



Security Tech Germany

SECVEST USER GUIDE

V3.01.11



CONTENTS

English

1. Scope of delivery.....	4
2. General	5
2.1 Safety information	5
2.2 Information on user guide	6
2.3 Warranty	6
2.4 Disposal	6
2.5 Declaration of conformity.....	6
3. Installation example.....	8
4. Overview of the system and control panel	9
5. Overview of the numerical keypad	10
6. Secvest display.....	12
7. Menu navigation and operation	13
8. Arming and disarming the system	13
8.1 Arming/disarming keys	13
8.2 Graphical display of arming/disarming on the display	14
8.3 Arming/disarming via the quick arm keys	14
8.4 Arming via the user code.....	14
8.5 Arming sub-areas	16
8.6 Individual sub-areas	17
8.7 Internal arming.....	17
8.8 Internal arming via chip key	18
8.9 Internal arming via remote control	18
8.10 Arming via wireless control panel.....	18
8.11 Arming via remote control.....	18
8.12 Arming via chip key	19
8.13 Arming via delay times.....	19
8.14 Preventing arming of the system	20
9. Responding to an alarm	21
9.1 Alarm types.....	21
9.2 Alarm forwarding.....	22
9.2.1 Alarm forwarding via telephone	22
9.2.2 Alarm forwarding to a monitoring station	23
9.2.3 Alarm forwarding via email.....	23
9.2.4 Alarm forwarding via text message	23
9.2.5 Alarm forwarding in the event of a personal or medical emergency	23
10. User menu	24
10.1 Users.....	26
10.2 Voice memo	27
10.3 Hide zones.....	27
10.5 System configuration	28
10.5.1 Functions.....	28

10.5.2 Date & time	33
10.5.3 Edit outputs.....	34
10.5.4 Remote controls.....	35
10.5.5 Volume settings	35
10.5.6 Web access	35
10.5.7 Remote updates.....	36
10.5.8 Time schedules active/inactive	36
10.6 Contacts	36
10.7 Test.....	38
10.7.1 Walk test	38
10.7.2 Sirens & sounders	39
10.7.3 Door locks	39
10.7.4 Outputs	39
10.7.5 Chip key	39
10.7.6 Remote controls	40
10.7.7 Emergency buttons.....	40
10.7.8 Telephone call	40
10.8 Log	40
10.9 Information	41
10.9.1 Alarm panel	41
10.9.2 Communication	42
11. Advanced system operation	44
11.1 Remote control	44
11.2 Wireless cylinder lock ("Secvest key")	44
11.3 Additional door lock (FU7010/7025E)	44
11.4 Operation via telephone.....	45
12. Operation via web (app/browser).....	46
12.1 Operation via web browser	46
12.2 Operation via app.....	46
13. Operation via web browser.....	47
13.1 Setting the Secvest IP address	48
13.2 Overview of the web interface	48
13.3 Arming & disarming.....	49
13.3.1 Hide zones	50
13.4 Additional web interface options.....	51
13.5 Configuring Secvest "time schedules"	54
13.6 Datasets.....	57
13.7 Exceptions	57
14. Terms and definitions.....	60
15. Technical data.....	67
16. Troubleshooting	80



For trouble free and safe operation, this device must be installed and regularly maintained by a specialist trained by us. Arrange regular maintenance appointments with your installer to ensure trouble-free operation over the long term with the latest safety updates and new functions.

Dear Customer,

Thank you for purchasing this SECVEST wireless alarm panel. This device is built with state-of-the-art technology and it complies with current domestic and European regulations. Conformity has been proven, and all related certifications are available from the manufacturer on request (www.abus.com). To guarantee safe operation, it is essential that you observe the instructions in this user guide. If you have any questions, please contact your specialist dealer.

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 resulting damage. No part of the product may be changed or modified in any way. If you do not follow these instructions, your warranty claim becomes invalid. Subject to technical modifications.

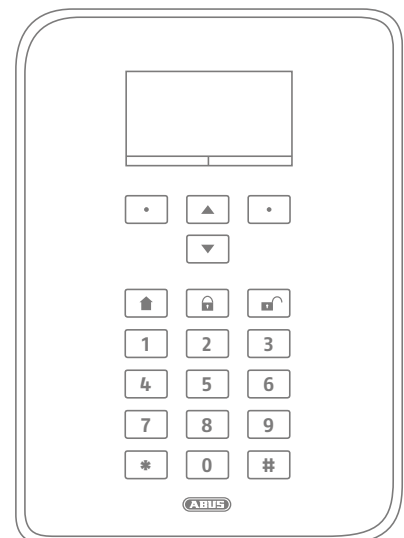
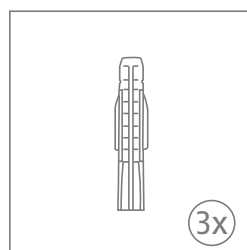
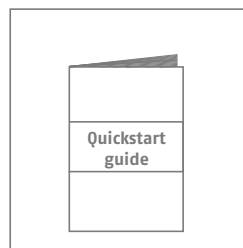
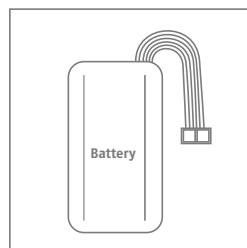
© ABUS Security-Center GmbH & Co. KG, 11/2018.

We reserve the right to make changes to this manual without prior notice. This wireless alarm panel is suitable for use in combination with detectors and sounders for the protection of property, such as your company, home, garage, garden shed and holiday home.

1. SCOPE OF DELIVERY

The following components are included in the scope of delivery for your new Secvest product:

- Wireless alarm panel
- Rechargeable battery
- Quickstart guide
- Mounting material
3 x screws
3 x screw anchors



2. GENERAL

2.1 Safety information

The alarm panel and its connected components must not under any circumstances come into contact with water, such as in the bathroom. 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. The power supply unit is suitable for operation on the public electrical grid with 230 V AC/50 Hz. No part of the product may be changed or modified in any way. 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. Only use the device for the purpose for which it was built and designed. Any other use is considered unintended.

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.

2.2 Information on user guide

These instructions contain important installation and operation information. Follow the directions and instructions in this user manual to ensure safe operation. Store this manual in a safe place for future reference. This manual constitutes part of the device. If you pass the device on to third parties, please remember to include this manual.



Note

S/W 3.01.11

This manual relates to software version 3.01.11 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. $< 2.00.00$.

2.3 Warranty

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. If you discover a defect on your wireless alarm panel which existed at the time of purchase, contact your dealer directly within the first two years.

2.4 Disposal

Dispose of the device in accordance with EU Directive 2002/96/EC – WEEE (Waste Electrical and Electronic Equipment). If you have any questions, please contact the municipal authority responsible for disposal. You can get information on collection points for waste equipment from your local authority, from local waste disposal companies or your dealer, for example.

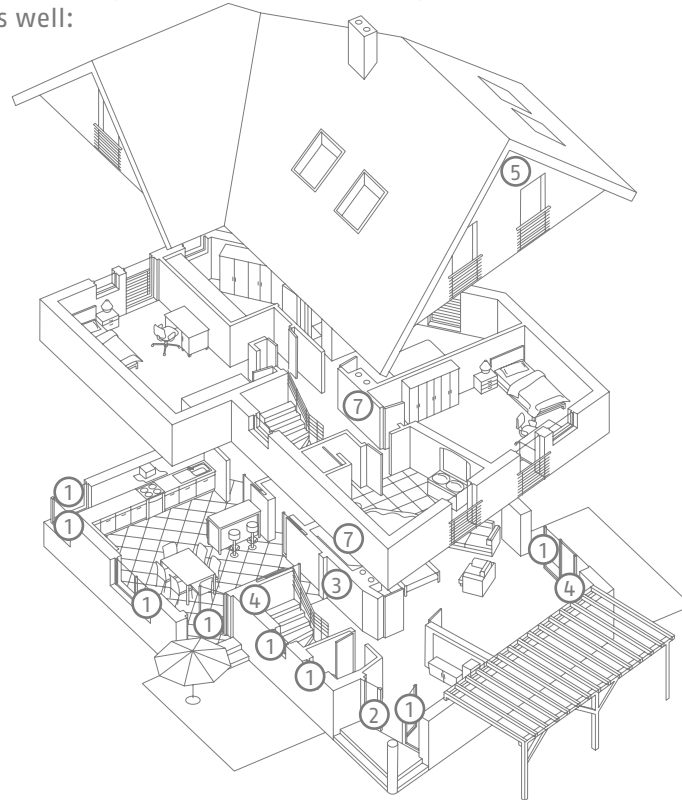
2.5 Declaration of conformity

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 Artikelsuche 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

3. INSTALLATION EXAMPLE

The following provides a simple installation example to show some important basic applications for the alarm system. The example focuses on a single-family detached home. A representative installation has been illustrated here, as an example of how it could be implemented in a similar or more advanced form for your property as well:



The following components are installed in this example:

- ① 8 x magnetic contacts at the windows and doors

- ② 1 x Secvest key (wireless cylinder lock) at the doors for easy arming/disarming

- ③ 1 x Secvest alarm panel

- ④ 2 x motion detectors indoors

- ⑤ 1 x wireless outdoor siren under the roof

- ⑥ 1 x wireless control panel in the bedroom

- ⑦ 1 x info module in the hallway

Perimeter protection: Protects against all possibility of access from outside (windows, doors, etc.). An alarm is triggered as soon as someone gains access to the property.

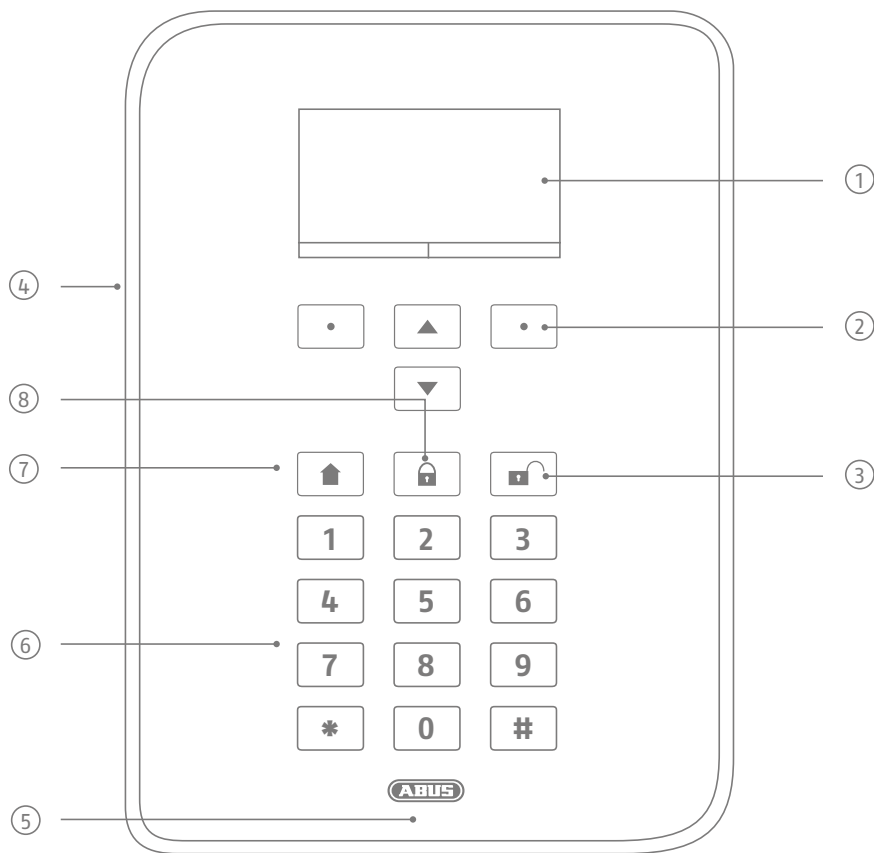
Interior protection: Predominantly used as a second line of defence, armed when the occupants of the building are away so that the perimeter protection acts as the first alarm and the interior protection as additional security against intruders.

Internal arming: If you are in the building you can arm just the detectors for the perimeter protection. The motion detectors indoors remain disabled in this case.

External arming: All available detectors on the premises are enabled.

An overview of **all** important terms concerning the alarm panel and alarm system can be found in the appendix under "Terms and definitions".

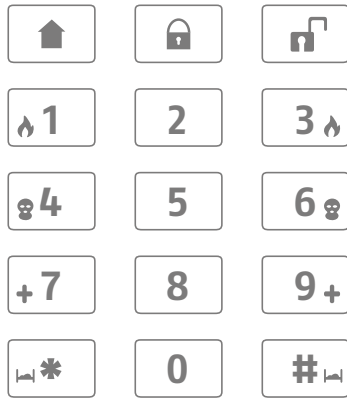
4. OVERVIEW OF THE SYSTEM AND CONTROL PANEL



- ① Graphical display for status, menus and additional information
- ② Keys for menu navigation (see "Menu navigation")
- ③ Quick disarm key for disarming the complete system (code entry required)
- ④ Microphone opening
- ⑤ Proximity chip key reader area
- ⑥ Numerical keypad (see following page)
- ⑦ "Internal arm" key for quick arming of perimeter protection
- ⑧ Quick arm key for arming the complete system

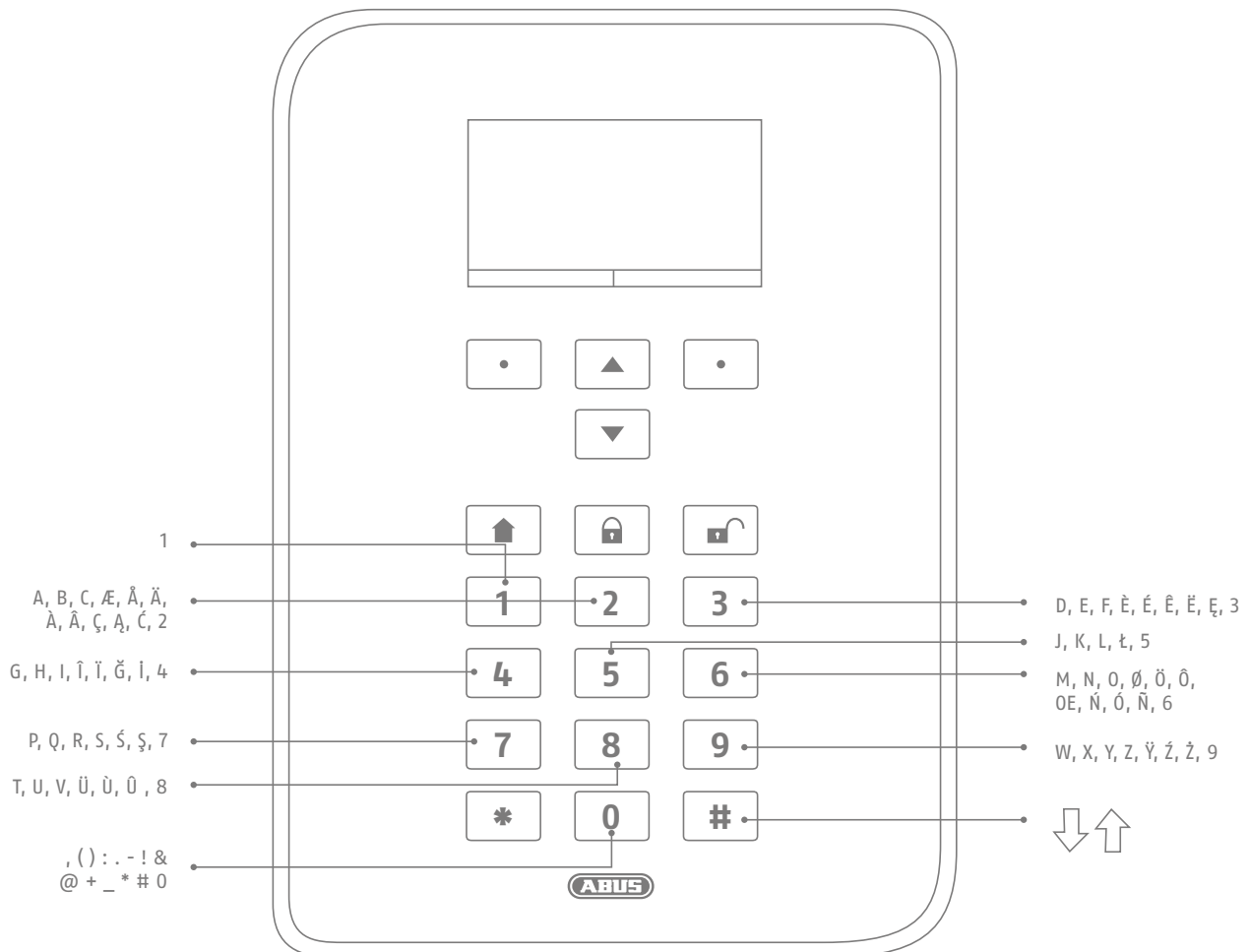
5. OVERVIEW OF THE NUMERICAL KEYPAD

The numerical keypad is used to enter values in certain menus. Letters and special characters are also stored on the keypad for entering things like user names or email addresses.



The numerical keypad can be used to input various information. For example, a name can be entered when creating a new user (see "Users"). The letters are not printed on the numerical keypad in order to provide a better overview during day-to-day operation. Letters are entered according to the legend provided below.

In addition to data input, numerical keys 1/3, 4/6, 7/9 and the */# keys are used for quick arming. If the quick arming function using key combinations is enabled (ask your specialist installation contractor), both keys of each key pair must be pressed at the same time. The following alarm options are available:



Fire alarm

Press both fire alarm keys at the same time to manually trigger a fire alarm (for example, if you notice a fire and wish to warn others in the household). The system beeps twice in cycles as a way of providing acoustic feedback.

Panic alarm

Press both panic keys to trigger a manual panic alarm (for example, if an intruder enters the property while you are at home). When the keys are pressed, either an acoustic alarm sounds (tone like for an intruder alarm) or a silent alarm is triggered, depending on your agreement with the specialist installation contractor. A silent alarm is transmitted to a monitoring station via the integrated dialler, for example.

Medical emergency call

Press both of these keys to trigger a medical emergency call. If there is a potential medical problem (such as a sudden feeling of faintness) this call sends a message to a rescue coordination centre specialised in handling medical emergencies.

Emergency call

If a vulnerable person resides in your home and requires help, this key combination triggers a related emergency call. In this case a rhythmic beep sounds from the alarm panel so that other people in the home are informed that there is a problem.

These and other functions must be set up by a specialist installation contractor as required. The alarms listed above must be configured by the specialist installation contractor as required when the alarm panel is installed.

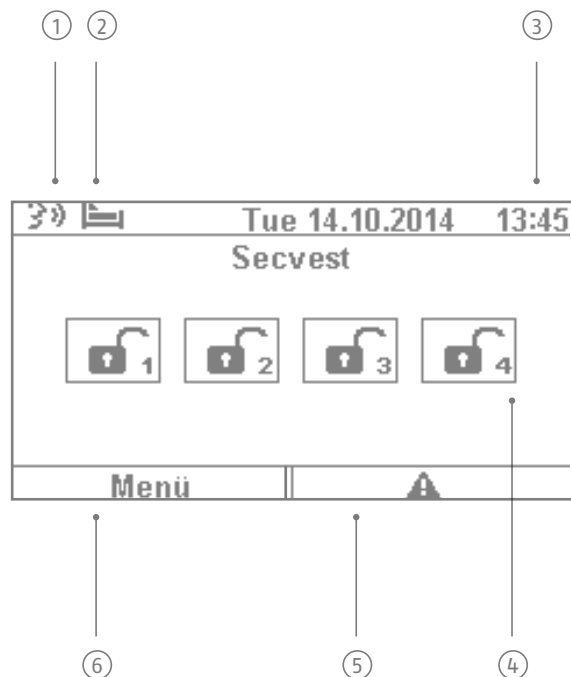
Note:

You are using the touch-front. The backlighting is set to "WHEN active" and the backlighting is dark.

The illumination is first turned on when a button is pressed (first touch). No other action results from a "first touch". From the second touch on, the keypad functions as normal.

For details, see section 10.5.1 Functions- Backlighting

6. SECVEST DISPLAY



① Voice message This symbol is displayed when a voice message has been recorded (for example, a reminder from another user). After the alarm panel has been disarmed the user receives the following audio message: "You have a message". The message can then be played back and deleted if desired.

② Symbol for activity monitoring. This symbol is only displayed when activity monitoring is active. This function is used for monitoring vulnerable persons and must be configured by the specialist installation contractor.

③ Display of time and date

④ Display of the status of up to 4 sub-areas: open padlock = system disarmed, closed padlock = system armed, house = internal arming active

Error symbol: indicates an alarm, reset, fault etc.

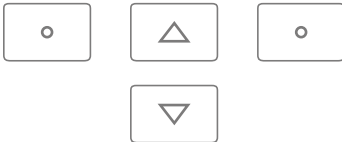
Note:

⑤ 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.



⑥ Menu symbol: used to access the user menu

7. MENU NAVIGATION AND OPERATION





Cursor control



The Secvest menu is mainly navigated using the cursor keys located below the display:

-  These keys are used to scroll through the menus and activate specific scenarios when the system is being armed, amongst other functions. More information is provided in the next chapter, "Arming and disarming the system".
- 

A manual restart is initiated when the "upward" and "downward" navigation keys are simultaneously pressed for more than five seconds. For details, see section 16.1 Manual restart

-  These keys are used to select menus or symbols, change values and also exit the menus again. The function of both keys adapts dynamically to the text shown on the display. If, for example, "Menu" is shown on the left side of the display, press the  key below and enter your user code. This brings you to the user menu which you can exit again by pressing the  key.
- 

The cleaning mode is started when the left and right navigation keys are pressed simultaneously. For details, see section 10.5.1 Functions - Cleaning mode

Note:


It is not possible to use the alarm panel during cleaning; this is especially true for the double key functionality (fire, intrusion, medical emergency, care).



8. ARMING AND DISARMING THE SYSTEM

8.1 Arm/disarm keys



The arm/disarm keys for the alarm panel are located below the cursor field. These keys can be used to quickly and conveniently arm or disarm the alarm panel. Additional arming options are covered in detail below. In the standard configuration, Secvest is armed on a time delay, meaning it is only armed after the exit delay programmed by your specialist installation contractor has expired.

-  This key is used to start "internal arming". Only the detectors for "perimeter protection" are activated, so that you are still able to move around the building freely (even if there are motion detectors installed indoors, for example).

-  This key is used to quickly arm the complete system. No user code is required for this. Note that when this key is pressed ALL detectors including those in all sub-areas (if there are any) are activated. This function will only work if the key has been enabled in consultation with your specialist installation contractor. This key has no function if it has not been enabled beforehand. If necessary speak to your installation contractor if this key function is required.
-  This key is used to disarm the system again. After the disarm key is pressed you must enter a valid user code. The complete system is then disarmed (including all sub-areas).

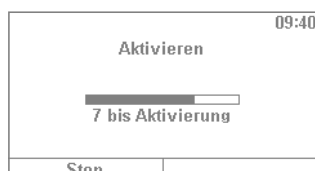
8.2 Graphical display of arming/disarming on the display


This section contains information on how the arming or disarming of the alarm panel is shown on the display. This assumes that your system has been configured with just one partition. All detectors are therefore assigned to partition 1. In this case partition 1 is the entire premises.

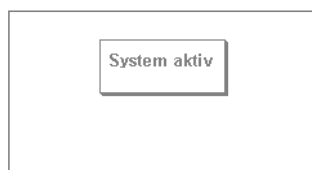
8.3 Arming/disarming via the quick arm keys




1. If the system is disarmed, the display responds as follows: The open padlock symbol indicates the disarmed status of the alarm panel.



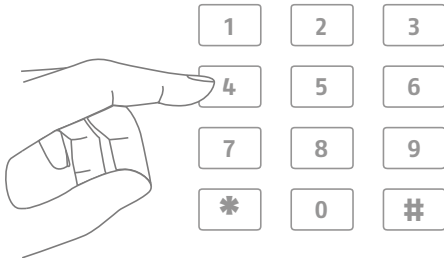
2. If the  key is then pressed, the system is completely armed. As mentioned previously, the system is armed only once the delay time has expired as programmed by your installation contractor.



3. You should leave the premises within this time delay. The closed padlock symbol then indicates the armed status of the alarm panel. To disarm the alarm panel again, simply press the  key and enter a valid user code. The system is then disarmed with the audio message, "The alarm system is disarmed" and the open padlock symbol visually indicates this status.

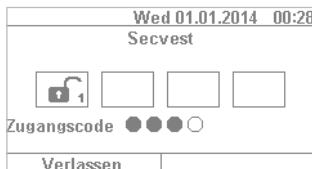
This method of arming the system as described here using the quick arm keys is one of the fastest and provides a representative example of how system arming works in general. The next section provides information on other ways to arm the system. Not all of these options may be available, as they depend on the configuration of your system by the specialist installation contractor. If necessary speak to your installation contractor if you desire a specific method of arming your system.

8.4 Arming via the user code

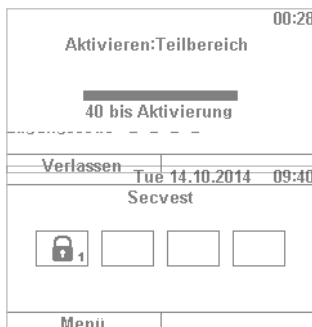


The system can be armed by directly entering a user code. The system has either been configured with a 4 or 6-digit user code in consultation with your specialist installation contractor.

This code should be changed during commissioning, however. If a new user is added, a separate code is created for this user. Every user should take note of their individual codes.



1. To arm the system, simply enter a user code. Please note that the "menu" key is not pressed before entering this code. Otherwise you will be directed to the user menu, from which you cannot arm the system.



2. After the code is entered the "delay time" starts (in the standard configuration of the system). You should leave the building within this time delay. For this reason, ensure that sufficient time is planned to exit the building. If, for example, 35 s has already passed and you still have to get out the door, there is not enough time. A false alarm may be triggered, as the opening and closing of the door takes a bit of time in itself.

3. If the delay time has expired, the system is armed: you have now successfully armed partition 1 and can disarm it again by entering a user code.

If a window is still open, for example, when the alarm panel is armed, an error message is displayed. Correct the error (close the window) and then rearm the alarm panel. If the error cannot be corrected, you can arm the alarm panel anyway by pressing the "Lock all" key. In this case the alarm panel is armed with "hidden zones". This means that all open detectors or detectors with faults are ignored during monitoring. These detectors will not trigger an alarm in this case!

These zones only remain hidden until the next time the system is armed.

8.5 Arming sub-areas

In addition to the option of arming a partition via a user code, the system can also arm additional sub-areas. The procedure for this is given here using the user code entry example. This function must be preconfigured by your specialist installation contractor.

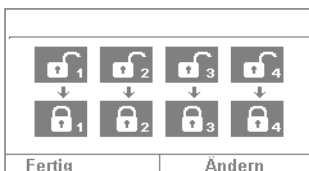
After entering the user code, you are asked to confirm which partition(s) you wish to arm. Alternatively you can also arm the complete system when, for example, you plan on leaving the premises.



1. In our example, the alarm panel is divided into 4 sub-areas. These are displayed as disarmed by the open padlock symbol. First enter your user code as usual.



2. Once the user code has been entered, the menu changes as follows:

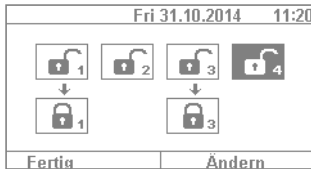



3. Select "Change" and the display changes as shown in the figure on the left. Click "Done" to arm all sub-areas. The system is now completely armed.



4. If you only wish to arm certain sub-areas, click on "Change" and use the key to navigate through the four sub-areas until the partition you wish to arm is selected. Click on "Done" to arm the selected partition. Repeat the same procedure to arm other sub-areas.

8.6 Individual sub-areas



1. If you wish to arm two sub-areas, proceed as follows: enter your user code. Using the  arrow keys, select the two sub-areas to be armed. The selections are visually highlighted. Set the selected sub-areas to the open padlock symbol via the "Change" function. Leave the sub-areas you do not wish to arm "empty". In this case the menu looks like the example given in the figure on the left.



2. Click on "Done" and system sub-areas 1 & 3 are armed, while sub-areas 2 & 4 remain disarmed. After the arming time, the Secvest display then looks like the example given in the figure on the left.

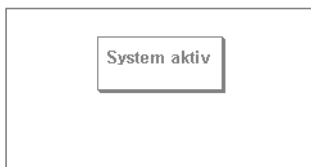


3. To arm only partition 2, repeat the steps as described above. Select the individual sub-areas, click on "Change" and set the value for the partition to "empty" as shown in the figure. The partition to be armed (partition 2 in this case) should be set to "active" using the "Change" function. Click on "Done" to arm just this partition.


8.7 Internal arming

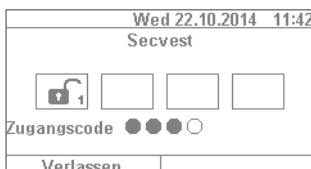
In addition to the option of arming the complete system and sub-areas, the system also offers the option of "internal arming". This type of arming is preferred when occupants are home and wish to arm just the perimeter of the premises. Certain detectors indoors (such as motion detectors) are disabled so that occupants can move freely within the building. A practical example here is application in a private home.

The following options are available for internal arming:




Option 1:

Press the  key to internally arm the system with just one touch. The quick arm option must be enabled in advance by the specialist installation contractor.



Option 2:

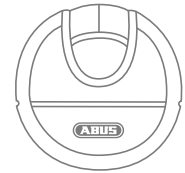
Enter a user code to arm the system. Click and hold "Change" until the house symbol  appears. Click on "Done" and the system is "internally armed".



You can now move freely around the house even though motion detectors may be installed. The perimeter of the premises is armed, so that an intruder attempting to break in from outside triggers an alarm.

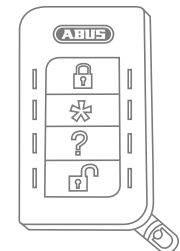
8.8 Internal arming via chip key

The procedure for internal arming via the chip key is virtually the same as arming the complete system: Hold the chip key in close proximity to the ABUS logo and swipe it over the logo briefly. A prompt appears, requesting confirmation on the type of arming required. Click on "Change" as usual and select the house symbol. Click on "Done" to arm the system internally.



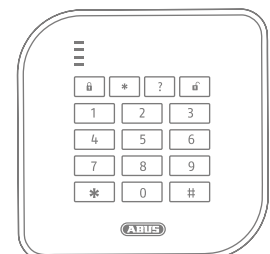
8.9 Internal arming via remote control

On the remote control, the * key is assigned the "internal arm" function as standard. This symbol is on key 2 of the remote control. Press the key and the system is internally armed. Visual feedback is provided next to the * symbol: brief flashing (green) for sending the signal, then flashing (red) to indicate successful internal arming.



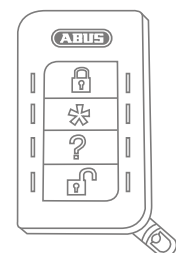
8.10 Arming via wireless control panel

An additional way of arming the system is provided via the optional wireless control panel. This arming/disarming option is as similar as possible to the other system options. Only the operation method is different, as the wireless control panel does not have a display. Please read the individual operation options in the user manual for the wireless control panel.



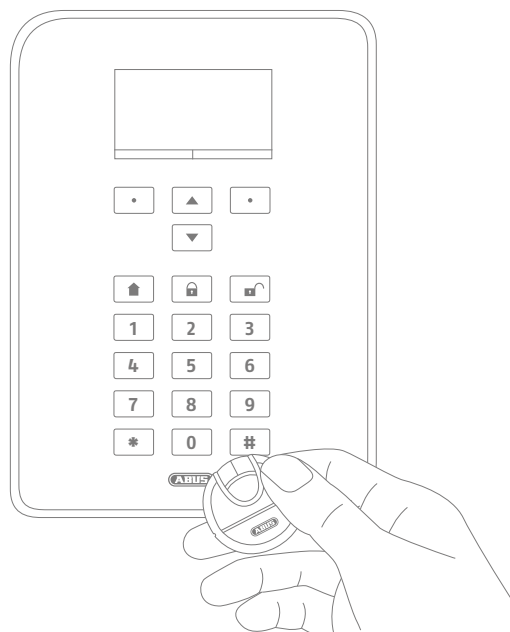
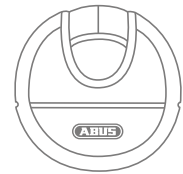
8.11 Arming via remote control

If there is a remote control, you can press the corresponding keys to arm/disarm the system (all sub-areas are armed/disarmed simultaneously) and internally arm the system if you as the user are authorised to do so. You can also check the status of the system. The remote control provides visual system feedback for all entries ("2WAY function"). For a detailed explanation of the individual functions of your remote control, please read the user guide for the remote control.



8.12 Arming via chip key

The chip key can be used to completely arm and disarm the wireless alarm panel (or a partition, if there are any) without touching the panel itself. The chip in principle eliminates the need to enter a code. If you as the user to whom the chip is assigned are authorised to arm or disarm multiple sub-areas, you must then decide which area to arm after you have swiped your chip key. The reader area for the chip key is located at the height of the ABUS logo. You only have to swipe the chip in the proximity of the reader area to arm the system – you do not have to touch the housing.



8.13 Arming via delay times

If you enter a code directly on the alarm panel (or via chip key or quick arm keys), the following "problem" occurs: You must still be able to leave the premises through the doors. If the system were automatically armed, you would not be able to leave the premises without triggering an alarm, if you have a magnetic contact on the doors, for example. For this reason there is a "delay time". The delay times are preconfigured by your specialist installation contractor.

There are generally two delay times:

- Exit delay
- Entry delay

The exit delay is set to 40 s as standard (the time can be adjusted by the specialist installation contractor according to your needs, however). Following the start of the exit delay, the premises must be left within this time.

Ensure that all windows and doors etc. are closed first before activation.

After the start, a continuous tone sounds.

Make your way out of the building and open and close the doors in time.

The continuous tone is replaced by a pulsed tone when the door is opened/closed. It will then return to a continuous tone.

The system also allows a special type of exit delay. The system is only armed once the doors are closed. The exit delay is therefore flexible to allow you to take whatever time you need to get out the door. Speak to your specialist installation contractor if you desire this type of arming.

Important: if the exit delay has expired and you are still inside the building, your movement, for example, will trigger an alarm if detected by a motion detector.

The entry delay gives you a sufficient timeframe to disarm the system after opening the doors when the system is armed. The entry delay should also be programmed in consultation with your specialist installation contractor. Ideally the entry delay should be as short as possible. If you enter your premises through the doors, you should hear a pulsed tone. As long as this tone sounds you have time to disarm the system. Disarm the system using your code (or chip key/disarm key).

Important: if the entry delay expires without the system being disarmed, an intruder alarm is triggered.

8.14 Preventing arming of the system

The alarm panel prevents arming in the following circumstances.

- Intrusion detectors (apart from the entrance) are open.

- Once they have been closed the arming procedure starts.

- A panic button or panic transmitter has been triggered.

- The system or a component or detector/zone is showing tampering.

- If communication or signalling devices have faults, this would prevent transmission of notifications.

- A supervision shutdown in a wireless component

The user can override permissible events (shutdowns).



9. RESPONDING TO AN ALARM

First of all: remain calm. An alarm does not always mean an intrusion. Sometimes an alarm is caused by something else, such as a self-triggered false alarm. For this reason, get a feel of the situation first and then respond accordingly in a composed manner. Disarm the system, check the reason for the alarm and then reset the alarm.

If an alarm is triggered, first disarm your alarm panel by entering a user code, for example. You will then be prompted to "reset" the alarm panel. This means that you must still "acknowledge" the alarm on the system in order for it to be ready for operation again.

The alarm is then shown on the display. "T2" means that an alarm has been triggered in partition 2. "Intrusion Z202 alarm" means that an intruder alarm has been triggered in "zone 202" in this partition. This "zone 02" is the second detector in the system, with the name "MC kitchen" (magnetic contact in kitchen). You can now go into the kitchen to see what exactly has happened near this detector.

Drücke Taste zum Rücksetzen	
T2:Einbruch Z202 Alarm	
MK Küche	
Verlassen	Rücksetzen

If the cause of the alarm is clarified and corrected, press "Reset". The system is then reset and ready to be armed again. Note that a reset is necessary. If this is ignored (e.g. if you press "Exit") the reset does not take place properly and appears automatically during the next arming process. If no entry is made, the graphical display disappears after 1 minute but remains on the system.

Important: occasionally you may find that an alarm cannot be reset. This may occur, for example, if the housing of your alarm panel and its components have been opened and a tampering alarm has been triggered. This can be corrected only by your specialist installation contractor.

9.1 Alarm types

An alarm can have various causes. The following alarms exist in principle:

- Tampering alarm
- Intruder alarm
- Panic alarm
- Technical alarm
- Fire alarm
- Emergency call or medical emergency alarm
- Entry delay exceeded
- Exit delay exceeded

The Secvest has four different types of alarm. Depending on the status of the system (disarmed, armed, internally armed), the following alarms are available (depending on the setup or programming of the alarm panel):

	Internal	Local	External	Silent
Alarm panel siren	✓	✓	✓	–
Indoor siren	✓	✓	✓	–
Outdoor siren	✓	✓	✓	–
Wireless control panel	✓	✓	✓	–
Information module	✓	✓	✓	–
Visual alarm, such as flashing light	✓	✓	✓	✓opt.
Diallers, such as monitoring station switching, text message, email, etc.	✓opt.	✓opt.	✓	✓
Relay	✓opt.	✓opt.	✓opt.	✓opt.

9.2 Alarm forwarding

If the communication interface of the Secvest has been programmed (speak to your specialist installation contractor), the following alarm forwarding options are available (depending on the configuration of your system and the connection used, such as IP, PSTN):

- Alarm forwarding via telephone (analogue or VoIP)
- Alarm forwarding to a monitoring station (MS)
- Alarm forwarding via email
- Alarm forwarding via text message
- Emergency call: emergency switching to medical services (e.g. Tunstall)

9.2.1 Alarm forwarding via telephone

With alarm forwarding via telephone you receive a telephone call and hear a message (recorded by you or the specialist installation contractor), for example: "Intruder alarm at bathroom window. Please arrange help." Proceed as follows:

1. The call occurs on the telephone and is displayed there like any other call.
2. Accept the call.
3. Listen to the entire message. The message is different depending on the cause of the alarm.
4. The recorded text is repeated three times. After the third time, the microphone on the alarm panel is enabled and you can listen to what is happening in the room. You also have the following key commands available (your telephone must be DTMF-compatible):

Telephone key (DTMF)	Meaning
Listen	1
Speak	2
Toggle between "Listen" and "Speak"	*
Playback messages	3
End call	5
End all calls	9

5. If you feel capable of resolving the problem yourself, acknowledge the alarm transmission by pressing 5 or 9. 5 means that the attempt to call you is stopped. Other contact numbers on the system may be called, however. 9 means that the attempt to make any calls is stopped. No other contacts are called.
6. If you cannot resolve the problem yourself, press 5 in any case. The alarm is forwarded to additional people.

You can “remotely control” the alarm panel via the telephone keypad (if this function is enabled). For more information, see "Advanced system operation".

9.2.2 Alarm forwarding to a monitoring station

If switching to a monitoring station is implemented, the monitoring station (MS) takes care of acknowledging the alarm transmission and coordinating help. Speak to your specialist installation contractor if you have questions about monitoring station switching.

9.2.3 Alarm forwarding via email

If the Secvest is connected to the internet (e.g. via a router), it can also forward an alarm via email. The alarm panel text (e.g. "Intrusion Z01 alarm") is sent to a predefined email address. If you are also using the Secvest PIR camera, the alarm image can also be attached to the email. Contact your specialist installation contractor if you wish to set up this function.

9.2.4 Alarm forwarding via text message

Similarly to email transmission, alarms can be forwarded via text message (for example, using the optional wireless mobile module).

9.2.5 Alarm forwarding in the event of a personal or medical emergency

If your household includes a vulnerable person, you can also set up forwarding for local alarms to a monitoring station specialised in handling medical emergencies. Speak to your specialist installation contractor about setting up this function.

The user menu helps you configure certain basic functions of the system. You can create and manage users, set the date and time and add and remove contacts.

10. USER MENU

10.1 Users

There are two different "levels" of the user menu. Log in as an "administrator" to delete other users, for example. Log in as a "normal user" to use the system with limited options in certain menus – you cannot edit or delete other users in this mode. Certain menus are not accessible for "normal users", such as "Contacts" and "Info". The administrator is in charge of managing these menus.

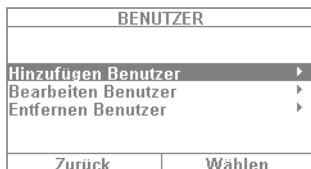
The following contains an overview of the structure of the user menu and the options provided by these menus when you are logged in as an administrator:



1. To log into the user menu, select "Menu" and enter an admin code. The first menu appears.



2. As a system administrator you can manage users and create new users. Log into the user menu with your admin code and go to the "Users" menu.



3. To add a new user, select "Add user". You are then guided through the setup options for a new user step by step.



4. User name: Using the Secvest keypad, enter the name of the user.



5. Select which user level the new user will have: **Normal user:** a normal user has limited options compared to an administrator. Normal users cannot create new users or edit existing users other than themselves, but they can change their own codes and assign remote controls, for example. **Administrator:** an administrator has advanced options in the user menu. Administrators can create new users and edit existing users. There are also more advanced options in other menus, such as in the system configuration. Usually one administrator per household is sufficient. If the premises involve a commercial property with multiple employees, for example, it may be a good idea to create additional administrators.

Benutzer 002	
Teilbereich	Ja
Teilbereich	Ja
Teilbereich	Ja
Teilbereich	Ja
Alle Teilbereiche	Ja
Fertig	Ändern

6. The next step involves assigning arming/disarming authorisation for sub-areas. Select "Done" if the user will be authorised for all 4 sub-areas. Otherwise make adjustments using the "Change" function.

Benutzer 002	
Neuen Code bestätigen ○○○○	
Zurück	

7. Assign an access code. This code should ideally be changed by the user themselves and kept safe by them. Ensure that the code is "secure". Code combinations such as "5678" are less secure than "2671", for example. For a higher degree of security, the system can be preconfigured to accept 6-digit codes. Speak to your specialist installation contractor if your system is configured for only 4-digit codes. A 4-digit code is created in this example. This code must be confirmed once after it is first entered. Alternatively you can also select "No code". In this case the user can only arm the system via chip key or remote control.

Benutzer 002	
Zugangscod zuweisen ○○○○	
Zurück	Kein Code

8. Additional components can be assigned to the new user. The first prompt is for a chip key. Take the chip and swipe it across the ABUS logo in close proximity to the housing. If no chip key is desired, select "No chip key".

Benutzer 002	
Zum Hinzufügen, Prox an die Zentrale halten	
Kein Chinschlüssel	

9. A remote control can then be assigned. Press any key of the remote control. If no remote control is desired, select "No remote control".

Benutzer 002	
Taste der FB drücken zum Identifizieren	
Keine Fernbedie...	

10. Nursing emergency call if your household includes a vulnerable person, you can give them a mobile emergency call button. This button is used to trigger an internal alarm quickly if the person needs help. Press the nursing emergency call button key once to assign it.

Benutzer 002	
Taste des Pflegenotruf- Senders drücken	
Kein Notruf-Sen...	

11. Panic alarm button: you can also use the emergency call button as a panic alarm button. Note that if the button is already being used as an emergency call button, it cannot also be used as a panic alarm button at the same time.

Benutzer 002	
Taste des Überfall- Senders drücken	
Kein UF-Sender	

12. Medical emergency call: you can also use the emergency call button/panic alarm button as a medical emergency call button. Note that if the button is already being used as a emergency call button or panic alarm button, it cannot also be used as a medical emergency call button at the same time.

Benutzer 002	
Taste des Medizinnotruf- Senders drücken	
Kein Notruf-Sen...	

13. The following confirmation then appears: "New user added". You can create additional users in the same way.

<div style="border: 1px solid black; padding: 5px; width: fit-content; margin: 0 auto;"> Neuer Benutzer hinzugefügt </div>	
--	--

Proceed as follows via the web interface:

Log in as an "administrator", click on "Users" on the right hand side and then click on "Add user".

You can now specify a name, type, code and partition.

Then login with the access details that have been set or the user details for this user and

add "Chip key", "Remote control", "Panic alarm", "Medical pendant" and "Care pendant".

Follow the instructions on the display.

10.1.1 Editing users

BENUTZER	
Hinzufügen Benutzer	▶
Bearbeiten Benutzer	▶
Entfernen Benutzer	▶
Zurück	Wählen

Here, the administrator can edit existing users.

Use the cursor keys to select the user to be edited. Then select "Edit user".

The administrator can only change the name, type and partition for other users.

The administrator can select and edit their own "Name", "Code", "Chip key", "Remote control", "Panic alarm", "Medical pendant" and "Care pendant".

10.1.2 Removing users

BENUTZER	
Hinzufügen Benutzer	▶
Bearbeiten Benutzer	▶
Entfernen Benutzer	▶
Zurück	Wählen

To remove users (such as an employee who has since stopped working at the premises), select the user in question and remove them from the system. All components assigned to this user, such as remote controls, are automatically deleted.

10.1.3 Creating a user "threat code"

Hinzufügen Benutzer	
Name :	abc
Überfall	
Entfernen	OK

In addition to the user levels of "normal user" and "administrator" you also have the option of creating a "threat code". This code is used to seemingly disarm the system during a hold-up when the intruder is watching. A silent alarm is still triggered in the background, however. For this function to be enabled, an appropriate communication interface (e.g. telephone or monitoring station switching) must be set up. The steps for setting up a threat code user are the same as those for setting up any other user. Proceed as follows:

Überfall	
Normaler Benutzer	
Administrator	
Bedrohungscode Benutzer	
Zurück	Wählen

User menu -> Add user -> Name -> "Threat code user". Create a code for this user. This code should be known to all users of the alarm panel. Then if an intruder enters the premises and forces you to disarm the alarm panel, simply enter this "threat code". The system appears to disarm as normal. The silent alarm is triggered via telephone switching, however.

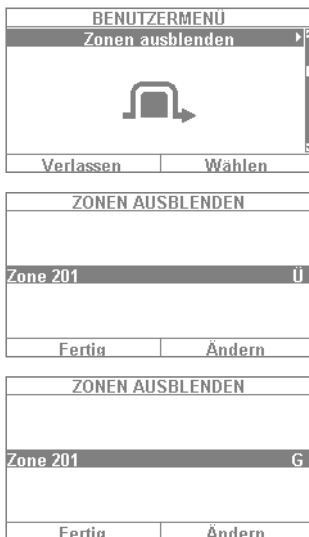
Important: Your specialist installation contractor must enable the function beforehand to make the "User threat code" option appear in the user menu. If in doubt contact your specialist installation contractor if this option does not appear in the menu.

10.2 Voice memo



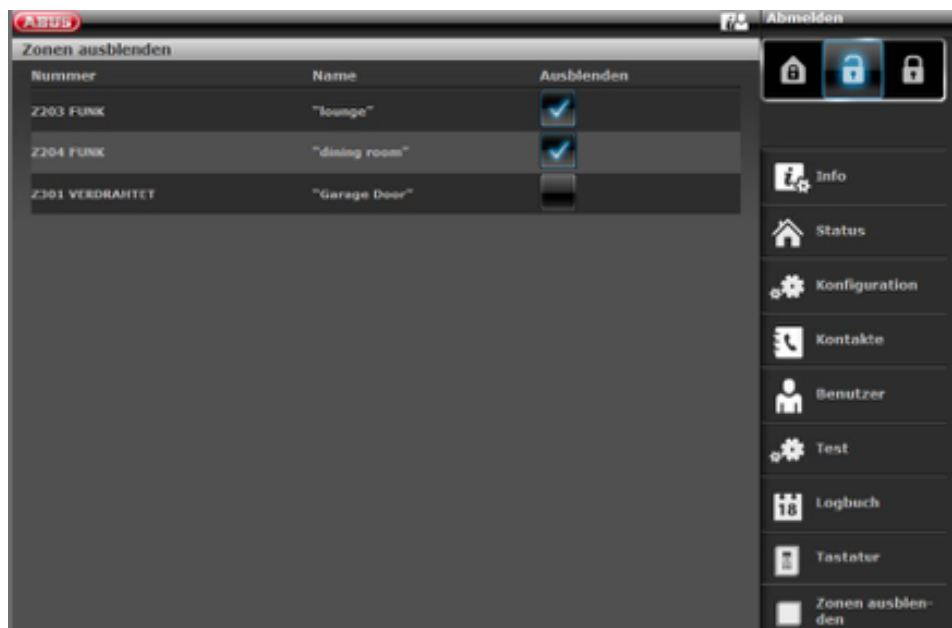
This function is used to leave someone else a message ("Memo function"). Record a short reminder, for example, and then arm the system. The next person to disarm the system is notified with the text "You have a message" and a corresponding symbol. Select "Recording" to record a 30-second message and then save it. Any user can delete this message after it has been played back. This function can be completely disabled in consultation with the specialist installation contractor.

10.3 Hiding zones



It may occasionally be necessary to exclude a detector (also called a "zone") from monitoring, for example if a detector is faulty or a zone cannot be closed for some reason. The system then indicates the detectors that can be hidden. The settings mean: Ü = monitored and G = locked (not monitored). Select the detector to be hidden and press "Change". Note that detectors to be hidden manually must first be configured for this function by the specialist installation contractor. For this reason not all of the detectors in the system may appear in the list of detectors which can be hidden if this has been set up that way beforehand. If detectors are hidden, they are no longer monitored when the alarm panel is armed. A hidden detector is "unhidden" the next time the system is disarmed and must be hidden again manually to be excluded from monitoring the next time the system is armed, if desired.

Using the web interface, it is also possible to hide zones. This requires selecting the "Hide zones" button, which will open a list of all the zones which can be hidden.



10.4 Outputs on/off

If your installer has configured the outputs as the "user defined" type, you can switch them on and off here.

10.5 System configuration



The following settings can be defined in the system configuration:

- On/off functions: settings for certain special functions such as door bell and voice messages.
- Date & time: setting for the date and time
- Remote controls: reprogramming of key assignments for remote controls
- Volume settings: setting for the volumes of different tones and messages
- Web access: activation/deactivation of web access
- Time schedules active/inactive: Configuration of time schedules for automatic arming/disarming

10.5.1 On/off functions

Select "Functions" to access the following options. These options will be clarified in the subsequent sections.



Key front menu	Touch front menu
Bell	Bell
Voice message	Voice message
Activity monitor	Activity monitor
Display contrast	Display contrast
Backlighting brightness	Backlighting brightness
Backlighting for menu keys	< hidden >
Backlighting for arm keys	< hidden >
Backlighting for number keys	< hidden >
Zone name announcement	Zone name announcement
Restart Panel Administrator only S/W >=1.01.00 hidden for normal users	Restart Panel Administrator only S/W >=1.01.00 hidden for normal users
Keypad tones	Keypad tones
< hidden >	Dynamic backlighting
< hidden >	Cleaning mode

Bell

If the "Door bell" property is configured for a detector (e.g. for a magnetic contact at the entrance of a business), the disarmed alarm panel triggers a tone similar to a door bell. This function must be configured by the specialist installation contractor. This indicates that someone has entered the business premises. If you wish to disable this function for a certain time period, it can be disabled here.

Voice message

In this menu you can disable the audible messages on the alarm panel (e.g. "Please note the message on the display").

Activity monitor

If the "Activity monitoring" property is configured for a detector (e.g. a motion detector in the hallway), the function of a motion detector can be "reversed". This function must be configured by the specialist installation contractor. If the function is reversed, an emergency call alarm is sent after a defined time period in which no movement has been detected. This function is used to monitor older, vulnerable members of the household. After a defined time period, an emergency call is sent when the regular "presence detection" at a previously designated motion detector has not triggered. This allows vulnerable members of the household who generally spend their time moving around a specific room to receive help quickly if their "presence" is not detected after a certain time due to a fainting spell or something similar.

Display contrast

Change the contrast of the Secvest display here.

Backlighting brightness

Change the display brightness setting. You can select "low", "medium" or "high".

LCD backlighting / backlighting

LCD backlighting

Only visible if the key front is installed. Here you can set the illumination of the display.

- **"Off"** turns the illumination off
- **"On"** web access enabled
- **"When active"** web access enabled

Backlighting

Only visible if the touch front is installed. Here you can set the illumination of the complete touch front. LCD backlighting, menu keys, arm keys and number keys

- **"On"** turns the illumination on in order to keep the complete touch front lit constantly.

Note: LCD backlighting and all backlighting of the keys are always turned on. The wakeup function is deactivated. In case of a power failure, the illumination switches to "When active" in order not to use unnecessary electricity from the battery.

- **"When active"** means that the illumination of the complete touch front only remains on for approx. 30 s after each use. It then turns off automatically.

Note: Wakeup function is activated. The illumination is first turned on when a button is pressed (first touch). **No other action** results from a "first touch". From the second touch on, the keypad functions as normal. The user can then touch one of the visible symbols (house/padlocks). **At the first touch**, the alarm panel will **not perform** the functions associated with these buttons. At first, only the illumination is turned on.

Backlighting for menu keys/backlighting for arm keys/backlighting for number keys

Only visible if the key front is installed. The same setup as for "LCD backlighting" applies here for the backlighting of the menu keys, arm/disarm keys and number keys. Set the desired lighting of the keys for menu navigation here.

Note: If the touch front is installed, these 3 menus are hidden.

Zone name announcement

Your detectors can be equipped with an additional audio message if desired. In consultation with your specialist installation contractor, the detectors are usually already given a name, for example "MC living room" for "magnetic contact in living room". This text can be recorded and saved here individually for each detector, with approx. 2 s allocated for each detector. If detector "MC living room" triggers an alarm, for example, the text not only appears on the display when the alarm is disarmed, but the name of the alarm is also audibly played back. Do not forget to select "Playback" after recording the detector text to check what was recorded and ensure it is correct and intelligible.

Voice message 2 second announcement for each zone

If this function is activated:

User menu -> Configuration -> Functions -> Zone name announcement ->

Enabled on and zone names are spoken, an additional announcement is made:

For an open zone

"The alarm system cannot be armed" + "<Zone name>" For several open zones, the zone with the lowest zone number will be announced in addition.

During an alarm

- **Voice dialler** Following an "individual message" and "Message x", the zone first triggered will be announced in addition.
- **Alarm panel** The zone first triggered will be announced with each partition. The partition with the lowest number will be first.

Example:

Alarms were triggered in the following zones in the following order:

Zone 226 Partition 3
Zone 225 Partition 1
Zone 203 Partition 1

The following can be heard over the system:

"The partition is deactivated! Important! An alarm was triggered!
<Zone 225 voice message>, <Zone 226 voice message> Reset required"

Restart Panel

You can use this to restart the alarm panel manually.

This is helpful for some problems, to reset the alarm panel to a defined initial state.

All the settings and configurations are retained.

Note: This menu item is only visible to the administrator, i.e. the administrator must be logged into the system.

A restart is only possible when

- all partitions are "disarmed" and
- the alarm panel has completed all important communications, transmissions and actions.

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".

There are more details in Section 16.1, Manual restart (switching off and switching back on).

Keypad tones

When "On" is selected, a clicking sound via the loudspeaker is generated by pressing or touching each key.

Dynamic backlighting

Only visible if the touch front is installed.

The brightness regulation is an option for dynamic light control.

If the "Dynamic backlighting" menu item is set to "Off", it will behave similarly to the Secvest with a key front with a fixed "high", "medium" or "low" value.

If the "Dynamic backlighting" menu item is set to "On", the backlighting will adjust proportionally to the ambient light.

The high, medium and low settings still have an influence on the level and degree of the increase. The minimum and maximum values are:

Backlighting brightness	Minimum values	Maximum values
High	15%	100%
Medium	10%	50%
Low	2%	11%

Cleaning mode

Only visible if the touch front is installed.

"Off" deactivates the cleaning mode.

"On" enables the cleaning mode.

The cleaning mode (factory default "On") is started when the left and right navigation keys are pressed. The keys are disabled for a total of 35 s. You can now clean the front without accidentally triggering an action. The display shows "Cleaning mode". An acoustic warning signal and notification on the display during the last 5 s signalise that the keys will shortly function as normal. The display will show: "End of cleaning mode"

Note: It is not possible to use the alarm panel when it is in cleaning mode; this is especially true for the double key functionality (fire, intrusion, medical emergency, care).

Cleaning mode will stop if an alarm occurs.

If an alarm occurs during cleaning mode, the cleaning mode will immediately be aborted and the keypad will return to normal use at once.

If a nursing emergency call timer starts, the cleaning mode will be aborted.

A 30 s "abort time" begins when the nursing emergency call alarm is pressed.

If an inactivity warning timer starts, the cleaning mode will be aborted.

A 2 minute "abort time" begins when the care activity monitor establishes inactivity.

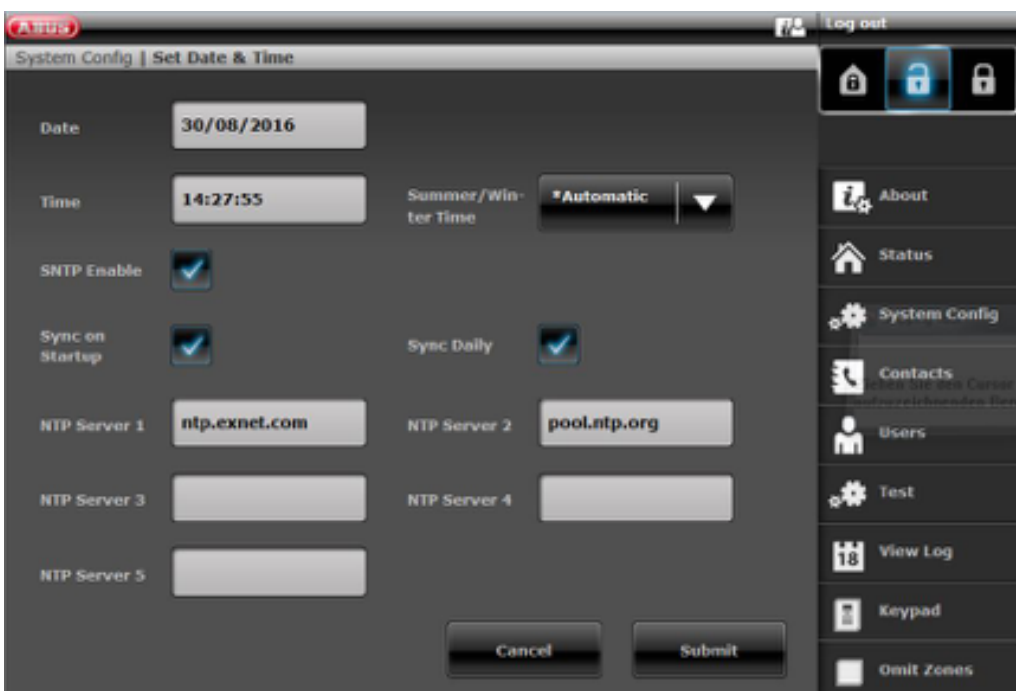
It is not possible to start the cleaning mode when an alarm is present.

10.5.2 Date & time

Only visible to the administrator.

Set the time and date here. Both can be entered directly using the number keys. Click on "Next" to navigate through the menu. Then define whether the system automatically adjusts for daylight saving time or whether you wish to adjust the system manually yourself. We recommend setting it to adjust "Automatically".

Activating the check box on the web interface allows the times to be called up from an NTP time server. Here, you can also set when the system should synchronise with the selected provider.

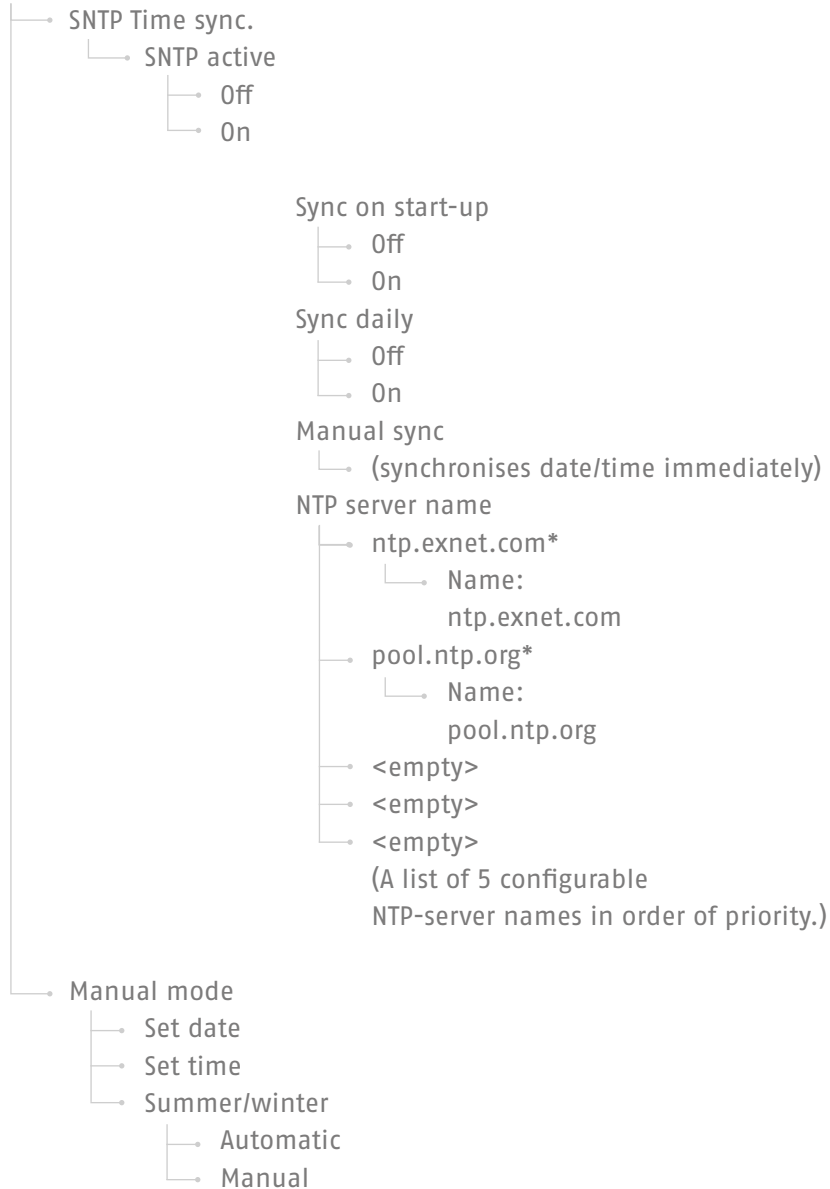


The screenshot shows a web interface for configuring the system date and time. The page title is "System Config | Set Date & Time". The interface includes the following fields and controls:

- Date:** A text input field containing "30/08/2016".
- Time:** A text input field containing "14:27:55".
- Summer/Winter Time:** A dropdown menu currently set to "Automatic".
- SNTP Enable:** A checked checkbox.
- Sync on Startup:** A checked checkbox.
- Sync Daily:** A checked checkbox.
- NTP Server 1:** A text input field containing "ntp.exnet.com".
- NTP Server 2:** A text input field containing "pool.ntp.org".
- NTP Server 3:** An empty text input field.
- NTP Server 4:** An empty text input field.
- NTP Server 5:** An empty text input field.

At the bottom of the form are "Cancel" and "Submit" buttons. On the right side, there is a sidebar menu with icons for "About", "Status", "System Config", "Contacts", "Users", "Test", "View Log", "Keypad", and "Omit Zones". A "Log out" button is located at the top right of the sidebar area.

User menu -> Configuration -> Date & time



10.5.3 Edit outputs

Only visible to the administrator.

If your installer has configured the outputs as the "user defined" type and as enabled editing, you can edit them here.

You can change the following:

Name of the output

Polarity

Continuous or pulse switching

Schedule

Event

- Up to 3 events can be assigned and edited.

10.5.4 Remote controls

Only visible to the administrator.

Assigned remote controls can be edited or removed here. The following options are available:

- Edit: press the * key of the remote control to reprogram it. The standard setting of the key is "Internal arming". If you wish to switch a relay output with this key instead, however, this function can be assigned to this key. A suitable relay output must first exist in the system. Speak to your specialist installation contractor if you require this function, such as to open the garage door via a relay output.
- Remove: remove a remote control that has been lost or is no longer needed. If you still have the remote control, press any key. If you have lost the remote control, press "No remote control" to delete it without having to press a key.
- Delete All you can delete all remote controls in the system at once here.
- Panic response: if the remote control has a panic alarm, this function can be disabled here. The "panic alarm" on the remote control can be triggered by pressing both padlock keys at the same time.

10.5.5 Volume settings

Only visible to the administrator.

LAUTSTARKE EINSTELLUNGEN	
Bedienungstöne	0
Infotöne	0
Alarmtöne	0
Sprache Lautstärke	▶
Nachricht Lautstärke	▶
Zurück	Wählen

Set the volume of different tones here. The tones can be changed by directly entering a number from 0–9, where 0 means muted and 9 represents maximum volume.

Operation tones: refers to all tones that occur when the system is being operated such as the feedback tones when operating the system via the keypad.

Info tones: refers to all info tones, such as feedback tones for error messages.

Alarm tones: The volume of the alarm tones (intrusion, fire, etc.) can be changed here. The volume of the messages can be changed by clicking "Select" and then adjusting the volume using the +/- keys.

We recommend leaving alarm tones set to "9". If you set the volume of the alarm tones too low, you may not hear an alarm in time or at all.

10.5.6 Web access

Only visible to the administrator.

Define whether or not your system can be programmed or operated remotely by the installer here.

- **Disabled** Web access disabled (admin, normal users and level 4 users still have access)
- **Enabled** Web access enabled

10.5.7 Remote updates

Only visible to the administrator.

Define whether your system can be remotely updated here. For details, see the installation manual, "B/W upgrade" appendix

"Disabled" A level-4 user cannot update your alarm panel.

"Enabled" Approval is granted so a level-4 user can update your system.

10.5.8 Time schedule active/inactive

Only visible to the administrator.

You can enable the "week planner" in this menu. For example, if on Monday to Friday you want the system to disarm at 7 a.m. and then arm at 6 p.m. (a typical timeframe for a shop), you can set this up here.

We recommend setting up the week planner via the web interface (see "Web access").

"Web access – Time scheduler" describes the setup of the week planner in detail.

10.6 Contacts

Only visible to the administrator.



You can manage your contacts in this menu. Use the telephone/IP interface or similar of your Secvest, for example, to forward alarms. The contacts can be adjusted here or new data entered. Not all fields must be completed.



Select "Contacts" to access the following menu:

You can choose up to 12 contacts. Usually the contacts are initially set up in consultation with your specialist installation contractor. Using the example of "Contact A", the following options can be seen:

- **Name:** Enter the name of the contact
- **Partitions:** 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.
- **Voice /SMS/Email:** The recipient can be assigned to partitions (Deactivated, Activated, Part Set). This means that the recipient will only receive a message when an event occurs in the specified partition with the corresponding state.
- **Tel. no 1:** Enter telephone number 1 of the contact
- **Tel. no 2:** Enter telephone number 2 of the contact
- **Email:** Enter the email address of the contact
- **SIP user ID:** If VoIP is used, the "User ID" is entered here.

Important: only make changes to contact entries, such as when a number has changed or the contact can no longer be reached. The assignment of sub-areas is only applicable to voice diallers, text messages and email, and not to ARC/ESCC connection.

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.

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

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.

10.7 Test

Only visible to the administrator.

The test menu provides the option of testing the various functions of your system to ensure they are working properly. Depending on the setup level of your alarm panel, certain functions may not be available.

Select "Test" to access the following menu:



The following options are available:

- Walk test
- Sirens & Sounders
- Door locks
- Outputs
- Prox Tag
- Remote controls
- Emergency buttons
- Telephone call

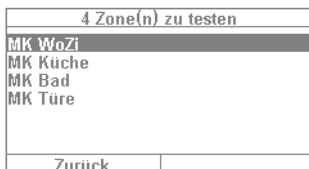
10.7.1 Walk test



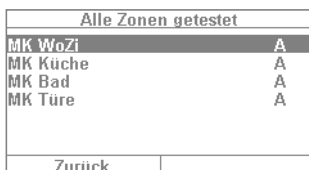
1. You can test your detectors in the "walk test". For example, if you want to know whether a certain detector is functioning properly, you do not have to trigger an alarm. Simply select "walk test" and test your detector. We recommend proceeding as follows: Open the walk test and activate the "Bell – on" menu.



2. A feedback tone sounds in this case when you trigger a detector during the walk test.



3. Select "System" and your detectors should be listed (the number of detectors varies depending on the setup level of the system – in this example you see 4).



4. Then open the window with the first detector (such as a magnetic contact). For a motion detector you should move around briefly within its detection range. Repeat this for all detectors (you may have to do different things to trigger them depending on the type of detector). After a successful test the menu should look like the example shown on the left. In this case "A" stands for a "virtual alarm" that was triggered. The detector is working properly. If there is no entry "A" for a detector and you have tested all detectors, repeat the test for the detector in question again. If the entry fails again, contact your specialist installation contractor.

Important: ensure that you do not open the housing of a detector. Otherwise the system automatically exits the walk test and triggers a tampering alarm. Detector housings are only opened by the specialist installation contractor for maintenance purposes.

Under "partitions" you can select whether only detectors from a certain partition are tested. Under "Zones" you can select whether only certain detectors are tested. The procedure is then the same as for the walk test.

10.7.2 Sirens & sounders

Test the function of different sirens and sounders here. Click on "Change" to test the following:

- **Internal sirens:** Test the installed sirens of the alarm panel and any indoor sirens here.
- **External wireless sirens:** If at least one wireless siren exists in the system, it can be tested here. We recommend only briefly testing this function. Warn your neighbours before testing if necessary.
- **Sounder Module** If a universal module (UVM) is installed as a "siren module", you can test its function here. Again: please warn your neighbours before testing.
- **Loudspeaker:** Test the installed loudspeaker of the Secvest here. Select "Play/Stop" to hear all existing messages in the system one after the other.

10.7.3 Door locks

If a Secvest key and/or additional door lock is installed, it is a good idea to check its function occasionally. Engage the lock while the alarm panel is disarmed – the message "Open" or "Closed" is displayed.

10.7.4 Outputs





If a relay output is enabled this menu appears here. Click on "Select" and test the output using the "On/off" function. If relay contacts (from the Secvest, universal module or wireless socket) have been enabled by the specialist installation contractor, you can test these if necessary. The corresponding relay contact must be enabled for you as the user in order to test it. There are relay contacts that only activate when an intruder alarm is triggered and therefore cannot be accessed in this menu. Speak to your specialist installation contractor if you wish to access a relay contact, for example to use a wireless socket for lighting control.

10.7.5 Proximity / chip key

If your system has a proximity chip key and you wish to test its function, take the key and swipe it over the chip key reader area in the lower area of the alarm system (at the height of the ABUS logo). If the chip key is read successfully, the display indicates which user the chip key is assigned to.

10.7.6 Remote controls

If you wish to test the function of a remote control, select this menu and press the different keys one after the other. The display then indicates which keys have been pressed and what function is assigned to the key in question. The standard assignment of the remote control is:

	Closed padlock	Complete arming
	Star key	Internal arming (= perimeter protection on)
	? key	Status query
	Open padlock	Complete disarming

The user assignment is also displayed and the signal level of the triggered remote control, e.g. RSSI:9. RSSI stands for "received signal strength indication". An RSSI value of "9" indicates an excellent received signal strength, as the scale for the Secvest runs from 1–9, where 9 is the maximum strength.

10.7.7 Emergency call button

An existing emergency call button (for nursing, panic alarm or medical emergency) can be tested here by pressing the emergency call button. Depending on which function has been assigned to the emergency call button, the function of the button is displayed. For example, "PFN alarm" (PFN = nursing emergency call). As with the remote control, the RSSI and user assignment are also displayed.

10.7.8 Telephone call

If your system is equipped with an active telephone interface (PSTN or wireless mobile), you can test the function of the connection by making a test call. Enter any telephone number. If dialling is successful you get a dial tone. However, when the other party answers, you can only hear the other party.

If the connection is not activated or is otherwise disrupted, you get the error message "Communication error". Check the other telephone connections in the house if there are any and contact your specialist installation contractor if necessary.

Note: You can also recharge the credit for your prepaid wireless mobile SIM card via the wireless mobile telephone connection. Dial the corresponding service telephone number, follow the instructions and enter your recharge code using the number keys. The service portal sometimes requires you to use the star key (*) or the hash key (#) for navigation. These keys can also be used here.

10.8 Log book



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). A list of the different log book entries can be found in the appendix under "Log book overview".

10.9 Info

Only visible to the administrator.



This menu is used to check the software version of the wireless alarm panel and query the communication interfaces. You cannot change any configurations in this menu.

10.9.1 Alarm panel

- **Version:** Information about software version, e.g. V2.01.08
- **S/N:** Serial number of the alarm panel, e.g. FUAA50000#E.....
- **Part no:** Article number of the alarm panel, e.g. FUAA50000
- **Language:** Set language including language version, e.g. English v1.24

RF Device exclusivity: Indicate which components can be added.

"Yes" only "new" components, e.g. FUMK500XX, FUBW50000

"No" all components, also "old" components, e.g. FU8320, FU8350

The web interface provides the following information:

ABUS Abmelden

Info | Zentrale

Version: v2.01.07 Sprache: Deutsch v1.24
Serien Nr.: SECVEST###GC028819AAB Part No.: FUAA50000
RF Device Exclusivity: Nein
Uhrzeit Zentrale: Datum: Datum & Uhrzeit
Zonen: Verfügbar: 58 Verwendet: IP: 0 FUNK: 5 VERDRAHTET: 0
Funk Bedienteil: 2 Funk Sirenen: 1
UVM: 0 Türschlösser: 2
Teilbereiche: 1
Ausgänge: Verfügbar: 36 Verwendet: FUNK: 0 VERDRAHTET: 0
Gehäusefront Sabo: Schallgeber Sabo: RF Jamming:
AC Störung Zentrale: Externe DC Störung
Ext. DC Voltage In:
Akku 1 Status: Akku 2 Status:
Auxiliary:

Schließen

Info
Status
Komponenten
Ausgänge
Teilbereiche
System
Kommunikation
Pflegenotruf
Test
Logbuch
Tastatur

Name/function	Explanation
Version, language	Version number of the software currently installed on the alarm system Version number for the configured language
Serial Number	Serial number of the alarm system
Part No.:	Article number of the alarm system
Alarm panel time, date	Currently set time and date on the control panel
Date & time	Synchronises date and time of the alarm panel with the date and time from the PC via mouse click
Zones	Overview of available and configured zones
Wireless control panel	Number of components in use
Wireless sirens	Number of components in use
WAM	Number of components in use
Door locks	Number of components in use
Partitions	Number of partitions in use
Outputs	Overview of available and configured outputs
Housing front tampering	Specifies whether the tamper contact on the front of the housing has been triggered
Bell tampering	Specifies whether the tamper contact on the wired, connected siren has been triggered
RF Jamming	Specifies whether the alarm panel has detected RF jamming
Alarm panel A/C fault	Displays whether the alarm panel is connected to 230 V or if a fault is present
External DC fault	Displays whether the alarm panel is connected to 13.8 V external DC power supply or if a fault is present
Ext. DC voltage in	Specifies the voltage of the external DC power supply
Battery status	Status of each battery (with voltage if required)
Auxiliary	Output voltage to the power supply output terminals

10.9.2 Communication

PSTN: Info => Communication => PSTN

INFO KOMMUNIKATION	
PSTN	▶
GSM	▶
Ethernet	▶
Zurück	Wählen

PSTN link status query. The Secvest then checks the installed landline. If it is not enabled or is disrupted, the error message "Error" appears. Otherwise the message "Test successful" appears.

Mobile: Info => Communication => Mobile

GSM - HUAWEI MG323-B	
Netzwerk	▶
IMEI	▶
Kunden-Nr.	▶
IMSI	▶
Version	▶
Rücksetzen	▶
Zurück	Wählen

(This menu only appears when the wireless mobile module is installed.) You can query information about the wireless mobile module here, such as IMEI, SIM card number (if supported by the provider) and network operator. Select "Network", for example, and the network operator and signal level are displayed.

GSM NETZ	
E-Plus	RSSI: 5
Zurück	Wählen

The signal level in this case ranges from 1 (very poor reception) to 10 (excellent reception).

The value inside the brackets indicates the availability of the data connection.

"Without" 2G network only available, voice, no data possible

(G) GPRS network available.

(4G) LTE/4G network available.

Ethernet Info => Communication => Ethernet

If the system is integrated in a network via a network cable (e.g. via the router in the home network), you can view the items listed below. Speak to your specialist installation contractor if in doubt, as for some of the listed values specific knowledge of networking is required.

IP address

If the Secvest is located on a network the IP address is shown here, e.g. 192.168.178.23. If (DCHP) is shown after this in brackets, the Secvest automatically obtains its IP address from a DHCP server, for example, in a router. If the Secvest is not networked, "0.0.0.0" is displayed here.

IP Subnet Mask

The subnet mask is displayed here. In a private network this is normally 255.255.255.0.

Gateway IP address

If the Secvest is located on a network the IP address of the gateway is shown here. An example of a gateway in a private network is the router, e.g. the Fritz!Box.

DNS primary IP address

This is the IP address of the Domain Name System (DNS).

MAC address

The hardware address of the network adapter for the Secvest is given here. A MAC address is globally unique.





IP Link Status

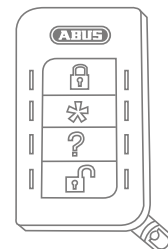
The message "OK" appears if the Secvest has a functioning network connection. "Error" appears if the network connection is disrupted or the Secvest is not connected to the network at all.

11. ADVANCED SYSTEM OPERATION

11.1 Remote control

If you have a remote control you can arm or disarm the wireless alarm system by pressing the remote control keys:

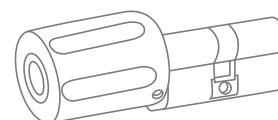
	Key 1	Arm
	Key 2	Arm internally (or 'Switch output'. The key has to be reprogrammed for this function).
	Key 3	Status query
	Key 4	Disarm



11.2 Wireless cylinder ("Secvest key")

Arming

The wireless cylinder lock can be used to easily arm the system. To arm the alarm panel, first press the button on the cylinder and then lock the doors. Once the doors are locked the alarm panel is armed.

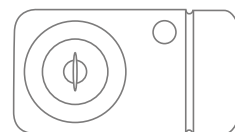


Disarm

Likewise, you can completely disarm the system by opening the doors. Open the doors as normal. The wireless cylinder lock transmits the signal to disarm the alarm panel, which disarms the system immediately.

11.3 Additional door lock (FU7010/7025E)

If a wireless additional door lock from ABUS is installed, you can arm and disarm the system in a way similar to the wireless cylinder lock. The additional door lock provides a high degree of electromechanical security as it ensures intruders are met with up to one tonne of pressure resistance and also triggers an alarm if there is an attempt to force the door open with a lever.



For more detailed information on this product's operation, see the relevant instruction manual. The practical steps are described here briefly.

Arm

To arm the alarm panel, lock the doors from outside using the key. After 2 complete revolutions from outside the system is automatically armed. Depending on the article number of the product, the system can also be armed from inside: for FU7010 (with rotary knob) you need one revolution, for FU7025 you need two. Important: if you wish to leave your premises very briefly but still want to lock the additional door lock, you must press the key for "suppressing arming". The door lock must then be activated within 30 s so that the system remains disarmed.

Disarm

To disarm the alarm panel unlock the additional door lock accordingly. Unlocking the lock automatically disarms the alarm panel.

11.4 Operation via telephone

If the alarm panel is connected via the A/B interface, the wireless alarm panel can call you to report an alarm. Once you have listened to the message, you can send commands to the system by pressing the keys on your telephone keypad. The system sends information about the status of your commands by playing back the voice messages (e.g. "Reset required"). You can also call your wireless alarm panel if no alarm call has taken place, in order to check your alarm system:



1. Select the alarm system telephone number. You will then hear three beeps in succession.
2. Enter the access code via the telephone keypad. You will then hear two beeps in succession.

You can then use all of the following commands upon consultation with your specialist installation contractor. The specialist installation contractor may still need to enable these commands before they can be used:

Function	Key combination
Listen	1
Speak	2
Toggle between "Listen" and "Speak"	*
Playback messages	3
End call	5
End all calls	9
Disarm system	#0*0
Arm system	#0*1
Internally arm system	#0*2
Stop sirens	#1*0
Reset system	#1*1
Query system	#3*
Switch output nnn to "On"	#9*nnn1
Switch output nnn to "Off"	#9*nnn0
Toggle output nnn	#9*nnn*

If you are called by the alarm panel in the event of an alarm, you do not need to enter the access code. However, you can operate the system using key combinations 1, 2, 3, 5 and 9. Key combinations #0*0 etc. must first be enabled by your specialist installation contractor before they can be used.

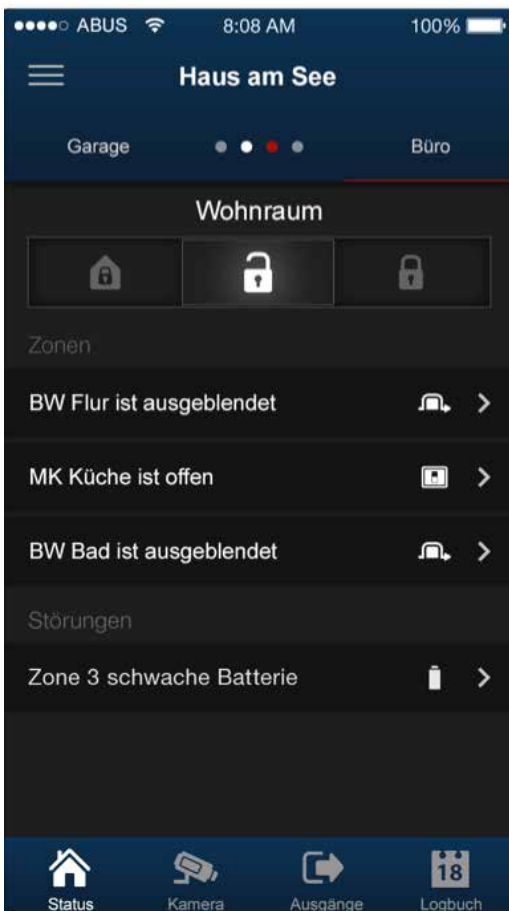
12. OPERATION VIA WEB (APP/BROWSER)

The Secvest can be easily and conveniently operated via the internet or a local network using the integrated network interface. To use these functions, the Secvest must be integrated in a network and configured accordingly by your specialist installation contractor. If you have any questions, please contact your specialist installation contractor. The following describes which options are available for operating the system via the network and how these options function.

In principle you should have these options for operating the system:

12.1 Operation via web browser

If you can access your home network from a computer, smartphone or tablet and the Secvest is also located on this network, you can access the web interface of the Secvest by entering the IP address of the Secvest in your browser (e.g. Firefox). The web interface can be used to operate the Secvest for arming and disarming the system with all the control options available directly on the alarm panel (see "Basic operation"). You can also switch to the user menu level and define settings via the web interface. You have virtually the same options as on the system itself in this case.



12.2 Operation via app

The second option for operating the Secvest via the network is to access it via the Secvest IP app. You can purchase the app in the iTunes or Google Play Store (account required). Once installed and set up on a smartphone or tablet, you can do the following things with the app:

- Arming, disarming
- Internally arm/disarm the system
- Arm/disarm sub-areas
- Switch outputs
- Submit status queries
- ...

As with operation via web browser, access to the system via network must be set up beforehand.

The following pages provide a detailed description of the procedure for both options.

In addition to operation via the app, the system can also be operated via a web browser.

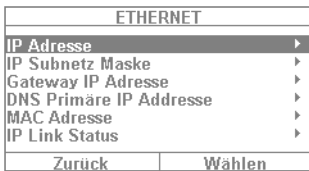
13. OPERATION VIA WEB BROWSER

You only need a normal web browser, such as Firefox. This section discusses how to operate the system via the web browser.

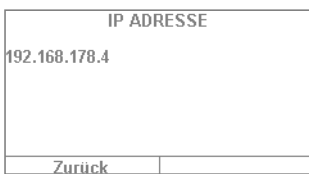
13.1 Setting the Secvest IP address



1. First you must know the IP address of your Secvest. This can most easily be found in the Secvest user menu under "Info": select "Communication" -> "Ethernet".



2. In this case the IP address has been assigned manually as 192.168.178.4. If (DHCP) were to appear after the address in brackets, this would mean that the address was automatically obtained (e.g. assigned by a router).



3. Enter this address in the address line of your web browser (without "www" or "http"). Firefox is the web browser used in this example. Depending on the browser you use, the display may look different. All standard browsers are supported, e.g. Internet Explorer, Firefox, Safari, Chrome and Opera.



4. Usually there is a message indicating that the connection is "untrusted". This does not mean that the connection between the PC and Secvest is not secure.



5. Click on "I Understand the Risks" and then "Add Exception". Then click on "Confirm Security Exception".



6. You are then directed to the login area of the web interface.



7. Enter your user name and password. In our example, this is "1234"/"1234". Then click on "Login".



8. You are then directed to the main menu of the Secvest. The next page provides an initial overview of the different options available to you at this level.



Important!

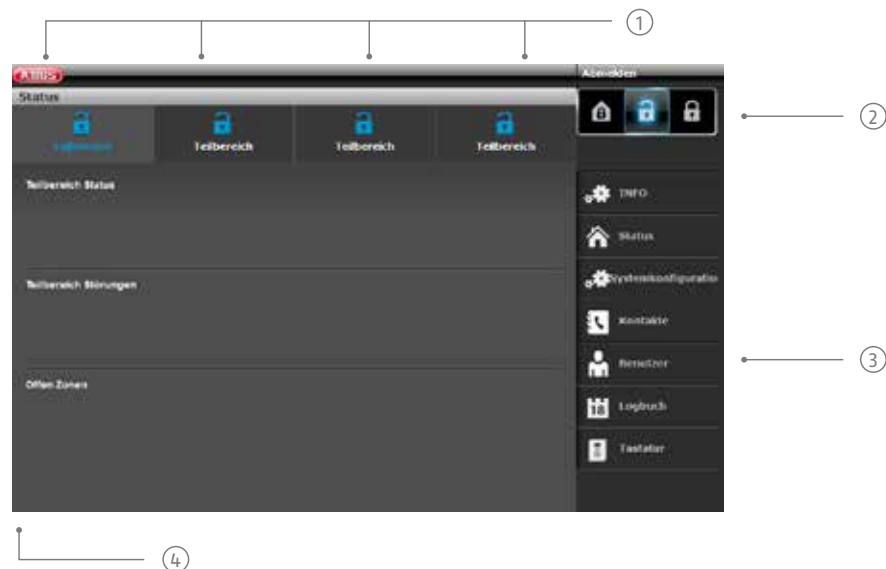
Automatic log out function:

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

- Normal user or administrator is logged in. The automatic log out occurs after **1 minute** of inactivity.
- iOS/Android app: Once opened, the app closes after 4:15 minutes have passed without an input (if "Remember PIN" is set to no) in accordance with the VdS 3169 standard.

13.2 Overview of the web interface

The web interface is very similar in its functional scope to the user menu. The control panels and menus are rearranged, however, in order to provide a more user-friendly display on the web interface. If you are familiar with the functional scope of the Secvest, the options of the web interface are described here briefly below:

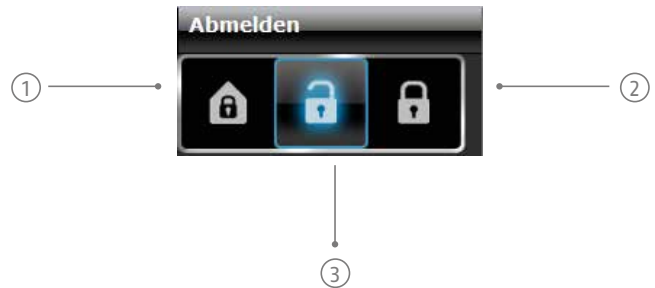


- ① Overview of status of 4 sub-areas:
open padlock = disarmed | closed padlock = armed | house symbol = internally armed
- ② Keypad for arming/disarming/internal arming
- ③ Menus for configuration, creating users, etc.
- ④ Overview of status within the specific partition. Are there errors/open zones?

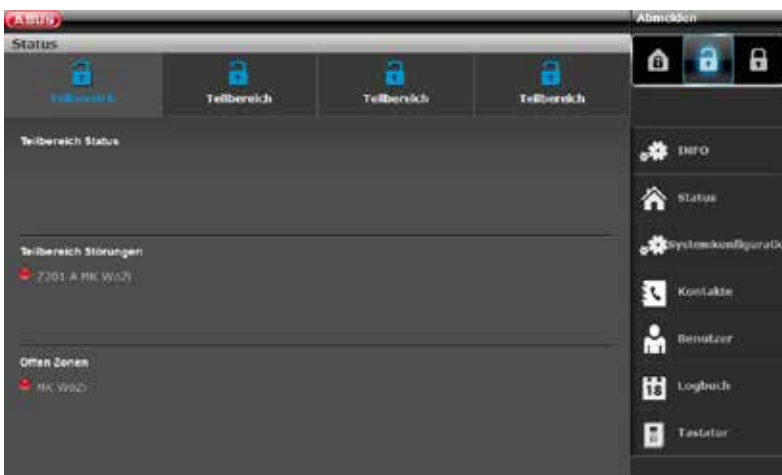
13.3 Arming & disarming

The following button can be used to arm and disarm the system. The symbols have the following meanings:

- ① Internally arm system
- ② Disarm system
- ③ Arm system



These commands can be implemented individually for each partition. First click on the partition in question and then on the corresponding arm/disarm key:



If there is an error in the system, the information on this is displayed as follows (in this example a magnetic contact is open):

If you click on "Arm" or "Internally arm" in this case, you will find that it is not possible – the padlock button remains "open". You must first resolve the error and then arm the system. If you have successfully armed the system via the web interface, the display looks like the example shown here in the following (a partition has been armed in our example).



If an alarm has been triggered within the armed partition, the display looks like the example in the figure on the left.



Acknowledge an alarm by selecting the red partition and confirming the prompt for whether the alarm should be acknowledged.



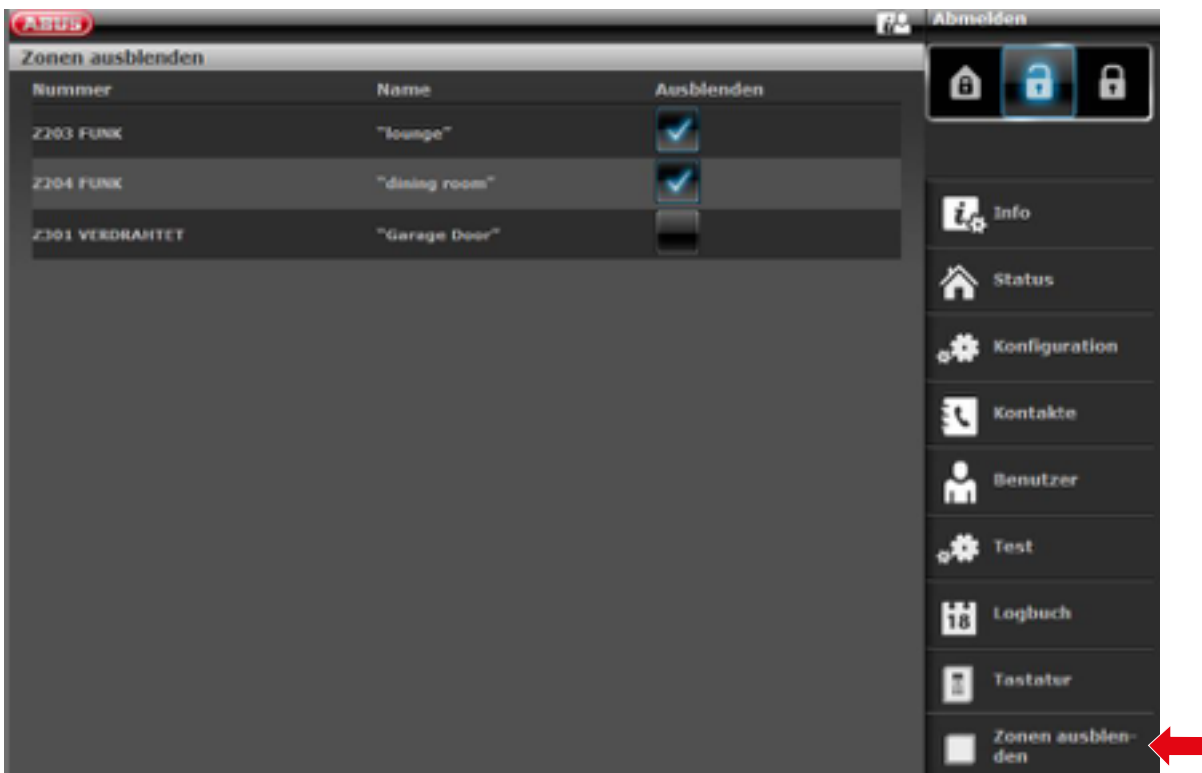
To reset the alarm panel, select the ! symbol that appears after acknowledgement in the triggered partition. This action must also be confirmed via a prompt from the alarm panel.



Obviously you can also "internally arm" your system in the usual way. Simply click the corresponding symbol (house with padlock inside).

13.3.1 Hiding zones

Using the web interface, it is also possible to hide zones. This simply requires selecting the "Hide zones" button, which will open a list of all the zones which can be hidden.



13.4 Additional web interface options

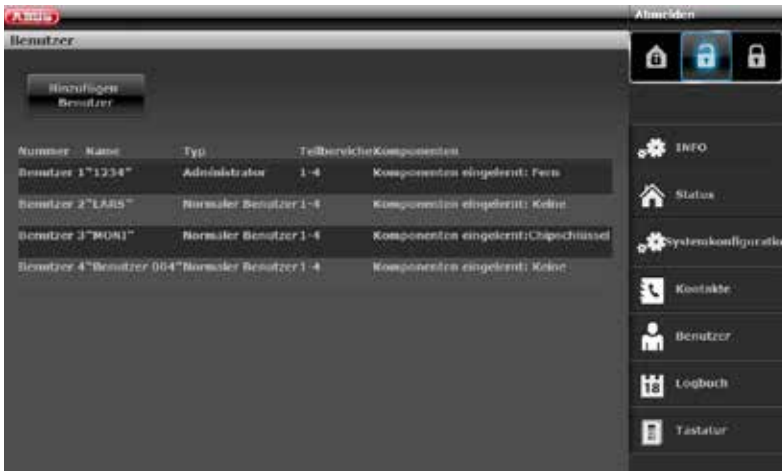
The following shows the additional options provided by web access: Many functions are explained in the "Secvest", "Basic operation" and "User menu" sections, so this section focuses on providing a brief explanation of the individual menu items. Only the "Time schedules active/inactive" menu item is described in more detail in this section. ABUS recommends configuring the time schedules via the web interface if possible, simply because it is easier and clearer to do so this way. More information can be found in the next section, "Configuring Secvest time schedules".



The same settings can be defined here as on the alarm panel itself under "System configuration".

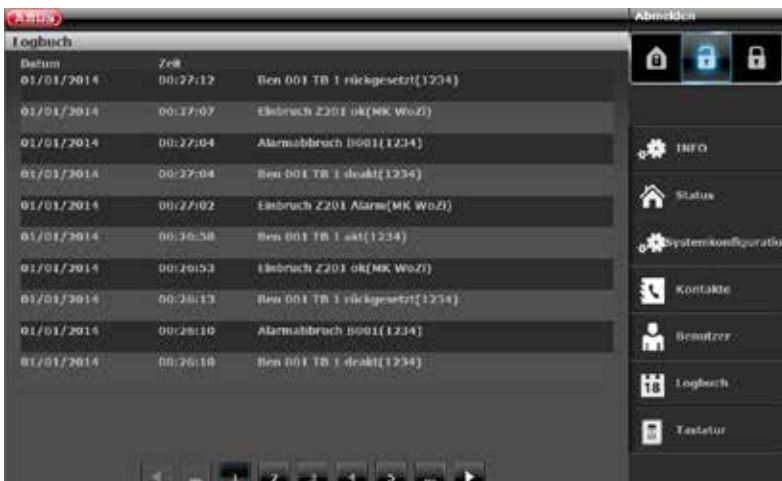


Click on "**Contacts**". Use this to edit your contacts for connections via telephone, VoIP, email etc. Please note, you should only make changes in certain circumstances, such as when one of the contacts has a new telephone number.



Then switch to "User". Just like in the user menu you can create new users here and manage and remove existing users. Click on "Add user", for example, and follow the instructions.

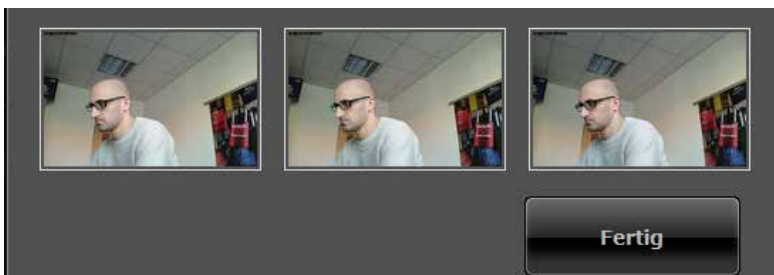
Important: for S/W<2.00.00, remote controls, chip keys, etc. cannot be added via the web interface. This must be carried out directly on the alarm panel!



Switch to the "Log book". You can view a graphical overview of the events in the log book. An overview of the different log book entries can be found in the appendix under

Logbuch		
Datum	Zeit	
03/11/2014	14:17:55	24h Z101 ok(Zone 101)
03/11/2014	14:17:55	24h Z101 Alarm(Zone 101)
03/11/2014	14:17:47	24h Z101 ok(Zone 101)
03/11/2014	14:17:47	24h Z101 Alarm(Zone 101)
03/11/2014	14:17:08	Ben001 Log in (Web)(1234)

If a "PIR camera" has been integrated in your system, there is one point of note here: in the web interface a special entry is created in the log book if the camera has triggered an alarm. To view these entries, proceed as follows:



Click on the camera symbol to access an overview of the recorded images.



Then click on the individual images. You can save these images to your hard disk by clicking "Save" in order to use them as evidence of a break-in, for example.



Under "**Keypad**" you will find the "Virtual control panel" function. You can use this function to view the Secvest menu via the web interface and assign a created user to a remote control, for example. Move the virtual cursor keys using the mouse and go to the "User" menu. Further options are displayed there.



To define "Time schedules" for the Secvest, configuration via the web interface is strongly recommended.

13.5 Configuring Secvest "time schedules"

Basic procedure: Your alarm panel's time schedule function is especially useful in places which have recurring routines, for example, a doctor's surgery with regular opening and closing times. A time schedule is used to automatically arm or disarm the Secvest.

Important: setting up time schedules in private households is generally not necessary and very difficult to implement. Schedules are usually difficult to plan as they vary so much from day to day. Consider the fact, for example, that an open window or similar situation is very problematic with an automated arming setup.

The following examples relate to a warning time of 10 minutes.

Arming events

Ten minutes before the programmed event, the alarm panel starts giving an audible warning that the system is about to be armed via a week planner event ("week planner arming"). The alarm panel also activates all "automatic arming warning" outputs.

At the end of the warning time for week planner arming, the alarm panel stops the warning tone and immediately arms the relevant partition(s), deactivates the "automatic arming warning" outputs and activates all "armed" outputs. The system logs week planner arming events as "automatic system arming" events along with the relevant partition numbers.

Timed Set

During the warning time for week planner arming, a user can delay the arming process. To do this, you need to enter your access code in the alarm panel or hold your proximity keyfob up to the alarm panel and select "Delay". Please note, the user must have authorisation for the partition which is to be armed.

If the timer has been delayed by a user the alarm panel stops the timer and delays all subsequent arming events for 30 minutes. After 20 minutes the alarm panel starts the ten-minute count down again.

Users can delay a week planner arming event in this way up to three times in total. After the third delay, the alarm panel is armed. Please note, this delay to the arming process has no effect on disarming events.

If there is an arming fault

If there is an error which would normally prevent the system from being armed then the system is not armed via week planner events either.

Ten minutes before a week planner arming event is due the alarm panel starts the warning tone for week planner arming as usual, but when the event is due the alarm panel is not armed. The alarm panel logs an "arming fault" and activates "arming fault" outputs. Please note, zones with the "force arming hidden" attribute are hidden if they are open when automatic arming is due.

Disarming events

When the alarm panel reaches the time for a disarming event, it disarms all relevant partitions.

There are no specific warnings for disarming partitions via week planner events.

Manual arming/disarming and week planner events.

If a user arms a partition which is to be armed later via a week planner event partition remains armed.

Similarly, if a user disarms a partition which is to be disarmed later via a week planner event the partition remains disarmed.

Manual arming and disarming have no effect on the times in the week planner.

If you require at least one scheduled switch, go to "System configuration" and select "Time schedules active/inactive". This opens a new window:

This allows you to configure the alarm panel such that the alarm system (or parts thereof) is armed or disarmed at specific times within a seven-day cycle. If the system has internal arming, you can use this option for complete or internal arming of the partitions. If the system is divided into partitions, you can arm it completely or arm any combination of partitions internally.

There are two fundamental elements that you can program in calendar arming: "Events" and "Exceptions". An event defines an action (arming, internal arming or disarming) that is regularly carried out at specific times and on specific days. An exception sets times, e.g. holidays, on which events should not take place. The alarm panel can store 160 events and 20 exceptions.

Tip: Set exceptions first and then the events.

Notes:

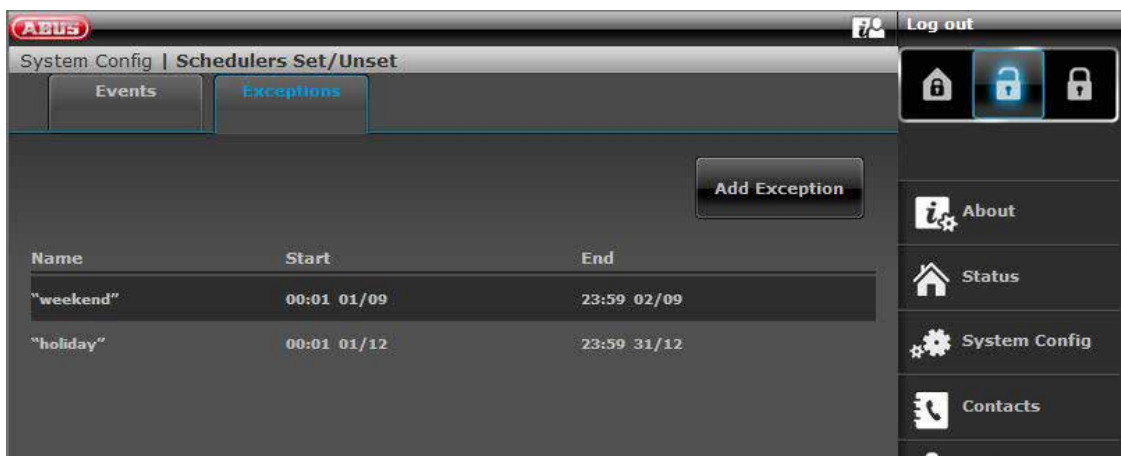
You cannot program an event such that the system or a partition switches directly from internal arming to complete arming or from complete arming to internal arming. You must first program an event that disarms the system or partition and another which completely or internally arms the system or partition. If, e.g., event A internally arms the system (or a partition), you cannot program event B such that it completely arms the system. You must program event B to disarm the system and then use an event C to completely arm the system.

If you create an event for disarming a partition and another for rearming the same partition, you must program the arming event such that it occurs at least 10 minutes after the disarming event.

The clock of the alarm panel switches between summer and winter time in spring and autumn. Do not schedule any disarming events for the autumn time changeover period on the relevant Sunday morning. For UK systems, this period is between 01:00 and 02:00. For EU alarm panels, this period is between 02:00 and 03:00. If the alarm panel disarms part of the system during this period, it does NOT rearm the system if the clock is set to winter time.

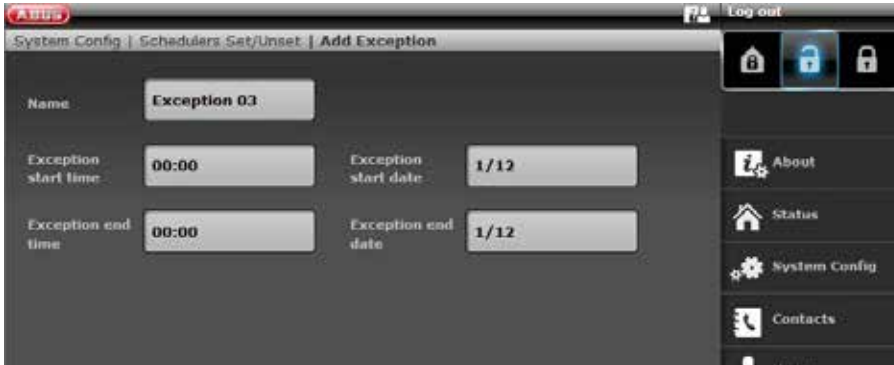
Please notify the installer of a potentially programmed time schedule during maintenance (including remote maintenance) or during configuration works. If the alarm panel is in installer mode, planned events are postponed. They will NOT be cancelled. Outstanding events take place once installer mode has ended. I.e., after maintenance by the installer, the alarm panel enters the mode desired and programmed by you for this point in time.

Add exception



Use this option to create exceptions. During the time specified by the exception, none of the events that assigned this exception take place. When you add an exception, the alarm panel guides you through the following steps:

The procedure is the same when operating the alarm panel directly.



- Name** Enter up to 12 characters.
- Exception start time** Set the time at which the exception shall begin. The time "00:00" stands for midnight, at the start of a new day.
- Exception start date** Set the date on which the exception shall begin (e.g. 31/12 for 31 December).
- Exception end time** Set the time at which the exception shall end.
- Exception end date** Set the date on which the exception shall end.

Click on "Submit" to save this exception.



Edit exception

This option allows you to edit individual parts of an exception.

Remove exception

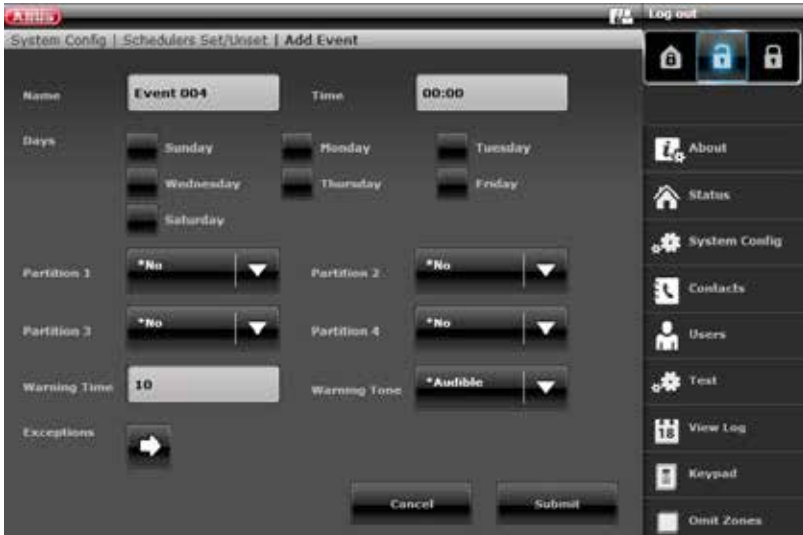
Use this option to delete exceptions.

Add event



Use this option to create events. When you select this option, the alarm panel guides you through the following sequence of options:

The procedure is the same when operating the alarm panel directly.



Name

Enter up to 12 characters.

Time

Set the time at which the event shall take place. The time "00:00" stands for midnight, at the start of a new day. Please note that if you set a start time that is less than 10 minutes from the time displayed by the alarm panel (i.e. a shorter time frame than has been set for the warning time), the event will take place on the following day.

Days

Select the days on which the event shall take place.

Actions of the respective partitions

Note: the individually assigned name of the relevant partition will be displayed – in this case "Partition 1", "Partition 2", etc.

Select the desired action. Choose from the following:

- Disarm – disarming
- Arm – complete arming
- Internal – internal arming
- None – no action

Warning time

Set the length of time (in minutes) for which the alarm panel shall sound the warning tone before an arming event takes place. Enter a value between 1 and 30 minutes. The standard setting is 10. There is no specific warning message for disarming events.

The warning tones are sounded by means of the control panels and loudspeakers assigned to the partition specified in the event. At the start of the warning time, the alarm panel activates all "Autoset warning" outputs (see installer manual). At the end of this time, the alarm panel switches off the warning tone, arms the relevant partitions immediately and deactivates all "Autoset warning" outputs.

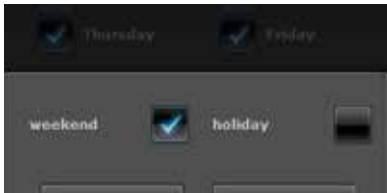
Warning signal

Choose between "Audible" and "Silent".

In the case of "Silent", the alarm panel does NOT emit a warning tone for the event (even though the warning timer is still running).

If the warning times run for longer than an event in a partition and one of the warning tones is set to "Audible", a tone will sound.

Exceptions



Select the exceptions (created using "Add exception") you wish to assign to the event.

Click on the exceptions you wish to assign to the event.

Ticked: the exception influences the event

Empty field: the exception has no influence on the event Click on "Submit" to save this assignment.

Click on "Submit" on the "Add event" page to save this event.

Edit event

This option allows you to edit individual parts of an event.



Remove event

Use this option to delete events.

Lock and unlock events

You can unlock and also lock individual events if an event is not currently required but you wish to retain the data for future use.

To do this, click on the field on the far left of the relevant row.

Ticked: the event is unlocked

Empty field: the event is locked

When operating the alarm panel directly, the procedure is as follows:

User menu -> Configuration -> Time schedules enabled/disabled -> Edit event ->

"Select" an event from the list of events -> Unlock yes/no

14. TERMS AND DEFINITIONS

Alarm system

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

Alarm type

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

Danger detector

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

Sounder

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

Alarm zone

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

Alarm panel

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

Arming, disarming

"Activation" of the alarm panel – the panel triggers an alarm if an intrusion is detected (e.g. door opener). "Deactivation" of the alarm panel – the panel does not trigger an alarm if an intrusion occurs.

Active intrusion protection

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

Outdoor siren

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

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 locks are used. The building's occupants can still move around freely within the building when the alarm system is armed. The targeted arming of the perimeter is also called "internal arming".

AWAG (telephone dialler)

Automatic dialling and messaging device: Sounder for transmitting voice messages.

AWUG (telephone dialler)

Automatic dialling and transmission device. Sounder for transmitting digital logs (for emergency monitoring stations).

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 – passive infrared), ultrasound (US) or microwave/radar (MW).

Bidirectional 2-way wireless (2WAY)

Bidirectional: Bidirectional components can also receive feedback from the alarm panel and evaluate it (e.g. via LED displays).

Chip key/proximity

Electronic "key" for quick access without code entry.

Coding of wireless signals

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

Display

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

Wired alarm system

Alarm system with detectors connected to the alarm panel via wires (good idea for new buildings and large buildings).

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).

Intruder alarm system, burglar alarm system

Alarm system that detects an intrusion and triggers an alarm ("burglar alarm system").

Individual identification of detectors

An exact designation of which detector has triggered is possible (see also "Wireless alarm zone").

External alarm (alarm type)

Alarm that causes all sounders to respond (indoors and outdoors). The event is also reported to a monitoring station, for example.

Shock detector

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

Remote access, remote configuration

Control/maintenance/configuration of the alarm panel carried out remotely.

Wireless alarm system

Alarm system with detectors that are connected to the alarm panel wirelessly (advantages: 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 window lock

Combination of mechanical window lock and electronic 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 panel is used.

Wireless remote control

For convenient arming/disarming of the alarm panel, status query and sending an emergency alarm etc. from any location.

Wireless detector

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

Wireless key switch

For convenient arming/disarming of the alarm panel without 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 buildings that is protected from severe weather (such as heavy rain) (e.g. covered entrance area or terrace).

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.

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.

Combination signalling device

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

Communication options

This allows for a silent alarm, via voice/test messages or digital logs, mobile wireless technology (wireless mobile module).

Local alarm

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 (flashing light) can remain on).

Medical emergency

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

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.

Programming

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

Proximity / chip key

Electronic "key" for quick access without code entry.

Programming

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

Smoke alarm (fire alarm)

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 consumers (for controlling light, electrical shutters or other sounders).

Tampering, tampering protection, sabotage

So that the alarm panel and its components when disarmed cannot be tampered with, each component is monitored for tampering. If a detector is opened or a cable is cut, an alarm is ALWAYS triggered. The components are usually protected by a cover contact (alarm when detector is opened) and an anti-removal wall contact.

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 panel).

Security frequency band

These frequency ranges (433 MHz or 868 MHz) are approved by the authorities (RegTP) for the security field. Signals from wireless earphones, mobile phones, garage door openers, etc. cannot interfere with devices operating in these ranges.

Seismic sensor

See "shock detector".

Signal generator

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

Status

Alarm panel status: either 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

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.)

Sabotage

See "Tampering"

Technical damage

For example, water damage, escaped gas, etc. (Protection against these things is provided by special danger detectors).

Partition

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 to an alarm panel via telephone (see AWAG, AWUG). Diallers can be integrated in alarm panels already or added as additional components.

Flood detector

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

Certifications

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

Zone


Synonym for line, describes a closed circuit to which alarm or tampering contacts are connected, which are then connected to the alarm panel.

15. TECHNICAL DATA

GENERAL

Product name	Secvest
Product description	Wireless alarm system
Manufacturer	ABUS Security-Center GmbH & Co. KG
Environmental class	II (EN 50131-1 + A1:2009 Section 7, EN50131-3 Section 7)
Protection class	IP34 (indoor)
Operating 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

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 Note  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 enabled/disabled	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 time server (SNTP time synchronisation) Accuracy when the alarm panel does not use time synchronisation via a time server: < ± 10 minutes over one year @ 20°C nominal temperature in accordance with EN50131-1 Section 8.10
Loudspeaker	1
Microphone	1

Voice messages	<p>33 voice messages for each language installed on the alarm panel</p> <p>5 messages recorded by the user (installer mode voice dialler) 12 second site message 8 seconds for each message 1–4</p> <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	1 (integrated piezo sounder) Sound pressure level > 96 dBA @ 1 m
Communication modules, plug-in	1
Ports	1x Ethernet 1x a/b 1x USB 1x SD card
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	Level 2 (EN 50131-1 + A1:2009 Section 6, EN 50131-3 Section 6)
Environmental class	II (EN 50131-1 + A1:2009)
Tamper protection (detection/protection)	Type B (EN50131-3 Section 8.7)
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.</p> <p>S/W <=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. $10^4 = 10 \times 10 \times 10 \times 10 = 10,000$ (combinatorial variation)</p> <p>1,000,000 code variants with 6-digit codes (000000–999999)</p> <p>The digits of the code are numbers between 0 and 9. $10^6 = 10 \times 10 \times 10 \times 10 \times 10 \times 10 = 1,000,000$ (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	<p>Keyboard is locked for 5 minutes after 3 incorrect codes in succession.</p> <p>Keyboard is locked for 5 minutes after 3 incorrect proximity keyfobs in succession.</p>														
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>88^{12} (215,671,155,821,681,003,462,656, 88^{12}, >1,000,000) All characters can be alphanumeric symbols or special symbols.</p> <table style="margin-left: auto; margin-right: auto;"> <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 () : . - ! & @ + _ * #</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 Σ</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 Σ
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 Σ														
Web encryption	<p>HTTPS TLS 1.2 < 2.0.0: Signature algorithm: SHA1 ≥ 2.0.0: Signature algorithm: SHA256 (SHA 2)</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

POWER SUPPLY

Type of power supply	Type A (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 @ 85VAC 190mA rms @ 230VAC 170mA rms @ 265VAC
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 (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	<p>I max. 700 mA (main pcba issue < 7) I max. 600mA (main pcba issue >= 7)</p> <p>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> <p>Running on DC input @13.0 V 12.8 V max, idle 12.2 V min, full load (@ 600 mA) @13,8 V 13.6 V max, idle 13.0 V min, full load (@ 600 mA) @14.5 V 14.3 V max, idle 13.7 V min, full load (@ 600 mA)</p> <p>Note  This output is not 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



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

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	<p>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</p> <p>Note  This output is not buffered by the battery in case of power failure. The output voltage during a power failure is directly 0 V.</p>
+BATT1 ,+BATT2	Battery polymer lithium ion, 7.4 V, 2500 mAh
OP 301, OP 302	<p>Relay output Potential-free changeover contact NO/C/NC Max. contact capacity: 500 mA @ 24 V AC rms or 30 V DC</p>
OP 303, OP 304	<p>Transistor output Open-drain Max. contact capacity: 500 mA @ 13.8 V DC</p> <p>Note  These outputs will drop to 0 V during power failures</p>
TR	<p>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.</p>
TRB	<p>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.</p>
10/100 LAN	<p>Ethernet/LAN Cat5e patch cable, RJ45 male Connector at each end, suitable for 10/100Base-T</p>
USB TYPE-B	<p>USB Mini-B connector for alarm panel USB-A connector for PC Max. length 3 m</p>
A B	<p>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 REN rating 1 PSTN data rates up to 1200 bps (V.22)</p>
Micro SD	<p>Secure Digital Memory Card Micro SD 11 mm x 15 mm x 1.0 mm 4 GB Micro SDHC</p>

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

Communication channels									
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 FUM050000 FUM050001 Quad-band GSM: 850/900/1800/1900 MHz								
GSM/GPRS (2G) LTE (4G)	Plug-in module, optional ESM050000 2G GSM: 900 and 1800 MHz 4G LTE: B3 (1800 MHz), B8 (900 MHz), B20 (800 MHz)								
Communication methods									
Web server	Web access, app and ABUS server								
ARC/ESCC reporting									
Receiver	2 Tel, 2 IP								
Protocols	<p>DTMF-based Fast Format, Contact ID</p> <p>FSK-based SIA 1, SIA 2, Ex SIA 3, Ex SIA 3 V2, Ex SIA 3 V3</p> <p>SMS-based CID in SMS</p> <p>IP Compatible with "SIA IP Reporting (TCP-2013)" DC-09 (SIA-IP), with Fast Format, Contact ID, SIA</p> <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<=3.00.03), unencrypted and encrypted (S/W>=3.00.03)</p> <p>Note:  For details, see the appendix to the instructions for installers entitled "ARC (ESCC) reporting protocol formats"</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"								
Emergency call									
Receiver	2 Tel								
Protocols	DTMF-based Scancom, Scanfast, Tunstall								

Voice dialler	
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
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) classification	The alarm panel contains an integrated SP2 (ATS2) communicator to fulfil the requirements of EN50131 for security grade 2. The alarm transmission system is compliant with EN50136-1:2012 as an SP2 (ATS2) communicator. The alarm panel supports options A, B and C for grade 2 as given in Table 10 in EN50131-1:2006+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 EN 50136-1:2012, 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 Section 6, Operation)

SW >= 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	ESM050000 FUM050001 FUM050000	ESM050000
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	2G fall back
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
---------------	---

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 T031 2014 edition

Security level: Level 2

Environmental class: Class II

If the alarm panel has been installed correctly, the Secvest will be compliant with EN50131 Grade 2.

The Secvest is compliant with EN50131-1 and EN50130-5 environmental class II.

Power supply is compliant with EN50131-1:2006+A1 2009 Section 9 and EN50131-6 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.

SW > 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 EN50131-1:2006+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.

16. TROUBLESHOOTING

16.1 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.

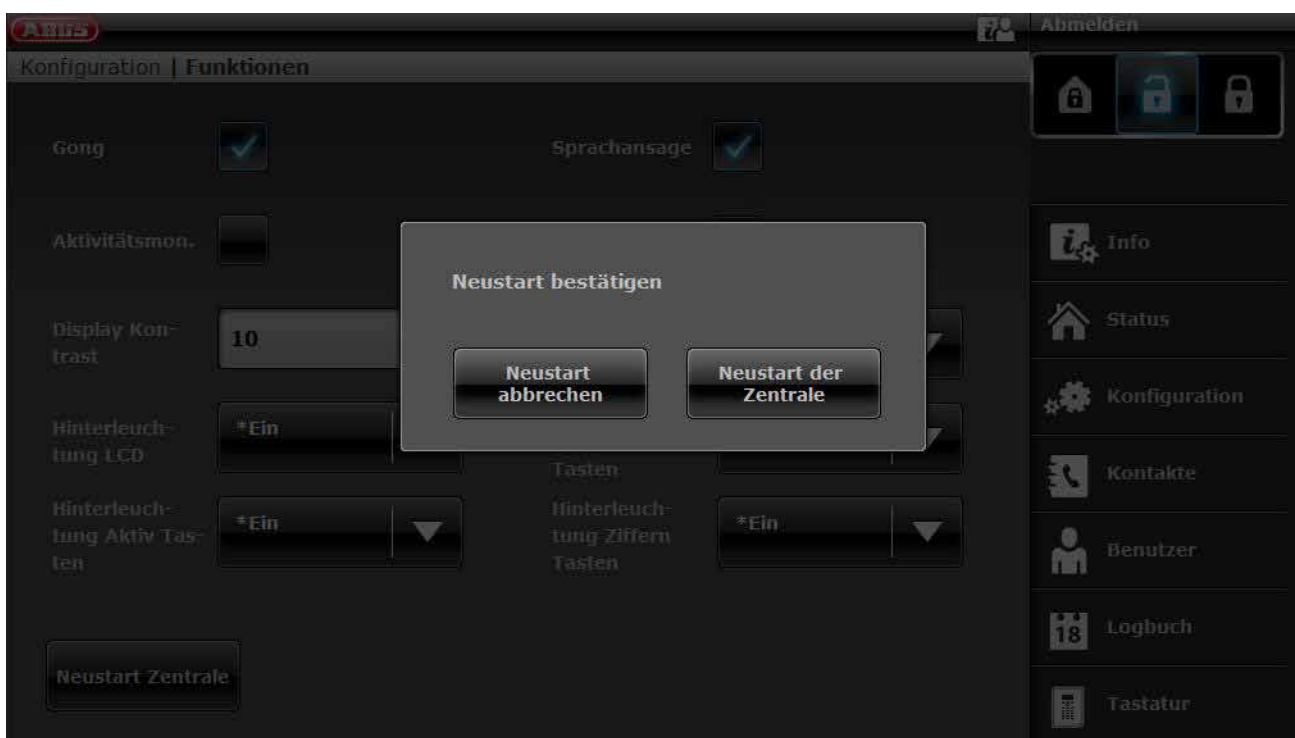
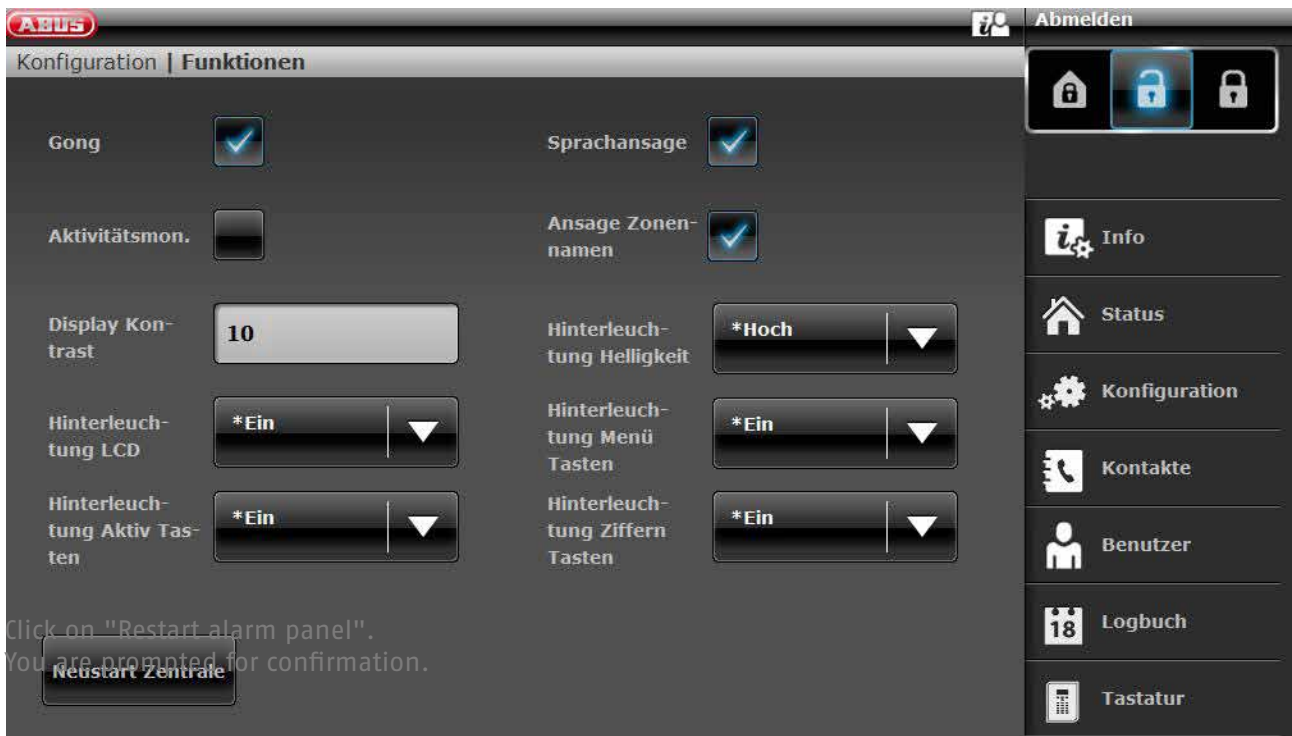
Select "Restart alarm panel" by pressing the "Change" menu key.
You are prompted for confirmation.
Press the "Yes" menu key.
At this point you can still cancel the restart.
Press "Back".

[2] Web server user menu

User menu -> Configuration -> Functions -> Restart alarm panel
You can use this to restart the alarm panel manually.

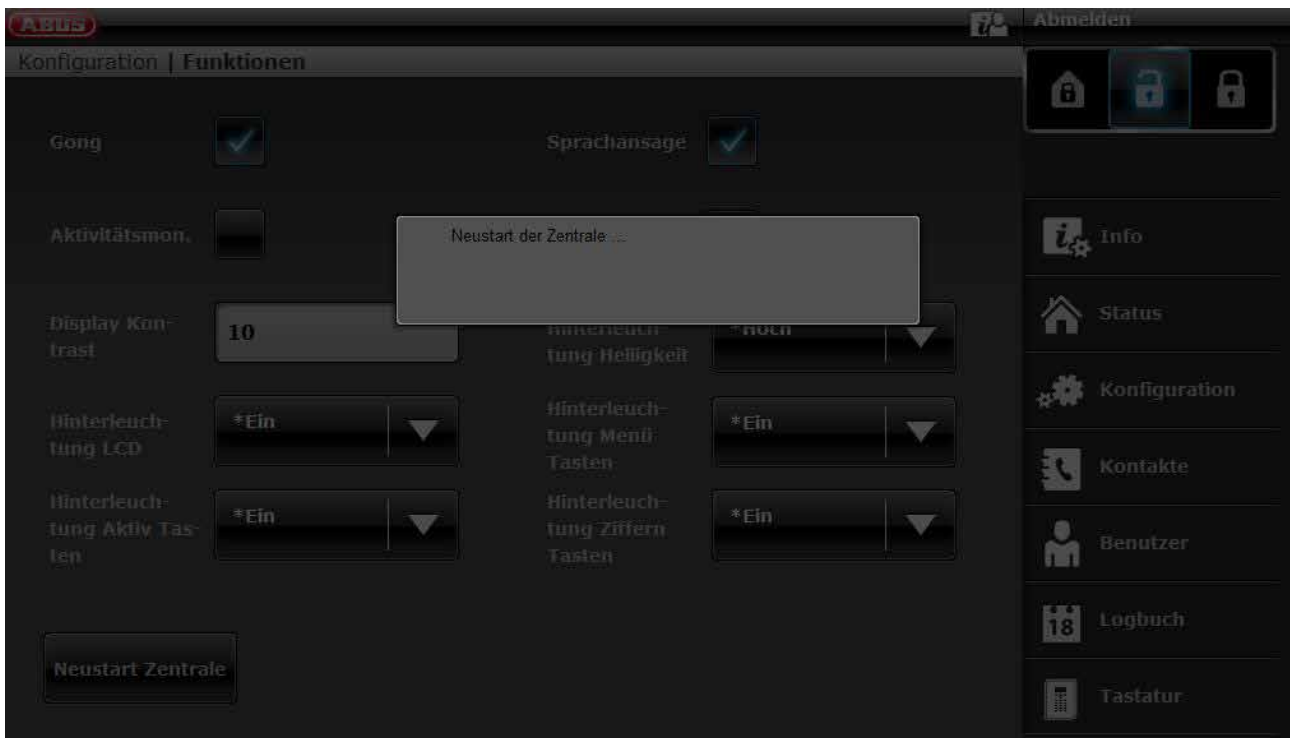
Note

This menu item is only visible to the administrator, i.e. the administrator must be logged into the system.



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.



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 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.

16.2 Wireless mobile manual test call, prepaid



Danger

Note

If you use a prepaid SIM card on a prepaid tariff, e.g. CallYa, Xtra or Magenta Mobil-Start, Please carry out a wireless mobile test call and/or send a wireless mobile test text message every month or every three months.

If you do not use the wireless mobile network for a long time, it may be that:
the wireless mobile alarm call does not work
the wireless mobile alarm text message does not work
and the card is temporarily locked by the network operator.
The card can no longer connect to the 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 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 wireless mobile test call and/or send a wireless mobile test text message **every month** or **every three months**.

However, your installer can also set up a permanent test call for you. This can take place on a daily, weekly or monthly basis.
With this type of test call, your communication channels are also tested for functionality.

ABUS Security-Center GmbH & Co. KG

Linker Kreuthweg 5
86444 Affing
Germany

Tel. +49 82 07 959 90 0
Fax +49 82 07 959 90 100

info.de@abus-sc.com
abus.com

V3.01.11