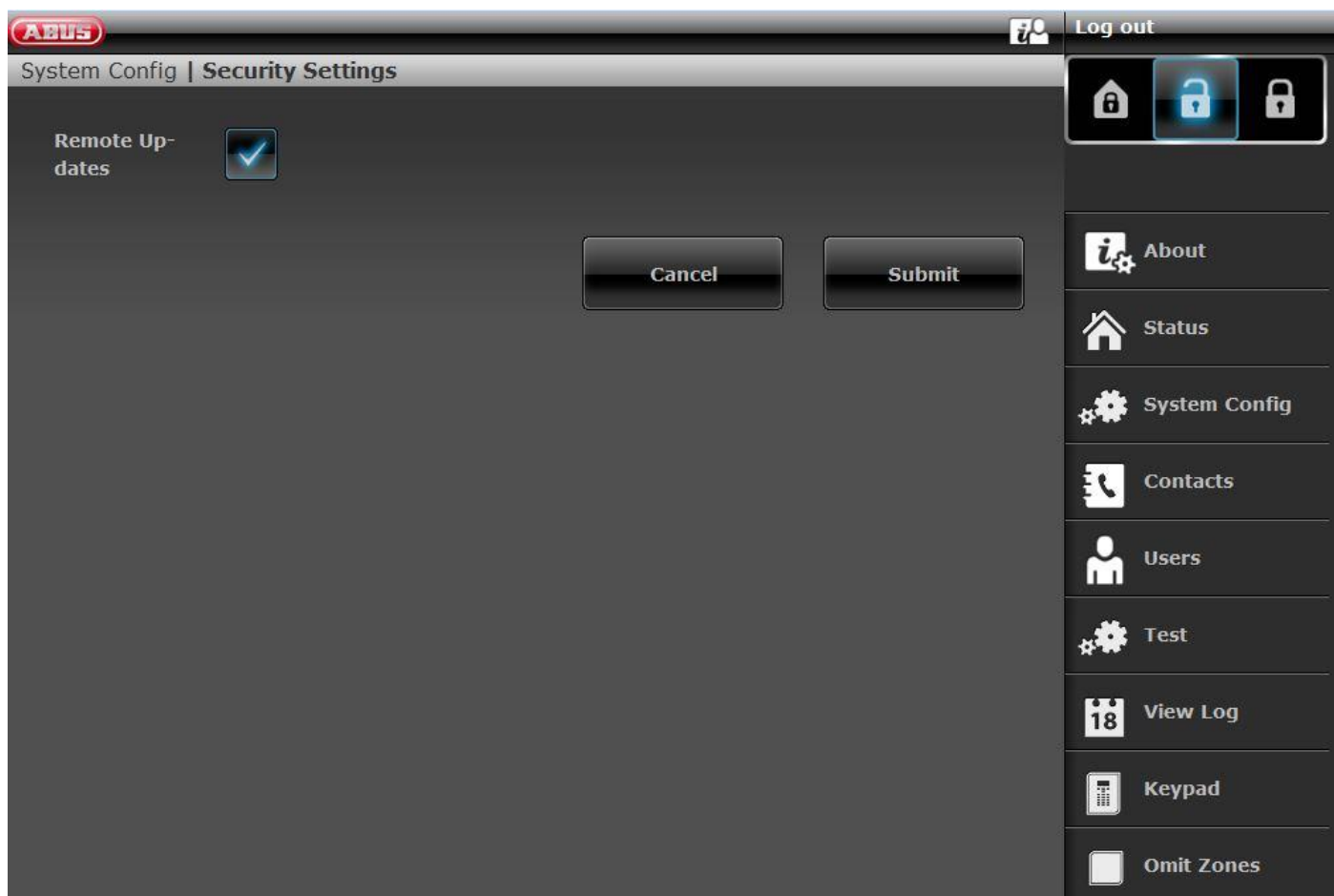
If the user selects "No", then the downloaded file will be deleted from the SD card.

This prevents a Level 3 user from arriving on-site and installing the new S/W on the SD card without opening the alarm control panel. This is not permitted for a Level 3 user, unless the alarm control panel is open.

Please note that the above-mentioned configuration number check is only run on alarm control panels, on which a version of the software with this function has already been installed (1.01.00 and later).

See also the user manual, chapter Remote Updates / Level4 Updates





Alarm panel

User Menu -> Configuration -> Level4 Updates

Or

WBI

User Menu -> Configuration -> Security Settings -> Level4 Updates

Blocked (deactivated – not ticked)

A Level 4 user can only change the "Level 4 Code" and the "Level 4 User Name".

Enabled (activated – ticked)

Provided the "Remote Update" option is also enabled in Installer Mode, a Level 4 user will only be shown 3 menu options if they log in to the web server using their Level 4 User Name and Level 4 User Code:

Level 4 User Details for amendment

Level 4 User Name

Level 4 User Code

and

Panel upgrade



**Note**

SSL certificate will be created, this can take several minutes (approx. 3 min).

Network functions are not available during this time.



**Note**

This message will display: Network initialisation, please wait...



**Note**

You can tell an update process is running from the following 3 processes on the alarm panel.

- 1)
  - Menu keys light up
  - Arm/disarm keys flash
  - Number keys are dark
4.
  - Menu keys light up
  - Arm/disarm keys are dark
  - Number keys flash
- 3)
  - Menu keys are dark
  - Arm/disarm keys start flashing again to show that the upgrade process is almost finished.
  - Number keys are dark

The first point of the start wizard appears (language selection).



**Important**

Wait until this process is fully complete. The power supply must not be disconnected during the upgrade process under any circumstances. This could lead to a complete crash/failure of the software.

If a touch front is installed, no keys light up during this process.



**Important**

Wait until something appears again on the display. The power supply must not be disconnected during the upgrade process under any circumstances. This could lead to a complete crash/failure of the software.

## Software upgrade with new files from the FTP server

SW >= 3.00.03

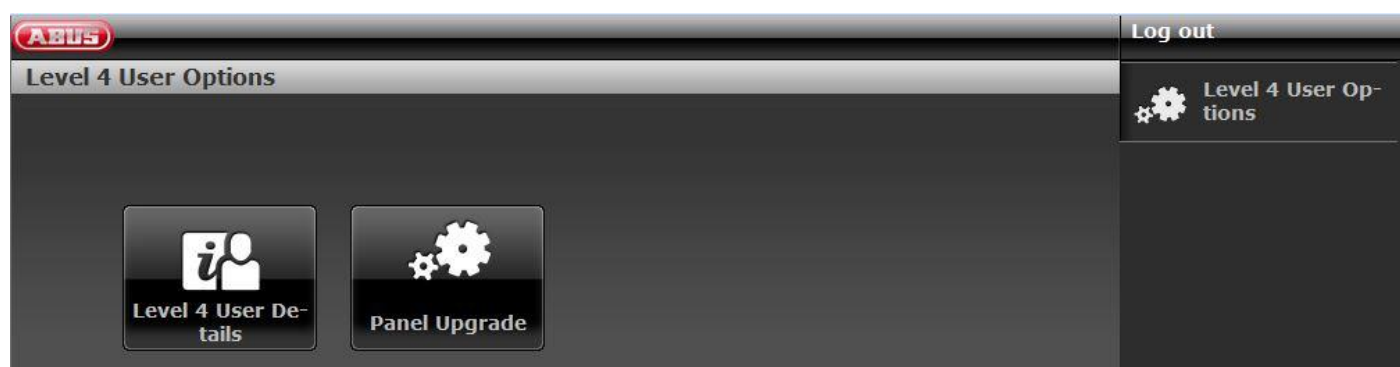


### Note

Please also observe the information in the chapter above.

This function is also available directly on the alarm panel itself. You will find further details in the chapter "System -> Check for upgrade?".

Log in to the web server as a Level 4 user.

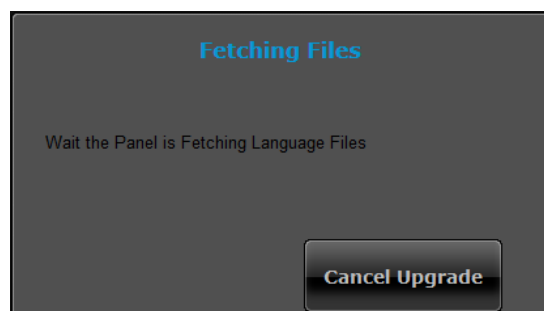
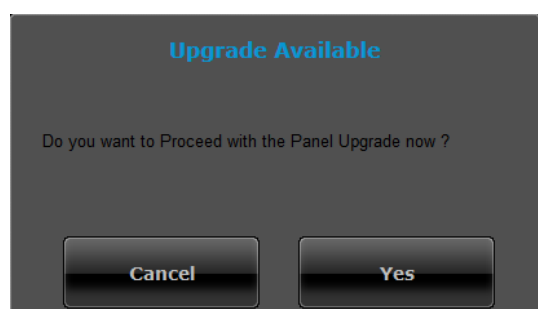


After logging in, the software automatically asks the ABUS FTP server: "Is new software available?"

You can also start this process again manually.

Click on "Check for upgrade?"

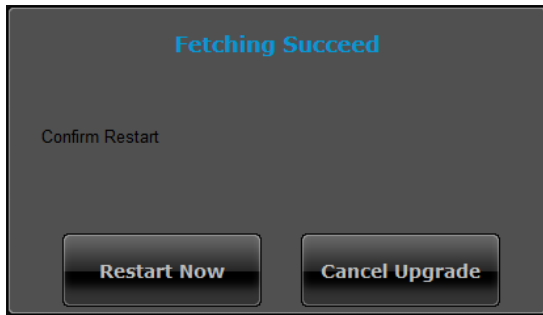
If the FTP server replies to this question with a "Yes", the following pop-up menus appear.





### Note

The current software comprises a new application file and language file. These files are stored on the SD card.



Click on "Restart the alarm panel".  
The alarm panel installs the new files and performs a reboot.



### Important

#### SW >= 3.00.06, saving and restoring the configuration

Before the alarm panel starts the upgrade, the configuration files and the SSL certificate are saved automatically on the internal flash drive. The new software is then installed, and the alarm panel restarted. At this point, the factory settings are used first, but the alarm panel then automatically reproduces the configuration files and the SSL certificate from the flash drive (as if the configuration had been saved/reproduced manually). This means that the Start Wizard is not used, the SSL certificate is not regenerated and, more importantly, that the installer does not have to go to the site in order to respond to the command prompt of the Start Wizard.

## **S/W upgrade with the Secvest update utility**

This variant is intended for special cases.

Specialist installers can request details on this from our Support team

### ARC/ESCC reporting

#### ARC/ESCC reporting protocol formats

**Note:**

To conform with EN50131, ARC (ESCC) reporting must be enabled. The alarm control panel automatically uses the classic protocols if the alarm control panel uses PSTN or GSM/wireless mobile as an outgoing communication path.

**Fast Format**

When using Fast Format, each message sent to the ARC (ESCC) consists of the following:

4, 5 or 6-digit account number.

8 data channels.

Each channel communicates the status of an output. The type of corresponding output (channel) is set under the "FF Channels" menu item (see page xyz). Each channel can provide the following values:

- 1 = New alarm and not yet reported
- 2 = Output status is open/disarmed
- 3 = Alarm reset and not yet reported
- 4 = Output status is closed/enabled
- 5 = No alarm
- 6 = Alarm but reported earlier

Test signal or status

**Contact ID**

The Contact ID format transmits data from the log book entries to the ARC (ESCC). Examples of messages in Contact ID format are:

**Example 1**

**1234 18 1137 01 015 2**

1234	This is the account number as specified in the Account Numbers menu item (page xyz).
18	This is the message type used to identify the message as a Contact ID
1137	This is the event identifier for a new event (1), followed by the event code for a system tamper alarm (137)
01	This is the partition number
015	This is the zone number
2	This is the checksum value that the ARC (ESCC) needs to check and confirm that a valid message has been received

**Example 2**

**1234 18 3137 01 015 3**



The only difference between this example and the first example is the event identifier of 3 to show a restore for the system tamper alarm and the checksum value.

### SIA 1, SIA 2, SIA 3, Extended SIA 3 and Extended SIA 3 V2

The SIA formats transmit data from the log book entries to the ARC (ESCC).

The four SIA formats differ based on the data volume that is transferred with each message.

Type	Format
SIA1	#AAAAAA NCCcc
SIA2	#AAAAAA Nidnnn/rinn/CCcc
SIA3	#AAAAAA Ntihh:mm/idnnn/rinn/CCcc #AAAAAA AS
Extended SIA 3	#AAAAAA Ntihh:mm/idnnn/rinn/CCcc/AS
Extended SIA 3 V2	#AAAAAA Ntihh:mm idnnn rinn CCcc AS
Extended SIA 3 V3	#AAAAAA Ntihh:mm/idnnn/rinn/CCcc^AS^

Whereby:

AAAAAA	Adjustable 6-digit account number (e.g. 123456).
"N"	New event (always N)
"ti"hh:mm/	Time (e.g. ti10:23/).
"id"nnn/	User number, when usable, otherwise not sent (e.g. id123/ or id6/)
"ri"nn/	Partition number (e.g. ri12/ or ri3).
CC	Event code (e.g. FA = Fire Alarm).
cc	Zone or control panel number, when usable, otherwise not sent (e.g. 23 or 5)
"A"S	Text description of the event, usually a description of the log book event

#### Note:

The alarm control panel sends the characters that are between " and " shown above exactly as they are listed in the table above.

#### Example

The different formats for the SIA protocol appear as follows in the event of a fire alarm in zone 2 of partition 4 at 10:15 with the account number 10 for partition 4:

SIA1	#000010 NFA2
SIA2	#000010 N/ri4/FA2
SIA3	#000010 Nti10:15/ri4/FA2 #000010 AFire Zone 2
Extended SIA3	#000010 Nti10:15/ri4/FA2/AFire Zone 2
Extended SIA3 V2	#000010 Nti10:15 ri4 FA2 AFire Zone 2
Extended SIA3 V3	#000010 Nti10:15/ri4/FA2^AFire Zone 2^

#### Note about Extended SIA3 V2:

## Appendix

---

Some S/W versions that work in the SIA recipients do not always recognise the "/" text separator. This may cause problems. This incorrectly results in "mains fail" messages on the ARC (ESCC). This may occur when arming or disarming the alarm control panel or when entering or exiting the Installer Mode.

Therefore, in version 2 of Extended SIA3, the "/" text separator has been replaced by a "|" text separator.

For example, the string will change from:

#000010|Nti10:15/ri4/FA2/AFire Zone 2

to:

#000010|Nti10:15|ri4|FA2|AFire Zone 2

If you are having problems with incorrect "power failure" messages, try this extended SIA3 V2 option.

### Note about Extended SIA3 V3:

Some S/W versions that work in the SIA recipients do not always recognise the "/" text separator. This may cause problems.

Therefore, in version 3 of Extended SIA3, the "/" text separator has been replaced by a "^" text separator in two positions.

For example, the string will change from:

#000010|Nti10:15/ri4/FA2/AFire Zone 2

to:

#000010|Nti10:15/ri4/FA2^AFire Zone 2^

## DC-09



### Note

The provisions of the following document apply here.

**ANSI/SIA DC-09-2013: Internet Protocol Event Reporting  
SIA Digital Communication Standard – Internet Protocol  
Event Reporting**

S/W <= v3.00.03 Messages are sent **without encryption (unencrypted)**.

S/W >= v3.00.03 Messages can also be sent **with encryption**.

The alarm control panel automatically uses the IP-based protocol DC-09 if the alarm control panel uses Ethernet (LAN) as an outgoing communication path.

In doing so, the data from traditional protocols are packed into IP packages and transferred.

Note:

Details can be found in the DC-09 and DC-07 specification from SIA and in the corresponding standards that are mentioned in these documents.

The **tokens** used are:

Protocol	Token	Definition
FF	"SCN-S8"	Scancom 4-8-1, 5-8-1, 6-8-1
CID	"ADM-CID"	Ademco Contact ID
SIA 1, SIA 2, SIA 3, Ex SIA 3, Ex SIA 3 V2, Ex SIA 3 V3	"SIA-DCS"	SIA DCS

## TCP

The **TCP** internet protocol is used for the transmission.



### Note

TCP uses port 9999.

If it is not possible to send messages, it may be that the firewall has also blocked various **outgoing** ports. Therefore, check the firewall settings on the router/IAD.

Information on implementation in the Secvest with reference to chapter 5.5.1 "Event Messages (PE)" of the CD-09 specification.

Contents	Chapter DC-09 Specification	Use in the Secvest	Comments
LF	5.5.1.1	Yes	
CRC	5.5.1.2	Yes	
OLLL	5.5.1.3	Yes	
ID	5.5.1.4	Yes	Token, see above
Seq	5.5.1.5	Yes	
Rrcvr	5.5.1.6.3	No	Nothing is sent
Receiver number			
Lpref	5.5.1.6.2	No	L0 is sent
Account prefix			
#acct	5.5.1.6.1	Yes	
Account number			
Pad	5.5.1.7	Yes	Within the parentheses "[" and "]"
Data	5.5.1.7	Yes	Within the parentheses "[" and "]"
Timestamp	5.5.1.9	Yes	Only in encrypted messages. Actual GMT Time difference (inaccuracy) between central time and ARC/ESCC recipient time must be max. +20/-40 seconds.
CR	5.5.1.10	Yes	



#### Note

A time zone is an area consisting of several countries and parts of larger countries in which the same officially-regulated time applies.

The zone time indicates 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

### CID/SIA Events

This menu only appears if you select "Contact ID" or one of the SIA versions at the following point:

Installer Mode -> Communication -> ARC Reporting -> Protocol

A detailed description of the CID and SIA formats can be found in the "ARC (ESCC) reporting protocol formats" appendix

To simplify the programming, the possible CID/SIA events are assigned to corresponding groups. In Table 1 and 3, you can see the CID/SIA events with the corresponding group assignment. In Table 2 and 4, you can see the groups with the corresponding CID/SIA events.

If you approve a group using "Yes", the alarm control panel can send every event from this group.

Notes:

CID/SIA alarm transmissions require significantly more time than Scancom Fast Format as the system transfers extended alarm data to the alarm receiving centre (ARC, ESCC).



#### Note

The alarm control panel delays the ARC reporting and entering in the log book by approx. 15-22 minutes (randomly), either in the event of a mains failure (power cut) or when leaving the Installer Mode with an existing mains failure (power cut).

The alarm control panel delays the ARC reporting and entering in the log book by approx. 60-90 seconds (randomly), either once the power supply is restored or when leaving the Installer Mode and the power supply is restored.

Table 1 CID codes – CID report groups

CID code	Contains:	CID report group
100	Medical alarm	Medical Alarm
101	Social Care (Social Emergency)	Medical Alarm
110	Fire Alarm and Fire Restore	Fire
120	Hold Up zone (Panic) and Restore Hold Up (Panic) silent and Restore Hold Up keypad (Panic) and Restore Hold Up RF (Panic) and Restore Hold Up wireless control panel (Panic) and Restore	Panic alarm
121	Duress Code alarm	Panic alarm
129	Hold Up (Panic) alarm acknowledged	Panic alarm
130	Intrusion Alarm and Intrusion Restore	Intruder alarm
131	Perimeter and Perimeter ok Entry attempt and glass breakage e.g. of FTSE	Intruder alarm
137	Alarm control panel housing front tampering and Restore Keypad tampering and Restore Detector tampering and Restore Control panel tampering and Restore Bell tampering and Restore Wireless control panel tampering and Restore External Sirens tampering and Restore WAM tampering and Restore Door Lock tampering and Restore	Tampers
139	Alarm confirmation	Intruder alarm
150	Technical alarm and Restore	Technical Alarm
150	Key Box open and closed	Key Box
300	Fault and Restore for: Aux. 12 V, system 12 V	Faults
301	A/C mains fail and Restore Alarm panel, HyMo	Mains Fault
302	Panel Battery flat/fault and Restore	Panel Battery
305	System or partition reset	Reset
311	Panel Battery flat/missing and Restore	Panel Battery
311	External battery fault and Restore	Faults
320	External sounder zone fault and Restore WAM fault and Restore	Faults
337	Indoor sounder, control panel, repeater, HyMo, smoke alarm, UVM PSU fault and Restor	RF Battery/PSU
337	External PSU fault and Restore via Zone n HyMo	Faults
338	External siren, UVM, repeater Flat battery / battery fault and Restore	RF Battery/PSU
338	External PSU low voltage via Zone n	Faults

## Appendix

342	External PSU AC fault and Restore	Faults
344	Jamming fault and Restore 1)	RF Jamming
351	Communication path fault and Restore	Faults
373	Smoke alarm device fault and Restore	Faults
375	Hold Up zone component fault and Restore	Faults
380	IP zone camera supervision fault and ok e.g. IP zone missing, IP-zone timeout).	Camera supervision
381	Zone supervision fault and Restore Supervision wireless control panel fault and Restore External Siren supervision fault and Restore 1) Supervision indoor sounder fault and Restore WAM supervision fault and Restore Door Locks supervision fault and Restore Repeater supervision fault and Restore HyMo supervision fault and Restore	RF Supervision
384	Flat battery zone fault and Restore	RF Battery/PSU
401	System or partition armed and disarmed	Set/Unset
401	System or partition armed internally	Part set
406	Alarm Abort	Intruder alarm
409	System or partition armed and disarmed with key switch	Set/Unset
409	System or partition armed internally with key switch	Part set
412	Download successful	Download
457	Exit Timeout and Restore	Exit Timeout
461	4 incorrect User Codes entered one after the other (also known as "User Code Tampering")	Tampers
573	User/system zone hidden, zone shown	Omit
601	Manually triggering test report 2)	/
602	Periodic/automatic test report 2)	/
625	Reset date and time	Time/Date Reset
627	Start alarm control panel Installer Mode (Web)	Installer Mode
628	End alarm control panel Installer Mode (Web)	Installer Mode

Note:

- 1) The alarm control panel communicates Jamming and Supervision if the system is disarmed.
- 2) Independent of a group/no reference to a group

Table 2 CID report groups – CID codes

CID report group	CID code	Contains:
Fire	110	Fire Alarm and Fire Restore
Panic alarm	120	Hold Up zone (Panic) and Restore Hold Up (Panic) silent and Restore Hold Up keypad (Panic) and Restore Hold Up RF (Panic) and Restore Hold Up wireless control panel (Panic) and Restore
Panic alarm	121	Duress Code alarm
Panic alarm	129	Hold Up (Panic) alarm acknowledged
Medical Alarm	100	Medical alarm
Medical Alarm	101	Social Care (Social Emergency)
Intruder alarm	130	Intrusion Alarm and Intrusion Restore
Intruder alarm	131	Perimeter and Perimeter ok Entry attempt and glass breakage e.g. of FTSE
Intruder alarm	139	Alarm confirmation
Intruder alarm	406	Alarm Abort
Technical Alarm	150	Technical alarm and Restore
Tampers	137	Alarm control panel housing front tampering and Restore Keypad tampering and Restore Detector tampering and Restore Control panel tampering and Restore Bell tampering and Restore Wireless control panel tampering and Restore External Sirens tampering and Restore WAM tampering and Restore Door Lock tampering and Restore
Tampers	461	4 incorrect User Codes entered one after the other (also known as "User Code Tampering")
Set/Unset	401	System or partition armed and disarmed
Set/Unset	409	System or partition armed and disarmed with key switch
Part set	401	System or partition armed internally
Part set	409	System or partition armed internally with key switch
Reset	305	System or partition reset
Exit Timeout	457	Exit Timeout and Restore

## Appendix

Omit	573	User/system zone hidden, zone shown
Key Box	150	Key Box open and closed
RF Supervision	381	Zone supervision fault and Restore Supervision wireless control panel fault and Restore External Siren supervision fault and Restore 1) Supervision indoor sounder fault and Restore WAM supervision fault and Restore Door Locks supervision fault and Restore Repeater supervision fault and Restore HyMo supervision fault and Restore
RF Jamming	344	Jamming fault and Restore 1)
RF Battery/PSU	337	Indoor sounder, control panel, repeater, HyMo, smoke alarm, UVM PSU fault and Restor
RF Battery/PSU	338	External siren, UVM, repeater Flat battery / battery fault and Restore
RF Battery/PSU	384	Flat battery zone fault and Restore
Panel Battery	302	Panel Battery flat/fault and Restore
Panel Battery	311	Panel Battery flat/missing and Restore
Mains Fault	301	A/C mains fail and Restore Alarm panel, HyMo
Faults	300	Fault and Restore for: Aux. 12 V, system 12 V
Faults	311	External battery fault and Restore
Faults	320	External sounder zone fault and Restore WAM fault and Restore
Faults	337	External PSU fault and Restore via Zone n HyMo
Faults	338	External PSU low voltage via Zone n
Faults	342	External PSU AC fault and Restore
Faults	351	Communication path fault and Restore
Faults	373	Smoke alarm device fault and Restore
Faults	375	Hold Up zone component fault and Restore
Installer Mode	627	Start alarm control panel Installer Mode (Web)
Installer Mode	628	End alarm control panel Installer Mode (Web)
User Code Chnge	/	/



---

Time/Date Reset	625	Reset date and time
Camera supervision	380	IP zone camera supervision fault and ok e.g. IP zone missing, IP-zone timeout).
Download	412	Download successful
/	601	Manually triggering test report 2)
/	602	Periodic/automatic test report 2)

Note:

- 1) The alarm control panel communicates Jamming and Supervision if the system is disarmed.
- 2) Independent of a group/no reference to a group

## Appendix

**Table 3 SIA codes – SIA report groups**

SIA code	Contains:	SIA report group
AT, AR	Mains fail and Restore Alarm panel, HyMo	Mains Fault
AT, AR	External PSU AC fault and Restore Alarm panel, HyMo	Faults
BA, BR	Intrusion Alarm and Intrusion Restore	Intruder alarm
BA, BR	Perimeter and Perimeter ok Entry attempt and glass breakage e.g. of FTSE	Intruder alarm
BA, BR	Key Box open and closed	Key Box
BB, BU	User/system zone hidden, zone shown	Omit
BC	Alarm Abort	Intruder alarm
BV	Alarm confirmation	Intruder alarm
BZ	Zone supervision fault and Restore Supervision wireless control panel fault and Restore External Siren supervision fault and Restore 1) Supervision indoor sounder fault and Restore WAM supervision fault and Restore Door Locks supervision fault and Restore Repeater supervision fault and Restore HyMo supervision fault and Restore	RF Supervision
BZ	IP zone camera supervision fault and ok e.g. IP zone missing, IP-zone timeout).	Camera supervision
CA, OA	Schedule arming, schedule disarming	Set/Unset
CE	Schedule arming delayed	Set/Unset
CL	System or partition armed internally	Part set
CL, OP	System or partition armed and disarmed	Set/Unset
CS	System or partition armed internally with key switch	Part set
CS, OS	System or partition armed and disarmed with key switch	Set/Unset
EA	Exit Timeout and Restore	Exit Timeout
FA, FR	Fire Alarm and Fire Restore	Fire
FT, FJ	Smoke alarm device fault and Restore	Faults
HA, HR	Duress and Restore	Panic alarm
HV	Hold Up (Panic) alarm acknowledged	Panic alarm
Yes	4 incorrect User Codes entered one after the other (also known as "User Code Tampering")	Tampers
JT	Reset date and time	Time/Date Reset
JV	User A changes User B's code	User Code Chnge
JX	User A deletes User B	User Code Chnge
LB (RB)	Start alarm control panel Installer Mode (Web)	Installer Mode
LS (RS)	End alarm control panel Installer Mode (Web)	Installer Mode
LT, LR	Communication path fault and Restore	Faults
MA; MH	Medical alarm and Restore	Medical Alarm
OA, CA	Schedule disarming, schedule arming	Set/Unset

OR	System or partition reset	Reset
PA, PR	Hold Up zone (Panic) and Restore Hold Up keypad (Panic) and Restore Hold Up RF (Panic) and Restore Hold Up wireless control panel (Panic) and Restore	Panic alarm
PT, PJ	Hold Up zone component fault and Restore	Faults
QA, QH	Social Care (Social Emergency)	Medical Alarm
RH	User codes reset to default	User Code Chnge
RP	Periodic/automatic test report 2)	/
RS	Download successful	Download
RU	Download failed	Download
RX	Manually triggering test report 2)	/
TA, TR	Keypad tampering and Restore Detector tampering and Restore Alarm control panel housing front tampering and Restore Bell tampering and Restore Wireless control panel tampering and Restore External Sirens tampering and Restore WAM tampering and Restore Control panel tampering and Restore Door Lock tampering and Restore	Tampers
TA, TR	WAM fault and Restore	Faults
UA, UR	Technical alarm and Restore	Technical Alarm
XQ, XH	Jamming fault and Restore 1)	RF Jamming
XT, XR	Flat battery zone fault and Restore	RF Battery/PSU
YA, YH	External sounder zone fault and Restore	Faults
YM, YR	Panel Battery flat/missing and Restore	Panel Battery
YM, YR	External battery fault and Restore	Faults
YP, YQ	Indoor sounder, control panel, repeater, smoke alarm, UVM PSU fault and Restor	RF Battery/PSU
YP, YQ	Fault and Restore for: Aux. 12 V, system 12 V	Faults
YP, YQ	External PSU fault and Restore via Zone n	Faults
YT, YR	External siren, UVM, repeater Flat battery / battery fault and Restore	RF Battery/PSU
YT, YR	Panel Battery flat/fault and Restore	Panel Battery
YT, YR	External PSU low voltage via Zone n HyMo	Faults
YW	System error	Faults

## Note

- 1) The alarm control panel communicates Jamming and Supervision if the system is disarmed.
- 2) Independent of a group/no reference to a group



Table 4 SIA report groups – SIA codes

SIA report group	SIA code	Contains:
Fire	FA, FR	Fire Alarm and Fire Restore
Panic alarm	HA, HR	Duress and Restore
Panic alarm	HV	Hold Up (Panic) alarm acknowledged
Panic alarm	PA, PR	Hold Up zone (Panic) and Restore Hold Up keypad (Panic) and Restore Hold Up RF (Panic) and Restore Hold Up wireless control panel (Panic) and Restore
Medical Alarm	MA; MH	Medical alarm and Restore
Medical Alarm	QA, QH	Social Care (Social Emergency)
Intruder alarm	BA, BR	Intrusion Alarm and Intrusion Restore
Intruder alarm	BA, BR	Perimeter and Perimeter ok Entry attempt and glass breakage e.g. of FTSE
Intruder alarm	BC	Alarm Abort
Intruder alarm	BV	Alarm confirmation
Technical Alarm	UA, UR	Technical alarm and Restore
Tampers	Yes	4 incorrect User Codes entered one after the other (also known as "User Code Tampering")
Tampers	TA, TR	Keypad tampering and Restore Detector tampering and Restore Alarm control panel housing front tampering and Restore Bell tampering and Restore Wireless control panel tampering and Restore External Sirens tampering and Restore WAM tampering and Restore Control panel tampering and Restore Door Lock tampering and Restore
Set/Unset	CA, OA	Schedule arming, schedule disarming
Set/Unset	CE	Schedule arming delayed
Set/Unset	CL, OP	System or partition armed and disarmed
Set/Unset	CS, OS	System or partition armed and disarmed with key switch
Part set	CL	System or partition armed internally
Part set	CS	System or partition armed internally with key switch
Reset	OR	System or partition reset

## Appendix

Exit Timeout	EA	Exit Timeout and Restore
Omit	BB, BU	User/system zone hidden, zone shown
Key Box	BA, BR	Key Box open and closed
RF Supervision	BZ	Zone supervision fault and Restore Supervision wireless control panel fault and Restore External Siren supervision fault and Restore 1) Supervision indoor sounder fault and Restore WAM supervision fault and Restore Door Locks supervision fault and Restore Repeater supervision fault and Restore HyMo supervision fault and Restore
RF Jamming	XQ, XH	Jamming fault and Restore 1)
RF Battery/PSU	XT, XR	Flat battery zone fault and Restore
RF Battery/PSU	YP, YQ	Indoor sounder, control panel, repeater, smoke alarm, UVM PSU fault and Restor
RF Battery/PSU	YT, YR	External siren, UVM, repeater Flat battery / battery fault and Restore
Panel Battery	YM, YR	Panel Battery flat/missing and Restore
Panel Battery	YT, YR	Panel Battery flat/fault and Restore
Mains Fault	AT, AR	Mains fail and Restore Alarm panel, HyMo
Faults	AT, AR	External PSU AC fault and Restore Alarm panel, HyMo
Faults	FT, FJ	Smoke alarm device fault and Restore
Faults	LT, LR	Communication path fault and Restore
Faults	PT, PJ	Hold Up zone component fault and Restore
Faults	TA, TR	WAM fault and Restore
Faults	YA, YH	External sounder zone fault and Restore
Faults	YM, YR	External battery fault and Restore
Faults	YP, YQ	Fault and Restore for: Aux. 12 V, system 12 V
Faults	YP, YQ	External PSU fault and Restore via Zone n
Faults	YT, YR	External PSU low voltage via Zone n HyMo
Faults	YW	System error
Installer Mode	LB (RB)	Start alarm control panel Installer Mode (Web)
Installer Mode	LS (RS)	End alarm control panel Installer Mode (Web)

User Code Chnge	JV	User A changes User B's code
User Code Chnge	JX	User A deletes User B
User Code Chnge	RH	User codes reset to default
Time/Date Reset	JT	Reset date and time
Camera supervision	BZ	IP zone camera supervision fault and ok e.g. IP zone missing, IP-zone timeout).
Download	RS	Download successful
Download	RU	Download failed
/	RP	Periodic/automatic test report 2)
/	RX	Manually triggering test report 2)

## Note

- 1) The alarm control panel communicates Jamming and Supervision if the system is disarmed.
- 2) Independent of a group/no reference to a group

### 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 unrecognised
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 user name 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

## Appendix

---

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

### GSM CME / CMS Error messages

The following tables show the user-relevant error messages:

#### CME Error codes

GSM Equipment related codes

0	Phone failure
1	No connection to phone
2	Phone-adapter link reserved
3	Operation not allowed
4	Operation not supported
5	PH-SIM PIN required
6	PH-FSIM PIN required
7	PH-FSIM PUK required
10	SIM not inserted
11	SIM PIN required
12	SIM PUK required
13	SIM failure
14	SIM busy
15	SIM wrong
16	Incorrect password
17	SIM PIN2 required
18	SIM PUK2 required
20	Memory full
21	Invalid index
22	Not found
23	Memory failure
24	Text string too long
25	Invalid characters in text string
26	Dial string too long
27	Invalid characters in dial string
30	No network service
31	Network timeout
32	Network not allowed - emergency call only
40	Network personalisation PIN required
41	Network personalisation PUK required
42	Network subset personalisation PIN required
43	Network subset personalisation PUK required
44	Service provider personalisation PIN required
45	Service provider personalisation PUK required
46	Corporate personalisation PIN required
47	Corporate personalisation PUK required
48	Hidden key required
49	EAP method not supported
50	Incorrect parameters
99	Resource limitation
100	Unknown
103	Illegal MS
106	Illegal ME

107	GPRS services not allowed
111	PLMN not allowed
112	Location area not allowed
113	Roaming not allowed in this location area
132	Service option not supported
133	Requested service option not subscribed
134	Service option temporarily out of order
148	Unspecified GPRS error
149	PDP authentication failure
150	Invalid mobile class
201	Alternate SIM conflict
256	Operation temporarily not allowed
257	Call barred
258	Phone is busy
259	User abort
260	Invalid dial string
261	SS not executed
262	SIM blocked
263	Invalid block
500	CTS Handover on Progress
501	Cellular Protocol Stack out of service state
502	CTS Unspecified Error
650	General AVMS error
651	Communication error
652	Session in progress
654	RDMS services are in "deactivated" state
655	RDMS services are in "prohibited" state
656	RDMS services are in "to be provisioned" state; no available NAP
772	SIM powered down
800	SIM Security unspecified error
902	No more sockets available; the maximum number has been reached
903	Memory problem
904	DNS error
905	TCP disconnection by the server
906	TCP/UDP connection error
907	Generic error
908	Fail to accept client request's
909	Data from KTCPSND/KUDPSND incoherent
910	Bad session ID
911	Session is already running
912	No more sessions can be used (maximum session number is 32)
913	Socket connection timer timeout
914	Control socket connection timer timeout
915	A parameter is not expected
916	A parameter has an invalid range of values
917	A parameter is missing
918	Feature is not supported
919	Feature is not available
920	Protocol is not supported
921	Error due to invalid state of bearer connection
922	Error due to invalid state of session
923	Error due to invalid state of terminate port data mode
924	Error due to session busy, retry later
925	Failed to decode HTTP header's name, missing ':'
926	Failed to decode HTTP header's value, missing 'cr/lf'

## Appendix

927	HTTP header's name is an empty string
928	HTTP header's value is an empty string
929	Format of input data is invalid
930	Content of input data is invalid or not supported
931	The length of a parameter is invalid
932	The format of a parameter is invalid

### CMS Error codes

#### GSM Network related codes

1	Unassigned (unallocated) number
8	Operator determined barring
10	Call barred
21	Short message transfer rejected
27	Destination out of service
28	Unidentified subscriber
29	Facility rejected
30	Unknown subscriber
38	Network out of order
41	Temporary failure
42	Congestion
47	Resources unavailable, unspecified
50	Requested facility not subscribed
69	Requested facility not implemented
81	Invalid short message transfer reference value
95	Invalid message, unspecified
96	Invalid mandatory information
97	Message type non-existent or not implemented
98	Message not compatible with short message protocol state
99	Information element non-existent or not implemented
111	Protocol error, unspecified
127	Interworking, unspecified
128	Telematic interworking not supported
129	Short message Type 0 not supported
130	Cannot replace short message
143	Unspecified TP-PID error
144	Data coding scheme (alphabet) not supported
145	Message class not supported
159	Unspecified TP-DCS error
160	Command cannot be executed
161	Command unsupported
175	Unspecified TP-Command error
176	TPDU not supported
192	SC busy
193	No SC subscription
194	SC system failure
195	Invalid SME address
196	Destination SME barred
197	SM Rejected-Duplicate SM
198	TP-VPF not supported
199	TP-VP not supported
208	D0 SIM SMS storage full

209	No SMS storage capability in SIM
210	Error in MS
211	Memory capacity exceeded
212	SIM Application Toolkit busy
213	SIM data download error
255	Unspecified error cause
300	ME failure
301	SMS service of ME reserved
302	Operation not allowed
303	Operation not supported
304	Invalid PDU mode parameter
305	Invalid text mode parameter
310	SIM not inserted
311	SIM PIN required
312	PH-SIM PIN required
313	SIM failure
314	SIM busy
315	SIM wrong
316	SIM PUK required
317	SIM PIN2 required
318	SIM PUK2 required
320	Memory failure
321	Invalid memory index
322	Memory full
330	SMSC address unknown
331	No network service
332	Network timeout
340	NO +CNMA ACK EXPECTED
500	Unknown error
512	User abort
513	Unable to store
514	Invalid status
515	Device busy or invalid character in string
516	Invalid length
517	Invalid character in PDU
518	Invalid parameter
519	Invalid length or character
520	Invalid character in text
521	Timer expired
522	Operation temporary not allowed
532	SIM not ready
534	Cell broadcast error unknown
535	Protocol stack busy
538	Invalid parameter
615	Network failure
616	Network is down
639	Service type not yet available
640	Operation of service temporary not allowed
764	Missing input value
765	Invalid input value
767	Operation failed

### Log

#### Log book entries

This appendix provides a short explanation of the messages that may appear in the alarm panel log. Please note that many of these messages refer to specific components with the respective component numbers. For this reason, it is not possible to show the exact log messages that you would see in a particular installation in this list. The list itself is in alphabetical order according to the message text. In the "Log entry" column you will see "==" or sometimes "#". These characters stand for zone, user or component numbers which the alarm panel has recorded for the event. In the "Explanation" column, this will be displayed as "nn" or "n". In the listed communication messages, "\$m" stands for the type of the communication channel used.

Log book entry	Explanation
"\$m Alarm OK"	Successful alarm transmission to the ARC via the corresponding transmission path (PSTN / IP / GSM / wireless mobile)
"\$m Email Fail"	\$m Email Fail
"\$m Line Restore"	Communication channel restored
"\$m Line Fault"	Communication channel fault
"\$m Modem Fault"	\$m modem fault
"\$m Modem Restore"	\$M Modem Restore
"\$m fault ESCC protocol"	\$m fault in communication monitoring station log
"\$m Social Fail"	\$M fail when sending the social care protocol
"\$m SMS Fail"	\$m SMS Fail communication
"\$m Speech Fail"	\$m Speech Dialler failed
"\$m WAN fault"	Faults in the IP communication channel <ul style="list-style-type: none"> <li>o Public area (WAN)</li> <li>o Private area (LAN)</li> </ul> in addition to the "Ethernet communication channel" directly at the alarm panel
"\$m WAN OK"	IP communication channel restored
"== A/C Fail Flt"	Extension == power supply restored
"== A/C Fail Rst"	Extension == power supply failure
"== Aux Fuse Flt"	Extension == fuse missing
"== Aux Tamper Rstr"	Extension == fuse restored
"== Aux1 O/P Flt"	Extension == power failure in output 1
"== Aux1 O/P Rst"	Extension == power in output 1 OK
"== Aux2 O/P Flt"	Extension == power in output 2 faulty
"== Aux2 O/P Rst"	Extension == power in output 2 ok
"== Miss Batt 1"	Extension == battery 1 missing
"== Batt 1 OK"	Extension == battery 1 ok
"== Miss Batt 2"	Extension == battery 2 missing
"== Batt 2 OK"	Extension == battery 2 ok



"== Ex Keys Rstr"	Tampering via too many incorrect code entries will be reset
"== Chargr 1 Flt"	Extension == battery 1 charger faulty
"== Chargr 1 RESTORE"	Extension == battery 1 charger ok
"== Chargr 2 FLT"	Extension == battery 2 charger faulty
"== Chargr 2 Restore"	Extension == battery 2 charger ok
"== Load 1 OK"	Extension == battery 1 load test OK
"== Load 2 OK"	Extension == battery 2 load test OK
"== Load 1 Fail"	Extension == load test for battery 1 failed
"== Load 2 Fail"	Extension == load test for battery 2 failed
"== Low Voltage"	Extension == power supply low
"== Low Batt 1"	Extension == battery 1 low
"== Low Batt 2"	Extension == battery 2 low charge
"== Sys Volt Flt"	Extension == system voltage fault
"== Sys Volt Rst"	Extension == system voltage repaired
"== Coms O/P Rst"	Extension == communication output restored
"== Coms O/P Flt"	Extension == communication output faulty
"== Voltage OK"	Extension == power supply OK
"Auxiliary 12V Rstr"	Alarm panel 12V output restored
"Auxiliary 12V Fail"	Alarm panel 12V output faulty
"Keypad 12V Restore"	Control panel 12V power supply restored
"24 hr Z=== Alarm"	24-hour alarm in zone n.
"24 hr Z=== OK"	24-hour alarm reset in zone n.
"24 hr Z== Alarm"	24-hour alarm in zone n.
"24 hr Z== OK"	24-hour alarm reset in zone n.
"Log out"	Logged out from the web server
"A/C restore"	Mains voltage was restored
"A/C Rstr Ptn ##"	Power supply fault in partition ## was reset
"A/C Fail Ptn ##"	Power supply fault in partition ##
"A/C fail"	No mains voltage
"Batt# Charger Rstr"	Battery # charged
"Batt# Charger Fail"	Battery # charging failure
"Battery # Load OK"	Battery # load test OK
"Batt # Load Fail"	Battery # load test failure
"Batt # Fault Rst"	Battery # failure corrected
"Batt # Low/Missing"	Battery # is low or missing
"Batt Load Tst Fail"	Battery load test failed
"Batt Low/Missing"	Battery is low or missing
"Set Fail Z=="	Arming not possible, zone == faulty or open
"Alarm CONF web server"	Alarm confirmed by web server
"Alarm CONF Z=="	Alarm confirmed by zone ==

## Appendix

"Alarm CONF "	Alarm confirmed on keypad
"Alarm CONF aux #"	Alarm confirmed by equipment # tampering
"Alarm CONF==ER"	Alarm confirmed by external proxy reader ==ER
"Alarm CONF =="	Alarm confirmed by extension ==*
"Alarm test call"	Test alarm has been triggered
"Alarm abort U--"	Alarm abort by user --
"Alarm Confirm K=="	Confirmed alarm control panel ==
"Alarm CONF CDV=="	Confirmed alarm wireless control panel ==
"Alarm CONF bell #"	Confirmed alarm sounder#
"Alarm sound generator"	Confirmed alarm sound generator
"Alarm CONF siren =="	Confirmed alarm siren ==
"Alarm CONF WAM =="	Confirmed alarm WAM ==
"AlarmCONF Z=="	Confirmed alarm zone ===
"Alarm CONF panel lid"	Confirmed alarm control panel tampering
"Alarm CONF aux"	Confirmed alarm connected accessories
"Alarm confirm"	Confirmed alarm
"Alarm CONF RPT=="	Confirmed alarm repeater
"Alarm CONF panel jam"	Confirmed alarm control panel jamming
"Log in"	Logged in to the web server
"ATE L.F. All"	All alarm transmission unit lines are faulty
"ATE L.F. Single"	One alarm transmission unit line is faulty
"ATE L.F. Restore"	All alarm transmission unit lines are repaired
"Auto Part Set #"	System # internally automatically activated
"Auto System Unset"	System automatically deactivated
"Auto System Set"	System automatically activated
"Auto Ptn # Set"	Partition # automatically activated
"Auto Ptn # Unset"	Partition # automatically deactivated
"Autoset off Ptn #"	Autoset partition # is disarmed
"Autoset on Ptn #"	Autoset partition # is activated
"Autoset defer U--"	Autoset was shunted by user --
"AS defer U-- P#"	User -- has delayed autoset of partition #
"Autoset off"	Autoset is switched off
"Autoset on"	Autoset is switched on
"Autoset Fail P#"	Autoset partition # is faulty
"Auto Ptn # PtSet"	Partition # internally automatically activated
"Aux # Tamper Rstr"	Tampering with the power supply, external device # reset
"Aux. 14V4 # Fail"	Alarm panel 14 V output faulty
"Aux Tamper Rstr"	Tampering with the power supply, external device reset
"Aux # Tamper"	Tampering with the power supply, external device #
"Aux 14V4 # Rstr"	Alarm panel 14 V output OK
"Aux Tamper"	Tampering with the power supply, external device
"U-- Sys. PtSet #"	User -- has part set the system
"U-- Set Override"	User -- has cancelled system activation

"U-- Download Fail"	User == download failure
"U-- Config Change"	The configuration was == changed by the user
"U--- PtSet # Exit"	User -- has started the output delay from output #
"U--- Medical Alm"	Medical emergency alarm triggered by user --
"U-- Panel Restart"	User -- has restarted the alarm control panel
"U--- Duress Restr"	Duress alarm from user == reset
"U--- Duress"	Duress alarm from user ==
"U--- Shunt Code"	Shunt code from user -- entered
"U-- Spch Tel = Chg"	User -- has changed a number on the speech dialler
"U-- System Exit"	User -- has started the exit delay
"U--- Ptn ## Exit"	User -- has activated the output delay in partition ##
"U--- Ptn ## Duress Rstr"	Duress alarm from user == in partition ## reset
"U--- Ptn ## Duress"	Duress alarm from user == in partition ##
"U-- Override"	User -- has activated system despite warning
"Low Battery Z===="	Low battery zone ===
"Low battery Z====restore"	Battery zone === restore
"Low Battery Z== restore"	Battery zone == restore
"Low Battery Z =="	Low battery zone ==
"Low Batt Restore"	Battery is OK
"Batt Low"	Low battery
"Fire Restore"	Fire alarm on control panel == reset
"K== Excess Keys"	Tampering via too many incorrect code entries on the control panel ==
"CDV== Fire"	Fire alarm on control panel == triggered
"CDV== Medical"	Control panel == medical alarm has been triggered
"CDV== HUA"	Control panel == hold up alarm has been triggered
"Occupancy Set W#"	Event log used by #
"U-- Change U =="	User -- has changed the code for user ==
"U-- On-Site"	User -- has opened the menu
"U-- Off-Site"	User -- has exited menu
"U-- Delete U =="	User -- has deleted user --
"U-- System Set"	User -- has activated the system
"U-- System Unset"	System unset by user --
"U-- System Reset"	User -- has reset the system
"U-- Ptn # Set"	User -- has activated partition #
"U-- Ptn # Unset"	User -- has disarmed partition #
"U-- Ptn # PtSet"	User -- has internally activated partition #
"U-- Ptn # Reset"	User -- has reset partition #
"U-- On-Site (Web)"	User -- has opened the web menu
"U-- Off-Site (Web)"	User -- has exited web menu
"U-- Time/Date"	User -- has changed time/date
"U-- Z == Omit"	User -- has omitted zone ==
"U-- Z === Omit Rst"	User --- has reactivated zone ===
"U-- Z === Omit"	User --- has omitted zone ===

## Appendix

"U--- Z=== HUA Omit"	Zone === hold up via user --- omitted
"U-- Soc. Emergency"	User -- has triggered an emergency social care call
"U-- Rem Download"	User == remote download successful
"Keypad == found"	New control panel == found
"Kpd == deleted"	Control panel == deleted
"Keypad == added"	Control panel == has been added
"RK== Excess Keys"	Tampering via too many incorrect code entries on the control panel ==
"Missing K=="	Control panel == missing
"Missing K== Restore"	Control panel == is restored
"U-- Ptn # Override"	User -- has activated partition # despite warning
"Care U-- Low Bat"	Care alarm battery low
"CO Z== Alarm"	Carbon monoxide alarm zone ==
"CO Z== Restore"	Carbon monoxide alarm zone == reset
"Excess Keys"	Tampering via too many incorrect code entries
"Codes Defaulted"	Codes have been reset to factory settings. Codes have been deleted and re-entered.
"Downloader Lockout"	Downloader locked out
"Wired SRN== Fault"	Wired sounder fault== Check the wiring between the TRB(Trouble) connection and 0 V as well.
"Wired SRN== Fault OK"	Wired sounder fault== has been reset
"Dup. == Restore"	Error: address given twice has been corrected
"Duplicate =="	Error: address given twice
"Burg Z== Alarm"	Burglar alarm zone ==
"Burg Z== Restore"	Burglar alarm zone == reset
"Burg Z=== Alarm"	Burglar alarm zone ===
"Burg Z=== Restore"	Burglar alarm zone == reset
"Entry Started Z==="	Zone === entry delay started
"Entry Stray Z=="	Straying from entry route, zone === triggered
"Entry Stray Z==="	Straying from entry route, zone === triggered
"Set Z=== Shunted"	Settings from zone === were shunted
"Config Change"	The configuration was changed
"Email error ---"	Email error ---
"Email error \$w"	Email error "w
"Email Test Call"	Email Test Call
"Expndr == found"	New extension == found
"Expndr == deleted"	Extension == was deleted
"Expndr == added"	New extension == has been added
"Ext A/C Rstr Z=="	Z== external supply voltage restored
"Ext A/C Rstr Z==="	Z=== external supply voltage restored
"Ext A/C Fail Z=="	External fault with Z== supply voltage
"Ext A/C Fail Z==="	External fault with Z=== supply voltage
"Ext Batt Fault Z=="	Z== external battery fault
"Ext Batt Flt Z==="	Z=== external battery fault
"Ext Batt Rstr Z=="	Z== external battery restore

"Ext Batt Rstr Z===="	Z==== external battery restore
"Ext DC Rstr Ptn ##"	External direct current in partition ## restored
"Ext DC Fail Ptn ##"	External direct current in partition ## faulty
"Ext Low Volts Z=="	Z== low voltage in external power supply
"Ext Low Volts Z===="	Z==== low voltage in external power supply
"Ext PSU Fault Z=="	Z== external power supply fault
"Ext PSU Rstr Z===="	Z==== external power supply restore
"Ext PSU Rstr Z=="	Z== external power supply restore
"Ext PSU Fail Z=="	Z==== external power supply fault
"Ext Volts Rst Z===="	Z==== external power supply restore
"Ext Volts Rstr Z=="	Z== external power supply restore
"External DC Fail"	External failure in the direct current
"Remote U-- Low Bat"	User -- remote control battery is low
"CDV== SUPERV fail"	Remote control device == Warning: radio monitoring fault detected
"CDV== Superv Rstr"	Remote control device == radio monitoring restored
"Missing == Rstr"	Extension == restored to system
"Missing == Rstr"	Missing control panel == is accessible again
"Missing =="	Extension == missing
"Missing =="	Control panel == missing
"Missing ==ER Rs"	External proxy reader == restored on control panel
"Missing ==ER"	External proxy reader == missing on control panel
"Remote Reset"	System was reset remotely
"Remsvc Complete"	Remote servicing successfully completed
"Fire alarm error was reset P#"	Fire partition # OK
"Fire Restore"	Fire alarm was reset
"Fire Restore"	Fire alarm on control panel reset
"Fire Reset"	Fire alarm was reset
"Fire Z== Alarm"	Fire alarm zone ==
"Fire Z== Restore"	Fire alarm zone == was reset
"Fire Z=== Alarm"	Fire alarm zone ===
"Fire Z=== Restore"	Fire alarm zone == was reset
"Fire alarm"	Fire alarm triggered on control panel
"Fire K== Alarm"	Fire alarm on control panel == triggered
"CDV## Care Emergency"	Remote control device ## care alarm triggered
"CDV== 4/6 Mismatch"	Remote control device == Wrong code length (4/6)
"CDV== low batt"	Remote control device battery low ==
"RK == Ex Keys Rstr"	Tampering via too many incorrect code entries on the wireless control panel == have been reset
"CDV== PSU Restore"	Remote control device == external power supply restored
"CDV== PSU Fail"	Remote control device == external power supply failure
"CDV== RF OK"	Wireless control panel == wireless connection ok
"CDV== RF Warning"	Wireless control panel == no wireless connection with the alarm panel for over 15 min
"CDV== SUPERV rstr"	Remote control device radio monitoring == restored

## Appendix

"CDV== SUPERV fail"	Remote control device == radio monitoring failure
"Enabled =="	...is enabled
"CDV== Tamper Rstr"	Remote control device == Tampering reset
"CDV== Tamper"	Remote control device == Tampering triggered
"RSN== Battery Rstr"	Radio siren == battery OK
"RSN== Low Battery"	Radio siren == low battery
"RSN== Tamper Rstr"	Radio siren == tampering error was reset
"RSN== Tamper"	Radio siren == tampering
"RSN== Superv Fail"	External siren == radio monitoring fault
"RF Failure Restore"	Radio frequency failure rectified
"RF Failure"	Radio frequency failure
"Lid Tamper Restore"	Tampering with alarm control panel housing has been reset
"Panel lid open"	Tampering with alarm control panel housing
"Disabled == "	...is disabled
"Glass Brk Rst Z===="	Glass breakage zone == was reset
"Glass Brk Z===="	Glass breakage detected in zone ==
"GSM CME Info --"	GSM CME info --
"GSM CME Info \$w"	GSM CME info \$w
"GSM CMS Info --"	GSM CMS info --
"GSM CMS Info \$w"	GSM CMS info \$w
"H/M== Tamper"	Housing opened at the hybrid module
"H/M== Tamper OK"	Housing closed at the hybrid module
"H/M== PSU battery empty"	Hybrid module power supply battery empty
"H/M== PSU battery OK"	Hybrid module power supply battery OK
"H/M== Superv fault"	No wireless connection with hybrid module for over 2 h
"H/M== Superv OK"	Wireless connection with hybrid module OK
"H/M== RF warning"	No wireless connection with hybrid module for over 20 min
"H/M== RF OK"	Wireless connection with hybrid module OK
"H/M== Jamming"	Hybrid module detected jamming
"H/M== Jamming OK"	No jamming at the hybrid module
"H/M== AC PSU fault"	230 V power supply fault at hybrid module
"H/M== AC PSU OK"	12 V power supply fault rectified at hybrid module
"H/M== DC fault"	12 V power supply fault at hybrid module
"H/M== DC OK"	12 V power supply fault rectified at hybrid module
"H/M== Aux fault"	12 V output power supply fault at hybrid module
"H/M== Aux OK"	12 V output power supply fault rectified at hybrid module
"H/M== Sounder tamper"	Sounder housing opened, TR input at hybrid module
"H/M== Sounder tamper OK"	Sounder housing closed, TR input at hybrid module
"Social Inactive P#"	Emergency social care call in partition # triggered due to inactivity
"Indoor sounder== Tamper"	Housing opened at the indoor sounder
"Indoor sounder== Tamper OK"	Housing closed at the indoor sounder
"In-SG== Low batt"	Indoor sounder batteries flat
"In-SG== Low batt OK"	Indoor sounder batteries OK

"Indoor sounder== LT sup fault"	No wireless connection with indoor sounder for over 2 h
"Indoor sounder== LT sup fault OK"	Indoor sounder wireless connection OK
"Indoor sounder== RF warning"	No wireless connection with indoor sounder for over 20 min
"Indoor sounder== RF OK"	Indoor sounder wireless connection OK
"Indoor sounder== Jamming"	Indoor sounder detected jamming
"Indoor sounder== Jamming OK"	No jamming at the indoor sounder
"Indoor sounder== PSU fault"	12 V power supply fault at indoor sounder
"Indoor sounder== PSU fault OK"	12 V power supply fault rectified at indoor sounder
"IP device disc."	IP device disconnected
"IP device connected"	IP device connected
"IP Polling Restore"	IP polling restored
"IP Polling Fault"	IP polling fault
"IP Z=== HTTP Err."	IP zone === HTTP Error
"IP Z=== Miss Rest."	IP zone === reconnected
"IP Z=== Missing"	IP zone === zone missing
"IP Z=== Timeout"	IP zone === Timeout
"IPZ=== IP Err 404"	IP zone === IP error "page not accessible"
"IPZ=== IP Err Auth"	IP zone === IP authorisation error
"Jamming == Rstr"	Extension == Jamming repaired
"Jamming =="	Extension == Jamming detected
"Comms 12V Restore"	Communication in the 12V power supply restored
"Comms 12V Fail"	Communication fault in the 12V power supply
"Comms Fail"	Communication failure
"Configuration Fail"	False configuration
"Sound generator # 12 V OK"	12 V sound generator # restored
"Sound generator # 12 V fault"	12 V fault in sound generator #
"Low Batt # Restore"	Battery # is OK
"Low Battery #"	Battery # is empty
"LO"	Login has been cancelled.
"Lockset Z=== Set"	Lock zone === has been activated
"Lockset Z=== Unset"	Lock zone === has been deactivated
"Log Event Types"	Log event types
"Log Search Cleared"	Log search ended
"Mask Restore Z==="	Masking fault zone === restored
"Mask Z==="	Masking zone ===
"Mask Fault Z==="	Masking fault zone ===
"Medi U-- Low Bat"	User's medical emergency alarm -- has a low battery
"Medical Alarm"	Medical emergency alarm triggered via control panel
"Medical Restore P#"	Medical alarm partition # restored
"Medical Restore"	Medical alarm has been restored
"Medical K== Alarm"	Medical emergency alarm via control panel == triggered
"Detector Flt Z==="	Zone === Terminal resistance fault
"Det Restore Z==="	Zone === Terminal resistance fault has been reset

## Appendix

"Soak Fail Z =="	Zone == soak fail
"Log Only"	Log only
"Batt Fault Restore"	Battery failure corrected
"External DC Rstr"	External failure in direct current restored
"Perim. Warn. Z=="	Perimeter breach alarm ==
"Social Emergency"	Care alarm triggered on control panel
"Pend U-- Low Bat"	User's care alarm -- has a low battery
"Bad Checksum"	Bad checksum
"PSTN Line Restore"	Communications fault on telephone line repaired
"PSTN Line Fault"	Communications fault on telephone line
"REP== low batt"	Repeater == battery empty
"REP== jamming Rstr"	Repeater == no jamming on the repeater
"REP== jamming"	Repeater == jamming identified
"REP== PSU failure Rstr"	Repeater == no power supply failure on the 12V input
"REP== PSU failure"	Repeater == power supply failure on the 12V input
"REP== RF warning"	Repeater == no wireless connection with the alarm panel for over 15 min
"REP== tamper Rstr"	Repeater == tamper restore
"REP== tamper"	Repeater == tamper
"REP== SUP failure Rstr"	Repeater == wireless monitoring failed, has been reset
"REP== SUP failure"	Repeater == wireless monitoring failed
"RF Jamming Restore"	Radio overlay OK
"RF Jamming"	Radio overlay
"Tamper ==ER Rst"	External proxy reader tampering == was reset
"Tamper ==ER"	External proxy reader tampering ==
"Tamper == Rstr"	Extension == tampering error was reset
"Tamper == Rstr"	Control panel == tamper alarm was reset
"Tamper =="	Extension == tampering triggered
"Tamper =="	Tamper alarm via control panel ==
"Tamper K== Restore"	Control panel == tamper alarm was reset
"Tamper K=="	Control panel == tamper alarm
"Tamper Z== Restore"	Tampering in zone == reset
"Tamper Z=="	Zone == tampering
"Tamper Z==="	Zone == tampering
"Tamper Z=== Restore"	Tampering in zone === reset
"Bell # Tamper Rstr"	Sounder # sabotage alarm was reset
"Bell # Tamper"	Sounder # sabotage alarm
"Bell Tamper Rstr"	Sounder sabotage alarm was reset
"Bell Tamper"	Sounder sabotage alarm
"Key Box Open Z===="	Key box open zone ====
"Key Box Close Z=="	Key box closed zone ==
"Key Box Open Z=="	Key box open zone ==
"Key Box Close Z=="	Key box closed zone ==
"Lock Sab Rst Z===="	Entry attempt zone == was reset



"Lock Sab Z===="	Entry attempt zone ==
"Key Sw Ptn # Set"	Partition # has been activated by the key switch
"Key Sw Ptn # Unset"	Partition # has been deactivated by the key switch
"Key Sw System Set"	System has been activated by the key switch
"Key Sw System Unset"	System has been deactivated by the key switch
"Key Sw System PtSet"	System has been activated internally by the key switch
"Key Sw Ptn # PtSet"	Partition # has been activated internally by the key switch
"SD Card Error or Not Fitted"	SD memory card error or card not fitted
"Shunt Group ## OFF"	Group ## shunting OFF
"Shunt Group ## ON"	Group ## shunting ON
"SRN== Superv Rstr"	Radio siren == radio monitoring restored
"SRN== Superv Fail"	Radio siren == radio monitoring faulty
"RSN== Superv Rstr"	External siren == radio monitoring restored
"RSN== Jamming Rstr"	Radio siren == jamming repaired
"RSN== Jamming"	Radio siren == jamming detected
"RSN== Fault Rstr"	Radio siren == fault repaired
"RSN== Fault"	Radio siren == fault
"Software changed"	The software has been changed
"Spch Tel = Ack All"	Speech dialler settings: All those called must acknowledge
"Spch Tel = No Ack"	Speech dialler settings: No acknowledgement required
"Speech Tel = Ack"	Speech dialler settings: Anyone called must acknowledge
"SRN== RF OK"	Wireless siren == wireless connection ok
"SRN== RF Warning"	Wireless siren == no wireless connection with the alarm panel for over 15 min
"PLGON Line Restore"	Integrated module in alarm panel reports communication channel OK
"PLGON Line Fault"	Integrated module in alarm panel reports faulty communication channel
"Keypad 12V Fail"	Control panel 12V power supply failure
"Set Fail Z===="	Arming not possible, zone == faulty or open
"Autoset Fail"	Autoset has failed
"Ext WD Fault Z===="	Z==== external wired sounder fault
"Remsvc Comms Fail"	Communications fault in remote servicing
"Soak Fail Z === Alm"	Soak fail zone === alarm triggered
"Soak Fail Z === Tmp"	Soak fail zone === tamper triggered
"Ext WD Restr Z===="	Z==== external wired sounder restore
"Soak Fail Z ==="	Zone === soak fail
"System 12V Restore"	12 V system supply restored
"System 12V Fail"	12 V System Fail
"System Tamper OK"	System Tamper was reset
"System Tamper"	System Tamper triggered
"System Rearmed"	System was rearmed
"System error"	Fault in main processor of alarm control panel. Try restarting.
"System start"	The system has been restarted after a power failure (main power supply and battery).
"Ptn # Remote Rst"	Partition # has been reset by the remote control device

## Appendix

"Tech Z== Alarm"	Technical alarm in zone ==
"Tech Z== Restore"	Technical alarm in zone == was reset
"Tech Z=== Alarm"	Technical alarm in zone ===
"Tech Z===Restore"	Technical alarm in zone === was reset
"Partn # Rearmed"	Partition # was rearmed
"Test Call OK"	Test call successful
"Test Call Fail"	Test call failed
"SMS Test Call"	Emergency social care test call carried out
"SMS Test Call"	SMS test call carried out
"Speech Test Call"	Speech dialler test call carried out
"Sound generator # Tamper OK"	Sabotage alarm sound generator # was reset
"Sound generator # Tamper"	Sabotage alarm sound generator # Check the wiring between the TR(tamper return) connection and 0 V as well.
"Sound generator tamper OK"	Sabotage alarm sound generator was reset
"Sound generator tamper"	Sabotage alarm sound generator Check the wiring between the TR(tamper return) connection and 0 V as well.
Trace	Trace ==
"Door PSU Fail Z===="	Door fault in the power supply zone ==
"Door PSU OK Z===="	Door power supply zone == OK again
"Dr Lock # Low Batt"	Battery empty at door lock #
"All Comms Pths Flt"	Faulty transmission along all communication paths
"All Comms Pths Rst"	Transmission along all communication paths restored
"Pri Comms Path Flt"	Primary transmission path fault
"Pri Comms Path Rst"	Primary transmission path repaired
"Sec Comms Path Flt"	Secondary transmission path fault
"Sec Comms Path Rst"	Secondary transmission path repaired
"HU K== Alarm"	Hold up alarm on control panel == triggered
"HUA Conf ==ER"	Hold up alarm confirmed by external proxy reader ==
"HUA Conf Panel Jam"	Hold up alarm confirmed by radio overlay of the alarm control panel
"HUA Restore P#"	Hold up alarm in partition # was reset
"HUA Restore"	Hold up alarm has been reset
"HUA Restore"	Hold up alarm has been reset
"HUA Restore"	Hold up alarm was reset
"HUA Z=== Alarm"	Hold up alarm in zone ==
"HUA Z=== Restore"	Hold up alarm in zone == was reset
"HUA Z== Alarm"	Hold up alarm in zone ==
"HUA Z=== Restore"	Hold up alarm in zone == was reset
"HUD Fault Z===="	Fault with hold up zone === has been reset
"HUA Confirm =="	Hold up alarm confirmed via sabotage sensor on WUM --
"HUA Confirm =="	Hold up alarm confirmed via control panel ==
"HUA Confirm Aux #"	Hold up alarm confirmed via external power supply to equipment #
"HUA Confirm Aux"	Hold up alarm confirmed via external power supply to the equipment
"HUA Confirm CDV=="	Hold up alarm confirmed via remote control device #
"HUA Conf HD =="	Hold up alarm confirmed via panic transmitter

"HUA Confirm sound generator #"	Hold up alarm confirmed by sound generator #
"HUA Confirm Sound Generator"	Hold up alarm confirmed by sound generator
"HUA Cnf RF HD U---"	Hold up alarm confirmed via user's emergency call transmitter ==
"HUA Confirm Pa CDV=="	Hold up alarm confirmed via HUA keys on wireless control panel.
"HUA Confirm SRN=="	Hold up alarm confirmed via external siren --
"HUA Cnf RF MD U---"	Hold up alarm confirmed via user's dead man switch ==
"HUA Confirm WAM=="	Hold up alarm confirmed via WUM
"HUA Confirm Websvr"	Hold up alarm confirmed by web server
"HUA Confirm Z===="	Hold up alarm confirmed from zone ==
"HUA Conf Panel Lid"	Hold up alarm confirmed by tamper contact with the alarm control panel
"Hold Up Alarm"	Hold up alarm triggered on control panel
"HUD Fault Z ==="	Fault with hold up zone ===
"Override"	System has been activated despite warning
"HUA U-- -- Alarm"	Alarm triggered by remote control of user --
"HUA U-- Low Batt"	User's remote control device -- has a low battery
"Invalid"	Invalid
"WAM== Superv Fail"	WAM == Wireless monitoring failed
"WAM== Battery Rstr"	WAM== Battery Rstr
"WAM== Low Battery"	WAM== Low Battery
"WAM== PSU Restore"	WAM== Fault with power supply
"WAM== PSU Fail"	WAM == Power supply restore
"WAM== RF OK"	WAM == wireless monitoring restore
"WAM== RF Warning"	WAM == no wireless connection with the alarm panel for over 15 min
"WAM== Tamper Rstr"	WAM== Tampering restore
"WAM== Tamper"	WAM== Tampering
"WAM== Sndr Tamper"	WAM== Sounder tampering
"WAM== Sndr Trouble"	WAM== Sounder fault
"WAM== Sndr Tmp Rst"	WAM== Sounder tampering restore
"WAM== Sndr Trb Rst"	WAM== Sounder trouble reset
"WAM== Superv Rstr"	WAM == Wireless monitoring restore
"WAM== Superv Rstr"	WAM == Wireless monitoring restore
"WAM== SupervFail"	WAM== Wireless monitoring failed
"Flood Z== Alarm"	Flood detector zone == Alarm"
"Flood Z== Restore"	Flood detector zone == was reset
"Websvr Excess Keys"	Tampering via too many incorrect code entries on the webserver access
"Websvr Ex Keys Rst"	Tampering via too many incorrect code entries on the webserver access, has been reset
"Defaults Loaded"	System set to default settings
"WSN== Trouble Rstr"	Fault with wired sirens has been reset
"WSN== Trouble"	Wired sounder fault
"Z== Follow Photos"	Photos were recorded because zone === was triggered.
"Z== PSU Rst"	Zone == smoke detector power supply unit fault reset
"Z== PSU Flt"	Zone == smoke detector power supply unit fault
"Z== Smoke PSU Rst"	Zone === smoke detector power supply unit fault reset

## Appendix

---

"Z== Smoke PSU Flt"	Zone === smoke detector power supply unit fault
"Z== Smoke Flt Rst"	Zone === smoke detector fault reset
"Z== Smoke Flt Rst"	Zone == smoke detector fault reset
"Z== Smoke Flt"	Zone == smoke detector fault
"Z== RF OK"	Zone === wireless connection ok
"Z== RF Warning"	Zone == no wireless connection with the alarm panel for over 15 min
"Z== Superv Rstr"	Zone == wireless monitoring restore
"Z== Superv Fail"	Zone == wireless monitoring failed
"Z=== Open"	Zone === is open
"Z=== Closed"	Zone === closed
"Z=== UnShunted"	Zone === was not shunted
"Z=== Smoke Flt"	Zone === smoke detector fault
"Z=== RF Warning"	Zone === no wireless connection with the alarm panel for over 15 min
"Z=== Superv Restr"	Zone === wireless monitoring restore
"Z=== Superv Fail"	Zone === wireless monitoring failed
"Z=== Shunted"	Zone === was shunted
"Z== Mon. OK"	Zone == wireless monitoring restore
"Panel A/C Restore"	Power supply to the alarm panel restored
"Panel A/C Fail"	Fault in power supply to alarm panel
"Panel Excess Keys Restore"	Tampering via too many incorrect code entries on the alarm panel has been reset
"Panel Excess Keys"	Tampering via too many incorrect code entries on the alarm panel
"Panel Ext DC Restore"	External power supply to alarm panel restored
"Panel Ext DC Fail"	Fault in external power supply to alarm panel

## User numbers

## S/W &gt;=1.01.00

User number	Explanation
00	Installer
01	Administrator
02-50	User
51	Quick Set/Quick Set keys pressed
52	Level 4/user access level 4
53	System/alarm control panel e.g. for summer/winter time change B053 time/date System 03:00:00 27/03/2015
54	Key switch
55	ARC/ESCC remote access, reset
56	Downloader
57	Virtual keypad via WBI
58	RF process
59	Alarm control panel output (without user code), status changes on the alarm control panel
60	IP Finder, ABUS IP installer This user number is recorded if the IP Finder application is used to find Secvest in the network. Name, IP address, type, status and MAC address can be determined with the IP Finder.
61	ABUS server DDNS client This user number is recorded as part of the configuration change, while the assigned ID is received after the device is added to the ABUS server.

## S/W &lt;1.01.00

User number	Explanation
00	Installer
01	Administrator
02-50	User
51	Quick Set/Quick Set keys pressed
52	System/alarm control panel e.g. for summer/winter time change B053 time/date System 03:00:00 27/03/2015
53	Key switch
54	ARC/ESCC remote access, reset
55	Downloader
56	Virtual keypad via WBI
57	RF process
58	Alarm control panel output (without user code), status changes on the alarm control panel
59	IP Finder, ABUS IP installer This user number is recorded if the IP Finder application is used to find Secvest in the network. Name, IP address, type, status and MAC address can be determined with the IP Finder.
60	ABUS server DDNS client

	This user number is recorded as part of the configuration change, while the assigned ID is received after the device is added to the ABUS server.
--	---

## Troubleshooting

### Manual restart (switching off and switching back on)

S/W >=1.01.00

This is helpful for some problems, to reset the alarm panel to a defined initial state. All the settings and configurations are retained.



#### Note

A restart is only possible when  
all partitions are "disarmed" and  
the alarm panel has completed all important communications, transmissions and actions.

There are three ways to do this

- [1] In the user menu on the alarm panel when logged in as administrator
- [2] In the user menu on the web server when logged in as administrator
- [3] On the alarm panel by pressing the "Up" and "Down" navigation keys

#### [1] Alarm panel user menu

User menu -> Configuration -> Functions -> Restart alarm panel  
You can use this to restart the alarm panel manually.



#### Note

This menu item is only visible to the administrator, i.e. the administrator must be logged into the system.

Select "Restart alarm panel" by pressing the "Change" menu key.

**You are prompted for confirmation.**

Press the "Yes" menu key.

At this point you can still cancel the restart.

Press "Back".

#### [2] Web server user menu

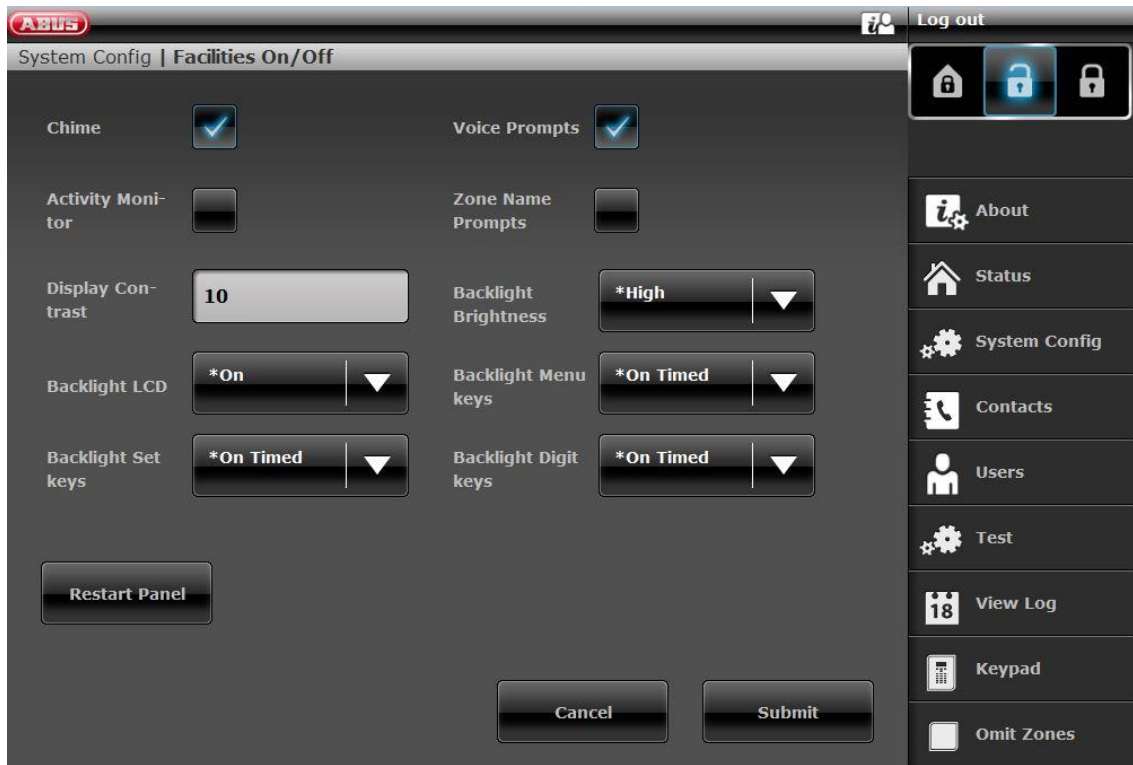
User menu -> Configuration -> Functions -> Restart alarm panel  
You can use this to restart the alarm panel manually.



#### Note

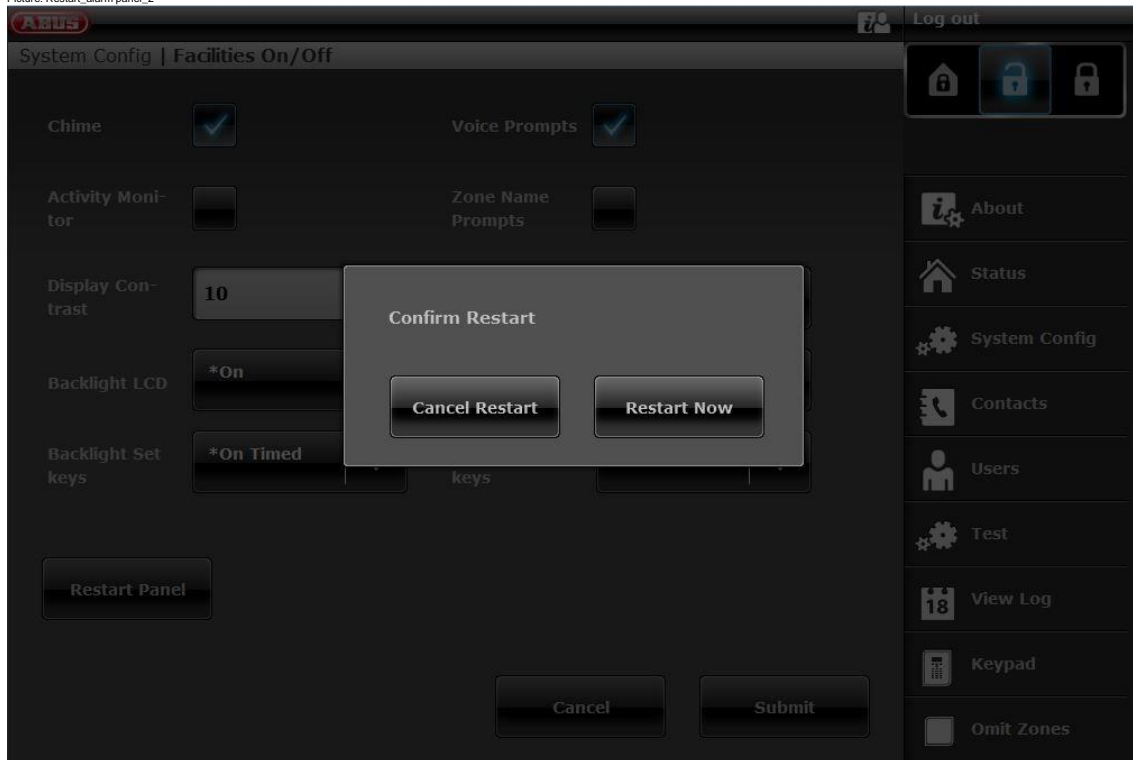
This menu item is only visible to the administrator, i.e. the administrator must be logged into the system.

Picture: Restart\_alarm panel\_1



Click on "Restart alarm panel".  
You are prompted for confirmation.

Picture: Restart\_alarm panel\_2

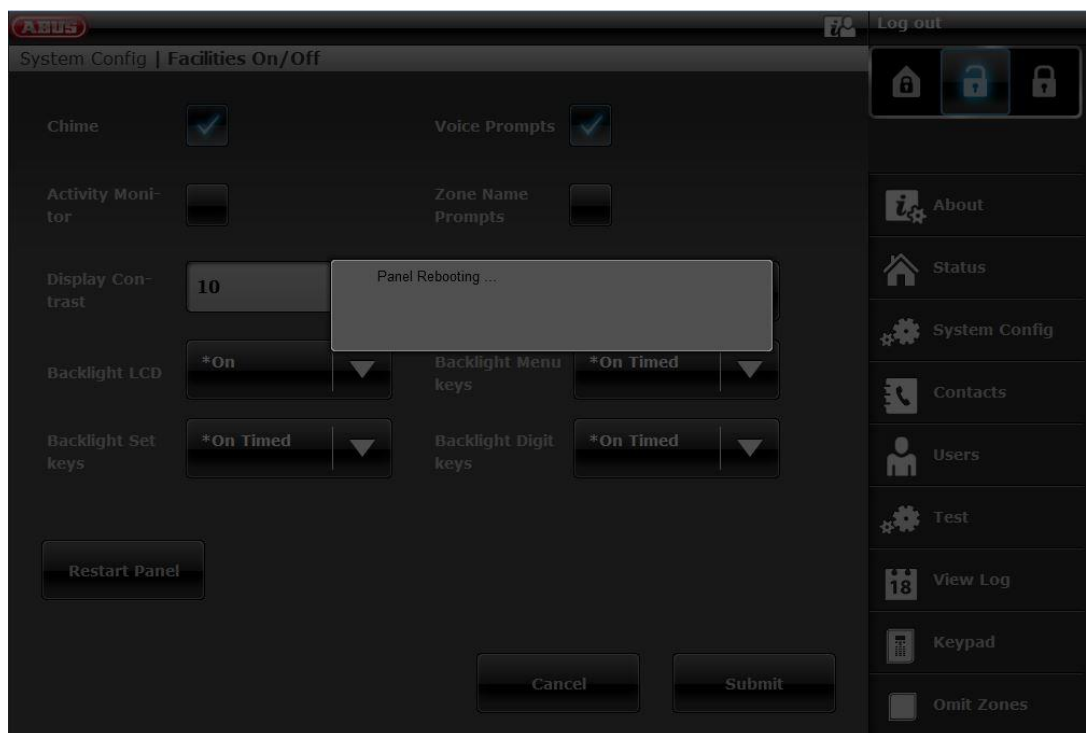


Click on "Restart alarm panel" again.  
At this point you can still cancel the restart.  
Click on "Cancel restart".

The restart is displayed as shown below.

Picture: Restart\_alarm panel\_3





After the restart you are automatically logged out of the web server. If you wish to continue working on the web server, please log in again with your user name and password.

### [3] Alarm control panel – "Up" and "Down" navigation keys

Hold down the "Up" and "Down" navigation keys simultaneously for longer than five seconds.

Installer in installer mode:

If the "Up" and "Down" navigation keys are held down simultaneously for longer than five seconds the alarm panel is restarted immediately.

Administrator in the user menu:

If the "Up" and "Down" navigation keys are held down simultaneously for longer than five seconds the alarm panel is restarted immediately.

Alarm panel in standby mode:

If the "Up" and "Down" navigation keys are held down simultaneously for longer than five seconds an access code entry screen appears.

Once a valid installer code or administrator code has been entered and subsequently confirmed with "Yes" the alarm panel is restarted.



#### Note

SSL certificate will be created, this can take several minutes.  
Network functions are not available during this time.



#### Note

This message will display: Network initialisation, please wait...

### Carry out a GSM/wireless mobile manual test call, prepaid



**Danger**  
and



**Note**

If you use a prepaid SIM card on a prepaid tariff,  
e.g. CallYa, Xtra or MagentaMobil-Start

Please carry out a GSM/wireless mobile test call and/or send a GSM/wireless mobile test text message **every month** or every **three months**.

If you do not use the GSM/wireless mobile network for a long time it can be that there is:

- no alarm call via GSM/wireless mobile,
- no alarm SMS via GSM/wireless mobile,

and the card is temporarily locked by the network operator.

The card can no longer connect to the GSM/wireless mobile network.

You will see a fault notification on the alarm panel.

This means it is **not possible** to trigger an **alarm call** or an **alarm text message**. Furthermore, the alarm panel **cannot be contacted** via GSM/wireless mobile.

If the network is not used for a long time the operator may do this with contract SIM cards as well.

Therefore, please also carry out a GSM/wireless mobile test call and/or send a GSM/wireless mobile test text message **every month** or **every three months**.

### GSM / Mobile communication module and Wi-Fi module



**Danger**

**External** must be used for the additional installation of the WI-FI module for the mobile communication antenna.

System -> Hardware -> Mobile antenna -> **External**

The internal wireless mobile antenna on the PCB can affect or completely suppress the connection of the Wi-Fi signal.

## Diagnostic LEDs on the motherboard and GSM/wireless mobile module

LED designation on the PCB	Explanation
HEARTBEAT	<p>Operating status display Flashing green, 1 Hz Normal operating status</p> <p>Secvest Update Utility in use: The "heartbeat" LED should be flashing quickly to show that the Secvest is currently working in "Update" mode.</p> <p>BOM: LED9 Y/G</p>
3V3	<p>Internal power supply 3.3 V On green Internal power supply 3.3 V is OK.</p> <p>BOM: LED7 Y/G</p>
13V8	<p>Internal power supply 13.8 V On green Internal power supply 13.8 V is OK.</p> <p>BOM: LED6 Y/G</p>
ACTIVITY	<p>Ethernet activity Off No Connection On green Connection Flashing green Activity</p> <p>BOM: LED10 Y/G</p>
B1 STATUS	<p>Battery 1 status On red Charging – preparatory treatment or constant current (CC) or constant voltage (CV). Off Charging complete Flashing red, 0.1 Hz Timer fault or cell temperature fault</p> <p>BOM: LED2 red</p>
B2 STATUS	<p>Battery 2 state On red Charging – preparatory treatment or constant current (CC) or constant voltage (CV). Off Charging complete Flashing red, 0.1 Hz Timer fault or cell temperature fault</p> <p>BOM: LED1 red</p>
OFF HOOK	<p>PSTN or a/b line status On</p>

## Appendix

	<p>The system has "lifted the telephone receiver" for PSTN</p> <p>Off</p> <p>The system has "hung up the telephone receiver" for PSTN</p> <p>BOM: LED3 red</p>
RFTX	<p>RF transmitter status</p> <p>On</p> <p>RF transmitter active</p> <p>Off</p> <p>RF transmitter not active</p> <p>BOM: LED4 red</p>
STATUS (GSM/wireless mobile module)	<p>Status GSM/wireless mobile module</p> <p>Off</p> <p>Sleep mode</p> <p>Flashing for 0.1 s in a period of 1 s</p> <p>Network search or no network status (including if the SIM card is not inserted and the PIN number is approved)</p> <p>Flashing for 0.1 s in a period of 3 s</p> <p>Connected to a 2G network</p> <p>Flashing for 0.1 s in a period of 0.125 s</p> <p>GPRS data service</p> <p>On</p> <p>Voice call</p> <p>BOM: LEDx red</p>

## Trace, recording communication sequences

Go to the following menu on the alarm control panel:

Installer Mode -> Info -> Communication

Press the \* button and then the <x> key. Below you will learn which digit "x" may be.

A live trace buffer (live mode) is displayed.

When the trace is displayed

Press the # button to see the time stamp.

Press the \* button to take a snapshot (snapshot mode). Use the up/down keys to scroll through the trace buffer. Press the \* button to return to the live mode.

Press the right-hand menu key in live mode or snapshot mode to move horizontally to the right. Go back by pressing the up or down keys.

To save the relevant trace to the SD card, press key 0 in live mode or snapshot mode. After removing the SD card, the trace can also be easily evaluated on a computer.

The trace is saved as follows:

\TRACE\trace\_0X.txt

Below you will learn which digit "x" may be.

Note:

">" means "outwards", the alarm control panel has sent it or it has been transferred from the alarm control panel.

"<" means "inwards", the alarm control panel has received it or it has been transferred to the alarm control panel.

### S/W <= v2.01.08

X = 0 = GSM / wireless mobile (e.g. "GSM – HUAWEI MG 323-B" or "plug-by")

Communication between the motherboard and the GSM/wireless mobile module, AT commands, etc.

Example:

```
AT command CSQ
< +CSQ: <rsqi>,<ber>
```

#### Parameter description

<rsqi>: receive signal strength indicator

0: ≤ -113 dBm

1: -111 dBm

2...30: -109...-53 dBm (2dBm Schritte)

31: ≥ 51 dBm

99: unknown or immeasurable

<ber>: bit error rate in percentage. The value of **ber** can be queried only during the call processing. Otherwise, only the value **0** or **99** is returned. Currently, only the value **99** is returned.

E.g.

```
+CSQ: 14,99
```

14 = -85 dBm (Secvest display RSSI 4)

Value range of up to 0-31 represents value range from Secvest 0-9

X = 1 = Email

The communication protocol between the alarm control panel and the SMTP server.

X = 2 = VoIP SIP

## Appendix

---

The communication protocol between the alarm control panel and the VoIP server.

X = 3 = Telephone call

The telephone report from the speech dialler via a/b (PSTN) or GSM/wireless mobile  
or

The telephone report from the ARC reporting via a/b (PSTN) or GSM/wireless mobile  
Note

There is no communication protocol in relation to DC-09 (ARC/ESCC IP transfer).

If you would like to produce a trace of the ARC/ESCC IP transfer, please use a corresponding network tool, e.g. Wireshark. Some routers can also be used to produce network recordings. In turn, you can use Wireshark for the evaluation.

X = 4 = HTTPS client

The communication protocol between the alarm control panel and the ABUS server.

X = 5 = HTTPS server

This view shows a snapshot recording every five seconds of the currently active HTTPS connections on the web server.

Example of a snapshot:

```
00001286.98:< # 4 | up 4 | idle 1 | host 192.168.1.204:10510 | system/partitions _=1432112428380
00001286.98:< # 3 | up 4 | idle 3 | host 192.168.1.194:54252 | logs--1
00001286.98:< # 2 | up 4 | idle 3 | host 192.168.1.194:53100 | system/partitions-2/zones
00001286.98:<HTTP(S) stats 00:21:28
```

It shows

- How long the TCP connection was (in seconds)
- How long the TCP connection was idling (in seconds)
- Host IP and port
- The requested file names, path and query string.

X = 6 = SNTP

The communication protocol between the alarm control panel and the NTP server.

Example

```
>***Timesync from ntp.exnet.com***
```

### S/W >= v3.00.03

X = 0 = GSM / wireless mobile (e.g. "GSM – HUAWEI MG 323-B" or "plug-by")

See above

IP mobile / mobile

```
>AT+CESQ
```

```
<+CESQ: 99,99,255,255,24,47
```

```
<+CESQ: <a>, <b>, <c>, <d>, <e>, <f>
```

**a, b**

informs about the signal strength and quality in **2G**

if the current supplying wireless mobile cell is **not** a 2G cell, then it will read **99**

Value range

a = signal strength, 0 (very poor) – 63 (very good)

b = quality, 0 (very poor) – 7 (very good)

**c, d**

informs about the signal strength and quality in **3G**  
 if the current supplying wireless mobile cell is **not** a 3G cell, then it will read **255**

**e, f**

informs about the signal strength and quality in **4G**  
 if the current supplying wireless mobile cell is **not** a 4G cell, then it will read **255**

Value range

e = quality , 0 (very poor) – 34 (very good)

f = signal strength, 0 (very poor) – 97 (very good)

X = 1 = Email

See above

X = 2 = VoIP SIP

See above

X = 3 = Telephone call

See above

X = 4 = HTTPS client

See above

X = 5 = HTTPS server

See above

X = 6 = SIA-IP (DC-09)

The communication protocol between the alarm control panel and ARC/ESCC. The actual DC-09 messages are listed in ASCII notation. The display of the DC-09 messages is similar to that in the examples in chapter "Appendix B: Example Message Frames" of the DC-09 specification.

```
>A38700b6**SIA-DCS"0013L0#7128[c499a115.....]....
```



**Note**

As required for DC-09, time stamps refer to GMT.

X = 7 = SNTP

The communication protocol between the alarm control panel and the NTP server.

Example

```
>***Timesync from ntp.exnet.com***
```

X = 8 = PPP

Point-to-Point Protocol

Mainly for mobile transmission

Example

```
>ATDT*99***1H
```

```
<CONNECT
```

tone dialling

X = 9 = Cloud Connection

The communication protocol between the alarm control panel and the ABUS cloud.

Example:

```
>Panel ID: U0yVq7k.....
```

X = 10 = System (**S/W >= v3.01.01**)

10 = Press the ▲ "Up" menu key

This view displays system errors

X = 11 = cameras (**S/W >= v3.01.09**)

11 = Press the ▼ "Down" menu key

This view shows communication faults between the alarm panel and the cameras.

X = 12 = ICMP Ping (**S/W >= v3.01.16**)

12 = Press the "Back" menu key

This view shows the Ping communication log between the alarm panel and the ABUS server.

Example when everything is OK:

- Ping triggered
- Trying DNS for ping.abus-server.com
- Sent ping request to 91.250.95.198
- Ping reply OK



### Note

(**S/W >= v3.01.16**)

Use \* followed by the 1 key and then press 1 repeatedly to cycle through the logs (the screens) of the respective communication processes.

## Router, IAD, Firewall

### ARC/ESCC reporting and DC-09



### Note

The **TCP** internet protocol is used for the transmission. TCP uses port 9999.

If it is not possible to send messages, it may be that the firewall has also blocked various outgoing ports. Therefore, check the firewall settings on the router/IAD.

TCP port 9999 uses the Transmission Control Protocol. TCP is one of the main protocols used in TCP/IP networks. TCP is a connection-based protocol; it requires handshakes to set up end-to-end communication. Only once a connection has been established can user data be sent bidirectionally via the connection.

Note: TCP guarantees the delivery of data packets to port 9999 in the order in which they are sent. Guaranteed communication via TCP port 9999 is the main difference between TCP and UDP.



---

## Time zones

A time zone is an area consisting of several countries and parts of larger countries in which the same officially-regulated time applies.

The zone time indicates 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

### Landline notification centre

Germany

<b>F-SMSC operator</b>	<b>Protocol</b>	<b>Service Centre Tel.</b>
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
<b>Telekom (D1)</b>	Telekom	+49 (0)1710760000
<b>Vodafone (D2)</b>	Vodafone	+49 (0)1722270333 (alternative: +49 (0)1722270000)
<b>o2</b>	o2	+49 (0)1760000443
<b>BASE (E-Plus)</b>	E-Plus	+49 (0)1770610000
<b>mobilcom- debitel</b>	Telekom	+49 (0)1710760315
	Vodafone	+49 (0)1722270880
	o2	+49 (0)1760000462
	E-Plus	+49 (0)1770602300
<b>1&amp;1</b>	Vodafone	+49 (0)1722270333 (alternative: +49 (0)1722270000)
<b>blau.de</b>	E-Plus	+49 (0)1770610000
<b>callmobile</b>	Telekom	+49 (0)1710760000
	Vodafone	+49 (0)1722270333
<b>congstar</b>	Telekom	+49 (0)1710760000
<b>FONIC</b>	o2	+49 (0)1760000443
<b>klarmobil</b>	Telekom	+49 (0)1710760000
	o2	+49 (0)1760000466
<b>McSIM</b>	Vodafone	+49 (0)1722270333 (alternative: +49 (0)1722270000)
<b>PHONEX</b>	o2	+49 (0)1760000443
<b>simyo</b>	E-Plus	+49 (0)1770610000

\* All information subject to change.

### 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

\*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

**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

## Appendix

---

### 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

## IP Mobile Setup / Mobile Data Communication



### Note

Here is some access data. Due to the large number of mobile network providers in Europe and an even larger number of SIM card providers (service providers), these are only a few selected examples.

All information subject to change.

### Vodafone Deutschland

APN	web.vodafone.de
User name	Without/empty
Password	Without/empty

### Telekom Deutschland

APN	internet.telekom
User name	t-mobile
Password	tm

### blau Deutschland

APN	internet.eplus.de
User name	Blue
Password	Blue

### Eplus Deutschland

APN	internet.eplus.de
User name	eplus
Password	Internet

### Aldi Talk Deutschland

APN	internet.eplus.de
User name	eplus
Password	gprs

### Sipgate (e.g. VoIP)

APN	Internet
User name	sipgate
Password	sipgate

### Customer service and support

#### End consumer

Please consult your dealer or installer if you have any questions.

#### Dealer/installer

In case of questions, please contact the appropriate support hotline.

Consult our website for product information.

ABUS Security-Center GmbH & Co. KG

86444 Affing

Linker Kreuthweg 5

GERMANY

[www.abus.com](http://www.abus.com)

[info@abus-sc.com](mailto:info@abus-sc.com)



## Decommissioning the alarm panel

- Select:  
*Menu -> Installer mode*
- Open the alarm panel
- Remove the backup battery or batteries
- Remove the power supply, the mains connection or the external PSU
- Remove the installation and dismount the alarm panel

## Data protection



### Danger



### Note

**When passing on the alarm panel, sending it in for repair or decommissioning it, please note that the folders**

**CONFIG**

**and**

**IMG\_X**

**on the SD card must be deleted.**

**or the SD card must be removed.**

**The SD card may contain important information about the user and their property.**

The folder

### **CONFIG**

contains the configuration of the alarm panel when backing up via the GUI.

The configuration includes, for example:

- the access data (password) to the ABUS server
- the access data (password) to the e-mail account
- the access data (password) to VoIP
- the access data (password) to the cameras
- the directory contact details

The folder

### **IMG\_X**

contains the images of the camera TVIP41550.

These are private images corresponding to the installation location of the camera.

### Disposal



Dispose of the device and the batteries in accordance with EU Directive 2012/19/EU – WEEE (Waste Electrical and Electronic Equipment). If you have any questions, please contact the municipal authority responsible for disposal. Information on collection points for waste equipment can be obtained from your local authority, from local waste disposal companies or your retailer, for example.

Dispose of the packaging material in accordance with local regulations.

## Index

- 2014/53/EU 3, 15
- ABUS Security-Center GmbH & Co. KG 8, 424
- Access level 1-4 35, 349
- Acoustic signal tones 342
- Activated 123
- Active intrusion protection 21
- Administrator names 10
- Alarm panel 21, 50
- Alarm panel error and tamper monitoring 36
- Alarm system 21
- Alarm type 21
- Alarm zone 21
- Alarming
  - External 24
- ARC reporting 210
- ARC/ESCC reporting 360
- ARC/ESCC reporting protocol formats 360
- Arm 31
- Arm components 31
- Arming, disarming 21
- Battery warning notes 13
- bidirectional 2-way wireless 22
- burglar alarm system 24
- Burglar alarm system 24
- Button
  - Log in 47
- Certifications 35
- CID codes 365, 367
- CID report groups 365, 367
- CID/SIA Events 364
- Cleaning mode 277
- CME / CMS Error messages 380
- Code reset PINs 19, 149, 153
- Coding of wireless signals 23
- Combination outputs 120
- Combination signalling device 28
- Communication 55, 196
- Communication options 261
- Communication options 28
- Compatible equipment 312
- Components 63
- Components 28
- configuration 30
  - Secvest 8
- Configuring
  - Peripheral devices for the wireless alarm system 8
- Conformity 310
- Connecting
  - components 40
- Connections 15
- Contact ID 360
- Contents 4
- Control elements 46
- Control panel
  - Arm button 17
  - Disarm button 17
  - Proximity reader 17
- Customer service and support 416
- Customisation 61
- danger alarm system 25
- Danger alarm system 25
- Danger detector 21
- Data communication mobile 415
- Data protection 417
- DC-09 362
- Declaration of conformity 3
- Decommissioning 417
- Default settings 148
- DEOL 24
- Detectors 67
- Device front 17
- Device overview 17
- DHCP 23, 198
- Diagnostic LEDs 403
- Disarm 31
- Display 23
- Disposal 418
- Door locks 96
- Double end of line 24
- Email 253
- Email error messages 376
- Email notification 412
- Email Setup 412
- Emergency call 229, 272
- EN50131-3 Section 9.1 gg 45, 321
- EN50131-3 Section 9.1 hh 45, 321
- EN50131-3 Section 9.1 jj 321
- EN50131-3 Section 9.1 m 45, 321

- EN50131-3 Section 9.1 p 16
- EN50131-3 Section 9.1 x 45, 123, 132
- EN50131-3 Section 9.1 y 45, 123, 132
- ESCC/ARC reporting 360
- ESCC/ARC reporting protocol formats 360
- Ethernet 57
- EU 3
- EU Directives 310
- Factory reset 42
- Factory settings 42, 150
- Factory settings staggered 149
- false alarm 11
- Fast Format 360
- Firewall 408
- Flood detector 35
- Function test
  - Secvest 8
- Glass breakage detectors 22, 25
- GMT 363, 409
- GSM CME / CMS Error messages 380
- GSM test call 402
- GUI 25
- handover log 8
- Housing tamper switch 40
- HW default values 320
- HW factory defaults 320
- Hybrid module 60
- Hybrid module 102
- Hybrid Module 26
- Hybrid module outputs 117
- Hybrid module zones 82
- IAD 408
- Index 419
- Individual identification 24
- Indoor sounder 89
- INFO 50
- Info bar 46
- Information module 92
- Initial start-up 42
- Input field
  - Password 47
  - User name 47
- Installation 26
  - Peripheral devices for the wireless alarm system 8
  - Secvest 8
  - Wireless alarm system 8
- Installer names 10
- Installing a wireless mobile module 40
- Intended use 9
- Interference filter, noise filter, interference suppression filter 11
- Interior protection 26
- Internal alarm 26
- Intuitive operation 27
- IP Mobile Setup 415
- IP zones 67
- key assignment 18
- Keypad front 41
- Level 1-4 28, 35, 349
- Limitation of liability 2
- Local alarm 28
- Log 294, 384
- Log book entries 384
- Log in
  - on the Secvest 43
- Logging in/out 8
- Logging out
  - from the Secvest 44
- login button 46
- Login screen 43, 47
- MAC address 57
- main menus 46
- Medical emergency 29
- micro SD card 41
- Mobile 58
- Mobile data communication 415
- Mobile test call 402
- Motion detectors 22
- mounting location 15
- Mounting plate
  - wall mount, wall bracket, wall arm, wall hanger, wall fixing, wall fastening 39
- notification centre 410, 411
- online help 46
- Opening detector 30
- Outputs 106
- Packaging 16
- Panic response: 145
- Part set 132
- Partition selection 62
- Partitions 33, 122
- Password 43, 47
- Perimeter protection 22
- Perimeter surveillance 30

- Power supply
  - Dangers 11
- Processing priority 16
- Protected outdoor area 25
- Prox Tag 23
  - Proximity switch 23
- Proximity reader 17
- PSTN 56
- PSU 11, 39
- Quickstart guide 8
- RC 31
- Reboot 399
- Recording communication sequences 405
- RED 3, 15
- Relay outputs 31
- Remote access 25
- remote configuration 25
- Repairs and maintenance 344
- Repeater 98
- Reset code PINs 19, 149, 153
- Restore defaults 148
- RF repeater 98
- Rolling Code 31
- Router 408
- S/W upgrade 345
- Sabotage 31, 33
- Saving the settings 44
- Scope of delivery 16
- SD card 41
- Security 9
- Security frequency band 32
- Security system access data 10
- Secvest
  - Arm/disarm 8
  - Arming/disarming 8
  - mounting location 15
- Seismic sensor 32
- shock detector 24
- SIA 361
- SIA codes 370, 373
- SIA report groups 370, 373
- SIA/CID Events 364
- Silent alarm 33
- Sirens – external sirens 22, 87
- Sirens – indoor sirens 26, 92
- Smoke alarm 31
- SMS 240
- SMS service centre 411
- SMSC 410, 411
- Sounder 21, 32
- Sounder - indoor 89
- SSL notifications 377
- Standard administrator code 10
- Standard installer code 10
- Standards 310
- Start Wizard 341
- Status 32, 62
- Status display 62
- Status feedback 32
- Status query 33
- submenus 46
- SW default values 321
- SW factory defaults 321
- symbols 9
- System 147
- Tamper 31
- tamper protection 31
- TCP/IP error messages 377
- Technical damage 33
- Technical data 298
- Telephone dialler 16, 33
- Terms and definitions 21
- Test 273
- Time conditions 36
- Time schedules active/inactive: 45, 123, 132
- Time zones 409
- Touch front 41
- Trace 405
- Troubleshooting 399
- User 22
  - Installer 43, 47
  - Logging in/out 8
- User guidance 22
- User numbers 397
- UTC 363, 409
- VdS 111
- Virtual keypad 297
- Voice dialler 32, 233
- VoIP error messages 379
- WAM 94
- Warning notice
  - Danger 9
  - Important 9
  - Note 9

## Index

---

- Warranty 3
- WBI 35
- wired alarm zone 24
- wired detector 24
- wired detectors 24
- Wired outputs 115
- wired zone 24
- Wired zones 81
- Wireless alarm system** 25
- wireless alarm zone 24, 25
- Wireless control panel 85
- Wireless control panel 25
- Wireless detector 25
- Wireless key switch 25
- Wireless mobile phone network 411
- Wireless operation 15
  - R&TTE certification 15
  - Wireless licence 15
- Wireless outputs 107
- Wireless range 25
- Wireless Remote Control 25
- Wireless window lock 25
- wireless zone 25
- Wireless zones 79
- Wizard, Start Wizard 341
- Zone 35



# **ABUS wireless alarm system**

Secvest

V3.01.17

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