ABUS

Security Tech Germany

Secoris Alarm System

USER GUIDE

ESEZ60500 – Issue 1.1

abus.com

Certified by KIWA

⚠

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.

Data protection notice

ABUS has designed the product for GDPR-compliant use. The operator is the entity responsible for ensuring the legally compliant use of the product in accordance with the GDPR.

CONTENTS

1. ABOUT THIS GUIDE

Dear Customer,
thank you for purchasing this Secoris 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. We reserve the right to make changes to this manual without prior notice.

These instructions contain important 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.

ℹ **Note:** Some features described in this guide may not be available, depending on configuration. Please ask your installer if you would like them to be available.

This manual relates to firmware version 1.00.00 and all other previously published software versions.
All new features that are only valid from a certain software version are marked accordingly, e.g. >=2.00.00.
All other features that are valid up to a certain software version are also marked accordingly, e.g. <2.00.00.

1.1 Explanation of Symbols

The following symbols are used in this manual:

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

1.2 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 alarm panel which existed at the time of purchase, contact your dealer directly within the first two years.

1.3 Handling log-in details for your Secoris System

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.

1.4 Important Safety Information

Power supply

Caution: All electrical connections must be carried out by a qualified electrician and comply with current local regulations.

Children

Important: Keep electrical devices out of reach of children. Never allow children to use electrical devices unsupervised. Children may not always properly identify possible hazards. Small parts may be fatal if swallowed. There is a risk of suffocation. This device is not intended for children. If used incorrectly, parts under spring tension may fly out and cause injury to children (e.g. to eyes).

Cleaning

Only clean the device housing with a damp cloth. Do not use solvents, white spirit, thinners or other caustic substances: Rub the surface gently with a cotton cloth until it is completely dry.

Disposal

Important: EU Directive 2012/19/EU regulates the proper return, treatment and recycling of used electronic devices. This symbol means that, in the interest of environmental protection, the device must be disposed of separately from household or industrial waste at the end of its lifespan in accordance with applicable local legal guidelines. Used devices can be disposed of at official recycling centres in your country. Observe local regulations when disposing of materials. Further details on returns (also for non-EU countries) can be obtained from your local authority. Separate collection and recycling conserve natural resources and ensure that all the provisions for protecting health and the environment are observed when recycling the product.

1.5 Declaration of conformity

ABUS Security Center hereby declares that the enclosed product complies with the requirements of the following directives:

- EMC Directive (2014/30/EU)
- RED Directive (2014/35/EU)
- RoHS Directive (2011/65/EU)

The full EU Declaration of the Conformity text can be obtained at the following address:

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

2. ABOUT SECORIS ALARM SYSTEMS

Secoris alarm systems are suitable for domestic and commercial properties. All systems support the use of radio (wireless) and wireless detectors.

The maximum number of detectors (zones) your system can use is dependent on the panel you have selected – please contact your installer if you need to know this information.

The **Secoris alarm system** supports a wide range of communication options, configuration settings and peripheral devices, which provide the flexibility needed to customise the system to match the most demanding applications.

All systems benefit from being futureflexible: as new features are developed, your alarm system can be updated remotely or locally with the latest software to keep it up to date.

3. OPERATIONAL FEATURES

This section provides an overview of other operational features of the **Secoris** alarm systems from a user's perspective.

3.1 Comprehensive set/unset flexibility

There are many options available to the installer to configure the setting/ unsetting process to match your specific requirements.

If at any time, your requirements change, please contact your installer, who may be able to adjust the set/ unset procedure without making any physical changes.

Your system is configured as a partitioned system:

A partitioned system consists of several partitions (perhaps one per company) that can be individually set or unset without affecting the others.

In addition, each partition can be set or part set (part set B, C or D).

3.2 Alarm communication

When the system detects an alarm, it starts the external sounder/strobe units and operates internal sounders, including the sounder in keypads.

If you wish, your installer can also configure the system to communicate alarms externally to:

- An Alarm Receiving Centre (ARC), via the internet or a fixed-line or mobile telephone network.
- An email address.
- A phone using a text or speechmessage.

Note: Communications via the internet is provided as standard. Connecting the control unit to a fixed-line (PSTN) phone network requires the installer to fit a plug-on module.

3.3 User options

Authorised users can access a User menu from a keypad. The menu contains options to add users, omit zones, view log information, test the system, configure the system and switch devices (outputs) on or off.

3.4 Users and user types

Secoris gives you the ability to define many different users, each of which can have a unique access code, remote control and HUA transmitter.

Each user has a user type, such as Normal User, Admin User or Master User. The user type determines the privileges that the user has to the system.

3.5 HUA / panic alarms

You can generate Hold-Up Alarm (HUA), otherwise known as a panic alarm, from a keypad, a remote control, hand-held HUA transmitter or using a separate panic button.

3.6 Full logging

The control unit logs all actions, alarms and alerts. You can review the logged events through the User menu.

3.7 Test options

The User menu contains a comprehensive set of options that you can use to test the system or to determine the owner of a device such as a remote control.

3.8 Installer remote access

The installer has a separate Installer menu, which contains the options needed to configure your system. The menu can be accessed through a keypad.

An alternative is to allow the installer to access your system remotely over the internet, which may provide service benefits.

You have the ability to enable or disable remote access as required through the User menu.

3.9 Jamming and tamper monitoring

Secoris alarm systems use advanced techniques to monitor your system continuously for possible jamming or tamper attacks.

4. USING THE SYSTEM

This section describes typical tasks that you may need to carry out from time to time once the system is set up.

4.1 Keypad keys

Figure 1 shows the layout of keys on a typical keypad.
The purpose of each key (other than the numerical keys) is described next.

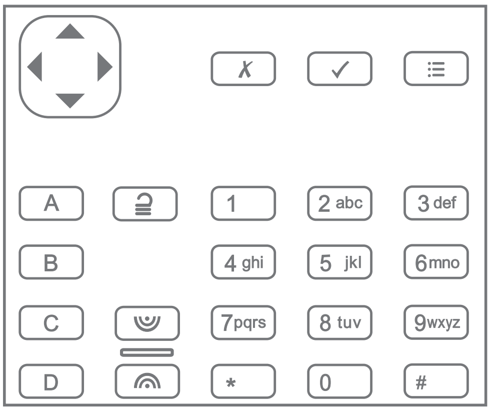


Figure 1: Typical keypad keys

Navigation key:

▲ Scrolls up, or moves the cursor left.

▼ Scrolls down, or moves the cursor right.

▶ Changes the value, displays further information, or inserts a space.

◀ Changes the value, or deletes the character to the left.

The key glows red, yellow or green to indicate system status
(green = normal; yellow = problems in setting a partition; red = alarm/fault).

✗ This key exits an option or cancels a change.

✓ Confirms an action, such as selection of an option or acknowledgement of an alarm.

☰ Pressing this key gives you access to the user menu when the standby screen is displayed (see page 13).

A It fully sets partition 1*.

B
C
D They fully set partition 2, 3 and 4 respectively*.

Unsets the system.

A Hold Up Alarm (HUA) is started when both of these keys are pressed (if enabled by the installer).

* This is the default action; the installer can configure these keys perform a different setting action, or to operate an output.

Note: A Keypad can be programmed to belong to specific partitions. When the Master user enters his code on a Keypad, it inherits all the partitions on the system. Thus, setting faults, will be shown from all partitions. Partition type users/code can be used to keep the Keypad indications just on the dedicated Keypad partitions.

4.2 About the standby screen

When the system is idle (either while set or unset), the display shows the “standby screen”. For example:

```
Secoris Alarm Panel
10:43 03/12/2019
```

4.3 Setting the system

Readying the system to start an alarm if someone moves into a protected area is called “setting” the system.

You can set your system using a variety of different methods, depending on system configuration. The following explains a typical method using a keypad.

1. Enter your access code at the keypad. If you enter your access code, the display shows a * for each completed digit:

```
Enter Access Code:
(*  )
```

2. If setting options are displayed, you can press ▲ or ▼ followed by ✔ to choose the option you require:

```
Setting Options
Full Set All
```

- **Full Set/Fulll Set All**: To set the whole system. Alternatively, press the A key*.
- **Partitions**: To set or part set a partition. Alternatively, press the B, C or D key to full set a partition*.

  * Your installer may have configured the system to allow you to quick set using A, B, C or D without entering an access code.

3. You will hear a continuous exit tone (unless the system is configured for silent or instant setting).

   The system sets when one of the following occurs, depending on how the system is configured:

- Immediately
- After a period of time
- When you exit the premises

The A, B, C or D key illuminates to indicate the set status (unless disabled by the installer). For example, by default the A key is illuminated if partition 1 is fully set.

4.4 Unsetting the system

Disarming the system so that people can move freely is called “unsetting”.

To unset the system from a keypad:

1. Enter through the designated entry route. Do not stray from this route –you may cause an alarm.
2. If you hear a tone, go directly to thekeypad, since you will have limited time to unset the system before it generates an alarm.
3. Enter your access code and press the unset button 🔓 .

4.5 Managing alarms

If there is an alarm, you will need to silence the sirens and sounders (if they are still running), acknowledge the cause of the alarm and reset the system.

To silence, acknowledge and reset an alarm:

1. Make sure that it is safe to enter the premises.
2. Enter your access code in the normal way. This silences the alarm (if the sirens and sounders are still operating).

Note: You can silence, acknowledge and reset an alarm only if it has been caused in a partition to which you have access.

3. The navigation key glows red and the display shows, for example:

```
Press tick to reset
Zone 000
```

The display alternates between showing the zone number & zone name (e.g. “Zone 000”) and alarm type.

4. If you see “reset” in the message (see above):

   - Press ✓ – this acknowledges the alarm and resets the system. The system returns to standby and is ready to set again. The navigation key returns to its normal (green) state.

   If you see “Call Installer” or “Call ARC” at the top of the screen:

   - Press ✓ – this acknowledges the alarm, but you will need to call theinstaller or ARC to reset the system.

     Although the system is not reset, you will still be able to set and unset the system normally. The navigation key and applicable set/unset icons stay red until the alarm is reset.

Note: Accidental alarms

Your installer may have configured your system so that if you set off an alarm accidentally, you have an "Abort Time" (by default 120 seconds) in which to cancel the alarm. Go immediately to a keypad and enter your access code.

If you do this within the Abort Time, the system will send an "Alarm Abort" message to the ARC (if used).

If the alarm is cancelled after the Abort Time, immediately call any ARC the control unit communicates with to notify them of the accident.

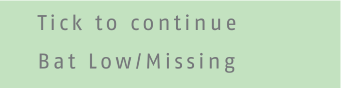
4.6 Managing alerts

An alert is an event that is not directly related to an intrusion event, such as a low battery or a communications fault.

An alert does not cause an alarm sound. Instead, the navigation key on keypads glows red when the system is unset, and keypads give a short "beep" approximately every second if the alert has not been acknowledged.

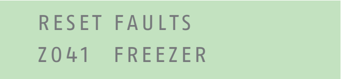
To view the cause of the alert:

1. Make sure the system is unset and thatthe keypad shows the standby screen.
2. Before entering your access code,press ✓.
3. Enter your access code to the keypad. The bottom line displays the most recent alert. For example:



```
Tick to continue
Bat Low/Missing
```

4. Press ✓ to acknowledge that you haveread the alert. Repeat this step for any other alerts that may be active.
5. If you see a message similar to the following:



```
RESET FAULTS
Z041  FREEZER
```

   This indicates that the alert has been caused by a "technical" zone (which typically is used to monitor equipment such as a freezer), and the detector is still active. If you can, rectify the problem and repeat the procedure to reset the alert.

   If you cannot clear the fault, please contact your installer.

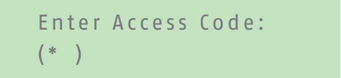
6. The standby screen is displayed and the beeping stops. The navigation key continues to glow red until the faults are rectified.

4.7 Accessing the User menu

The User menu gives access to user options such as to omit zones, view log information and add new users. The range of options available to you depends on your user type (privileges).

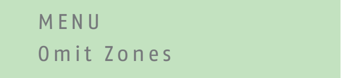
To access the User menu:

1. Make sure the display shows the standby screen.
2. Press ☰.
3. Enter your user code:



```
Enter Access Code:
(*  )
```

The first option is displayed:



```
MENU
Omit Zones
```

Press ▲ or ▼ to scroll through the options, followed by ✓ to select the option you require.

4. To leave the menu and return to the standby screen, press ✘ (if necessary, everal times).

4.8 Managing users

4.8.1 About users

A user is a person who is able to enter an access code at a keypad to perform an action such as to set or unset the system, raise a duress alarm or gain access to the user options.

When the system is new, there is only one user: the default master user, who has full access to perform any action that a user is able to do and access all user options. The master user can add new users, and while doing so, specify the user's type (Appendix A, page 39), which determines the actions the user can carry out.

4.8.2 About the Users menu

If you are a master or admin user, you can use the Users option in the main menu to:

- Add new users to the system, including the remote control and HUA transmitter allocated to each user (Users – Add User).
- Edit user details (Users – Edit User).
- Delete users (Users – Delete User).

Note: If you are not a master or admin user, the Users menu does not contain Add User, Edit User and Delete User options. Instead, depending on your user type, it may include options from the Edit User menu that allow you to change your own details, such as your access code. For some user types, the Users menu is not available at all. The menu map (Appendix B, page 41) shows the user types that have access to Users menu, and the options available. See page 17 for a description of each option.

4.8.3 Adding Users

If you are a master or admin user, you can use Users – Add User to add new users. When adding a new user, you can:

Specify the user's name, type, partitions (if applicable) and access code. Each user must have a unique access code.

- Assign a remote control and radio Hold Up Alarm (HUA) transmitter (depending on user type – a shunt code user, duress and BMS users can have none of these devices).

  If you do not wish to assign these devices, most user types can assign the devices to themselves at a later date using the Users option (depending on user type – see the menu map on Appendix B, page 41).

  A user can have only one remote control or HUA transmitter. No two users can have the same device.

Note: The level-4 user can be created only by the installer. There can be only one level-4 user.

To add a new user:

1. Select Users – Add User

2. The next available default user name is displayed If you wish, edit this default name of the user (12 characters maximum). Press ✓ to continue.

3. The default user type is displayed (normal user):

   ```
   User 004
   Normal User
   ```

   Press ▲ or ▼ to select the user type (see Appendix A, page 39 for a description of each user type). Press ✓ to continue.

4. If you are adding a user other than a master, shunt code or BMS user, you are prompted to specify the user's partitions:

   ```
   USER 004
   Partition 1    Yes
   ```

   By default, a new user belongs to all partitions. Press ▲ or ▼ to scroll through the partitions and ▶ to change the setting to Yes or No. Press ✓ to continue.

5. You are prompted to specify an access code for the user:

   ```
   Assign Access Code
   (      )
   ```

   Enter an access code, or ✓ if you do not want to assign one. When prompted, enter the code a second time.

6. You are prompted to assign a remote control to the user (except for shunt, duress and BMS users):

   ```
   Press button to
   identify Remote
   ```

   To assign a remote control, press any button on the remote control, then choose one partition to assign to the remote control. The remote control must not be already assigned to another user.

   If you do not want to assign a remote control, press ✓ at the above prompt.

Note: If you have a remote control that is already allocated, you can find out who it belongs to by using Test – Remotes (reference page 23)

7. You are prompted to assign a radio HUA (Hold-Up Alarm) device (except for shunt, duress and BMS users):

```
Press both buttons
to identify HUA
```

Press a button on an unallocated HUA transmitter until you see "HUA added", or ✓ if you do not want to assign one.

Note: If you have an HUA transmitter that is already allocated, you can find out who it belongs to by using Test – Hold Up Alarms (reference page 24).

Note: While you are registering a new HUA transmitter, the control unit will not respond to an alarm signal from any radio HUA it has already learnt.

8. If you are adding a shunt code user, press ▲ or ▼ followed by ✓ to select the shunt group to assign to the user:

```
User 005
*Shunt Group 1
```

The * indicates the currently-selected shunt group.

9. The control unit confirms that the user has been added:

```
New User Added
```

4.8.4 Editing Users

Editing another user's details

To edit another user's details (such as the user's name or type), you must log in as a master or admin user and select Edit User from the Users menu. Edit User is available only if you have logged in as a master or admin user.

You can use Edit User to change a user's name, user type, allocated partitions (if applicable) and access to the Secoris App.

Note:

- Only master users can edit the details of other master users, and even then, only the name and app access settings can be changed.
- If you are an admin user, you can edit only those users who belong to the same partitions as you.
- If a user forgets their code, a master or admin user must delete that user and recreate a new user with a new code.
- You cannot edit a user when the partition they belong to is set.
- If you want to delete another user's remote control, see "Deleting remote controls" on page 32.

4.8.5 Editing your own user details

If you are a master or admin user, you can edit your own user details (such as your user code) by selecting your user name in the Users, Edit User menu.

If you are not a master or admin user, the Users, Edit User menu is not available, but the Users menu may (depending on your user type) contain options to change your own user details. The menu map (Appendix B, page 41) shows the user types that have access to Users menu, and the options available.

You can (depending on your user type):

- Change your own access code.
- Add or delete your own remote control, Medical/Social Pedant or HUA transmitter.
- Specify the partition that your remote control can set, unset, etc.
- Enable or disable access to the Secoris App.

4.8.6 Using the Users option

To edit user details:

1. Select Users.
2. If you are a master or admin user, select Edit User, then press ▲ or ▼ followed by ✓ to select the user you wish to edit. Alternatively, enter the user number (e.g. 004) and press ✓.
3. Press ▲ or ▼ followed by ✓ to select the option you require:

Name

To change the user name.

Type

To change the user type. See (Appendix A, page 39) for a description of each user type.

Partitions

To change the partitions that the user belongs to. You cannot change the partitions allocated to a master user, since master users always belong to all partitions. Every user must belong to at least one partition.

Code

To change your own access code.

Remote

To add or delete your own remote control.
You can use the Remote Partition option to specify the partition that the remote control can set, unset, etc. Use ▲ or ▼ to scroll through the partitions, and ▶ to choose Yes or No. Press ✓ on completion.
Use Delete Remote to delete your remote control if it has been lost.

Hold Up Alarm

To add or delete your own HUA transmitter.

Remote Password

To set the remote password for a BMS or level-4 user.

App access

To enable or disable use of the Secoris App.

4.8.7 Deleting Users

If you are a master or admin user, you can use the Users – Delete User option to delete users.

Once you delete a user, the system does not respond to their access code. The control unit also deletes the identity of any remote control or HUA transmitter assigned to the user.

Note: You cannot delete User 001 (the default master user).

To delete a user:

1. Select Users – Delete User.
2. Press ▲ or ▼ followed by ✓ to select the user you wish to delete. Alternatively, enter the user number (e.g. 004) and press ✓.

```
DELETE User 004
Are you sure?
```

3. Press ✓ to delete the user (or ✘ if you have changed your mind).

4.9 Omitting zones

You can omit a zone before setting the system. Omitting a zone prevents it from generating an alarm if the zone is triggered while the system is set. You may, for example, want to omit a zone that protects a garage to enable access without causing an alarm while the system is set.

Note: The zone returns to normal operation when the system is unset.

Note: You can omit only those zones that the installer has specified can be omitted.

To omit zones:

1. Access the User menu, as described in the previous section.
2. Select the **Omit Zones** option. The firstzone you can omit is displayed. For example:

```
OMIT ZONES
Zone 000
```

An “O” is displayed at the end of the line if the zone is Omitted. An “I” is displayed if the zone is Included.

3. Press ▲ or ▼ to display the zone you wish to omit, then ▶ to mark it for omission. Press ▶ again if you made a mistake and want the zone to be included.

   Repeat this step for any other zones you wish to omit (or change to be included).

4. Press ✓ to store changes.

This product must be installed and maintained only by qualified service personnel.

4.10 Using shunt groups

About shunt groups

A shunt group is a collection of zones that can be "shunted". "Shunting" is another way of preventing a zone from causing an alarm. The difference between shunting and omitting a zone is the length of time that the control unit ignores the zone. When you omit a zone (see the previous section), the control unit ignores it for one setting/unsetting cycle. When you shunt a zone, the control unit ignores it until you unshunt it.

The installer sets up the shunt groups, each of which can consist of one or more zones. You should agree with the installer what zones need to go into each shunt group, and record that information. A zone can be in more than one shunt group.

Once the shunt groups are defined, there are three ways of shunting them:

a) Master and admin users can use the Shunt Groups option to shunt all zones in selected shunt group. A master user can select any shunt group and an admin user can select any shunt group in the same partition as the admin user.

b) A master user can use the Users – Add User option to add a Shunt Code user type and assign a shunt group to that user. When the code is used at a keypad, all zones in the shunt group are shunted. When the code is used again, the zones are unshunted.

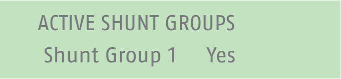
c) The installer can fit a key switch to a special zone, and link the zone to one or more shunt groups. Turning the key shunts all zones in the shunt groups. Turning the key again unshunts them.

When a user tries to set the system or a partition where zones are shunted, the keypad displays "Shunt Active tick to continue". If the user presses ✓, the system continues to set.

4.10.1 Activating or deactivating a shunt group

A master or admin user can activate or deactivate a shunt group from a keypad as follows:

1. Select Shunt Groups. The first shunt group set up by the installer is displayed:



```
ACTIVE SHUNT GROUPS
 Shunt Group 1    Yes
```

2. Press ▲ or ▼ to select the shunt group.

3. Use ▶ to change the setting to Yes (zones in shut group will be shunted) or No (zones will be unshunted).

4. Press ✓ to confirm the change.

4.11 Viewing the Log

The control unit keeps a log of events such as alarms and setting/unsetting actions. You can view the log as follows:

1. Select View Log from the main menu.

The display shows the most recent event, for example:

```
*U001 Ptn 1 Unset
10:52:07   01/12/2019
```

When applicable, the event includes the associated user number (001 in the above example), as described in the next section.

5. If applicable, press ▶ to see a more detailed description of the event, such as the user name (rather than user number) associated with the event.

   If you need information about a log event, please contact your installer.

6. Press ▼ to show older events, or ▲ to show more-recent events.

7. Press ✘ to finish viewing the log.

4.11.1 User numbers

The control unit identifies each user by a unique number as shown below.

Meaning	User Number
	Secoris Alarm Panel
Action by installer	000
Action by default master user	001
Action by other added user	002-200
Quick Set (A/B/C/D key used)	201
Action by Level 4 user	202
Action by control unit	203
Keyswitch zone used to set/unset	204
Remote reset carried out by ARC	205
Action through virtual keypad	207
Action through Secoris App	211
Action through ABUS Cloud (no user-specific action)	212
Action through web interface	“Web”

4.12 Testing the system

A master or admin user can use the Test option to test various components of the system, and to check the current owner of a remote control or HUA transmitter.

4.12.1 Testing sirens and sounders

To carry out the test:

1. Select Test – Sirens & Sounders.
2. Press ▲ or ▼ followed by ✓ to select the devices to test:

   Ext. Radio Sirens

      External radio sirens and their strobes.

   Wired Sirens

      Wired sirens and their strobes.

   Loudspeakers

      Extension loudspeakers, keypads and other internal sounders.

   Wired Keypads

      Sounders in wired keypads.

3. Press ▲ or ▼ to select whether to operate all sirens\ sounders of the selected type that are assigned to a specific partition. Press ▶ to switch the sirens\ sounders on, and ▶ again to switch them off.
4. Press ✘ to finish the test.

4.12.2 Testing a wired keypad

Note: You can test only the keypad you are currently using (you cannot test a keypad remotely).

To carry out the test:

1. Select Test – Wired Keypad.

   The bottom line of the display shows the keypad name and bus address. For example:

   ```
   Press keys to test:
   KP 51 :Keypad K1-51
   ```

   All four ABCD LEDs and LEDs around the navigation keys should glow red.

2. Press ▲, ▼, ▶ and ◀ in turn to test the navigation keys. Each time you press a key, the LEDs should change colour and the display show the key you pressed.
3. Press both HUA keys at the same time. The display should confirm that you pressed the HUA keys. An HUA alarm is not generated.

4. Press any other key to test it. The display should confirm the key you pressed.

5. Press ✘ to finish the test.

4.12.3 Performing a Walk-Test

Master and admin users can use Test – Walk Test to test detectors without starting an alarm. Walking past motion detectors should be enough to trigger them. If you have detectors connected to doors or windows, you will have to open them to trigger those detectors.

During the test, if the detector is working, the control unit sounds a confirmation tone and indicates that the detector has passed the test.

Note: You cannot test wired HUA buttons, fire detectors, and 24-hour zones during a walk test. The control unit will always start an alarm if you activate those detectors.

To carry out the test:

1. Select Test – Walk Test. The following is displayed:

```
WALK TEST
Chime          Once
```

2. Press ◀ or ▶ to select one of the following:

   Once Causes a single chime for each zone that is triggered during the walk test.

   Off Switches off chiming.

   On Generates a chime every time a zone is triggered.

3. Press ▲ or ▼ followed by ✓ to select the method of testing:

   System

   This option allows you to walk round the entire system and test all the zones.

   Partitions

   This option allows you to select one or more partitions, and test only the zones within those partitions.

   Press ▲ or ▼ to scroll up or down the list of partitions, and ▶ to display “Yes” at the end of the bottom line to mark the partition as one you want to test.

   Zones This option lets you select one or more individual zones, and test only those zones.

   Press ▲ or ▼ to scroll up and down the list of zones. Press ▶ to display “Yes” at the end of the bottom line to mark the zone as one you want to test.

4. Press ✓ to begin the test.

   The top line shows how many detectors remain to be tested. The bottom line provides a list of all the detectors ready for testing (press ▲ or ▼ to scroll through the zones):

```
10 Zone(s) to test
Zone 040
```

5. Walk round and trigger each detector in turn. If you have enabled Chime, there is a double-tone chime when you trigger a detector.

   You can see which zones still need to be tested by pressing ▲ or ▼ to scroll through the zones: an "A" is shown at the end of the bottom line for each zone that has been tested. Alternatively, you can press ≣ and scroll through the untested zones (press ≣ again to return to displaying all zones).

6. If you wish, you can press ✘ to finish the test early.

7. Once all zones are tested, you will see (for example):

```
 All Zones tested
Zone 040          A
```

   Signal Strength

   This option allows you to check the signal strength of connected RF-Zones.

   Press ▲ or ▼ to scroll up and down the list of zones.

4.12.4 Testing outputs

Master and admin users can use Test – Outputs to test outputs the installer has configured as "User Defined". The outputs may be used to control external devices, such as lights or locking equipment.

Note: You can activate or deactivate user-defined outputs at any time (see page 33).

To carry out the test:

1. Select Test – Outputs.

   The display shows the first in a list of any user-defined outputs allocated for your use. For example:

```
TEST O/P PAN>01  W
PORCH LIGHT        OFF
```

   The top line shows the address and type of the output. In the above example, the address is PAN>01 and the type is W (wired). The output type is displayed for control units that have built-in radio and wired outputs. The bottom line shows the name of the output (which may be the same as the address) and whether the output is currently on or off.

2. Press ▲ or ▼ to select the output.

3. Press ▶ to switch the output on, and ▶ again to switch it off. Check that the output is working as expected. Outputs operated via radio may take several seconds to change state.

4. Press ✔ to end the test.

4.12.5 Testing remote controls

Master and admin users can use Test – Remotes to test remote controls.

To carry out the test:

1. Select Test – Remotes.

The following is displayed:

```
Press required
Remote button
```

2. Press and hold a button on the device you wish to test until the transmit LED on the device flashes. The keypad gives a double-beep confirmation tone and you will see the results of the test:

   ```
   RM001.S:User 001
   Set Ptns>          SS:9
   ```

   The top line shows the number of the device, the button you pressed, and the name of the user the device is allocated to. The bottom line shows the function of the button and the strength of the signal.

   If the signal strength is less than 4, contact your installer.

3. Repeat step 2 for the other buttons.

Note: If you wish to test the Hold-Up Alarm buttons, make sure you press them both at the same time.

4. Press ✔ to end the test.

4.12.6 Testing user HUAs

Master and admin users can use Test – User HUAs to test radio Hold-Up Alarm (HUA) devices.

To carry out the test:

1. Select Test – User HUAs.

   The following is displayed:

   ```
   Press both HUA
   buttons
   ```

2. Press and hold both HUA buttons on the device you wish to test until the transmit LED on the device flashes. If the device has a lock button, make sure you unlock the button before the test. The keypad gives a double-beep confirmation tone and you will see the results of the test:

   ```
    User: User002
                      SS:9
   ```

   The top line shows the name of the user the device is allocated to. The bottom line shows the strength of the signal.

   If the signal strength is less than 4, contact your installer.

3. Repeat step 2 for the other HUA devices.

4. Press ✔ to end the test.

4.12.7 Testing ARC reporting

The Test – ARC Reporting option is available if the control unit uses a 4G- or PSTN-module to communicate alarms to an Alarms Receiving Centre (ARC). Master and admin users can use Test – ARC Reporting to test the connection to the ARC.

To carry out the test:

1. Select Test – ARC Reporting.

The following is displayed:

```
 ARC REPORTING
Recipient A <Tel 1>
```

2. Use ▲ or ▼ to choose one of the two recipients selected by the installer. Each recipient uses a separate telephone number to the ARC. Depending on how the installer has configured communications, the second line may be used if the first fails to connect.

3. Press ✔ to start the test.

```
 Test call started...
```

The keypad shows the progress of the call. Check with the ARC that the test call arrived. If the call fails, the display shows "Call failed", followed by the reason.

4.13 System configuration

The System Config menu allows you to change some parts of the system to suit your particular needs.

4.13.1 Switching facilities on/off

System Config – Facilities On/Off can be used to switch the following facilities on or off:

Chime

Use this option to enable or disable the chimes that occur when a zone is triggered that has a Chime attribute (as set up by the installer). For most zone types, a chime occurs only when the system is unset.

Remote Access

Use this option to enable or disable remote access to the control unit from the web interface or ABUS Cloud.

Note: By default, this feature is off for security reasons. Make sure that any installer requesting access is your authorised installer. Switch off remote access once the installer has finished.

Level 4 Update

Use this option to enable or disable access to the control unit from the level-4 user. There can be only one level-4 user, which only the installer can create.

The level-4 user is able to:

a) Update the firmware and language files at the control unit automatically or using the web interface.

b) Log into the user menu or web interface and change the level-4 user name and code.

The level-4 user cannot perform other tasks, such as to set or unset the system, omit zones, etc.

Activity Monitor

Use this option to enable or disable the activity monitor function which is the inversion of detectors for social care monitoring.

To switch facilities on or off:

1. Select System Config – Facilities On/Off .
2. Use ▲ or ▼ to choose the facility, then ▶ or ◀ to switch it on or off.
3. Press ✔.

4.13.2 Setting the date and time

You can use System Config – Set Date & Time to set the date and time. You may need to do this if, for example, the control unit lost all power for an extended period of time.

Select the option, enter the date (dd/mm/yyyy) and then the time.

Note: The installer may have set up the control unit to obtain its time automatically from the ABUS Cloud service. The internal clock adjusts itself for daylight saving in Spring and Autumn.

4.13.3 Configuring calendar sets

You can use System Config – Calendar Set to configure the control unit to set, part set or unset any collection of partitions of the alarm system at fixed times of day on a seven-day cycle. There are two basic elements that you can program within the calendar set option: the “event” and the “exception”. An event defines an action (setting, part setting or unsetting) to occur regularly at set times and days. An exception defines periods such as holidays when you do not want the event to occur. The number of events and exceptions the control unit can store is dependent on the control unit model.

Hint: Set up exceptions first, and then the events.

Note:

- You should not program an event to change the system/partition directly from one part set level to another. You should program an event to unset the system/partition first, and another event to set the system/partition to a different part set level. For example, if event 01 part sets the system (or a partition), do not program event 02 to full set the system. Instead, program event 02 to unset the system and then use event 03 to full set the system.
- If you create an event to unset a partition, and another event to set the same partition again, you must program the setting event to occur at least 10 minutes after the unsetting event.

- The control unit adjusts its clock in Spring and Autumn to allow for Summer Daylight Saving Time. At the Autumn change-over, avoid configuring any unset events to take place during the changeover time on the Sunday morning. For UK systems, this time is 01:00 to 02:00. For EU control units, this time is 02:00 to 03:00. If the control unit unsets any part of the system at these times, it will NOT set the system again when the clock changes back to Winter Time.

Manually setting and unsetting partitions does not alter the times programmed in calendar sets. If a user sets a partition that is due to be set by a calendar event, the partition remains set when the calendar event time is past. Likewise, if a user unsets a partition before a calendar event is due to unset the partition, the partition remains unset.

Add Event

Use System Config – Calendar Set – Add Event to create an event. When you select the option, the control unit will guide you through the following series of options:

Event Name

Enter up to 12 characters or press ✔ to leave the default name. See APPENDIX C on page 43 for details of how to edit text.

Event Time

Specify the time you want the event to occur, then ✔ to display the next prompt.
The time “00:00” is midnight, at the beginning of a new day.
Note that if you specify a start time that is less than 10 minutes from the current time shown by the control unit clock (that is, less than the period set by Warning Time), the event will not take action until the following day.

Event Days

Choose the days you want the event to occur.
Press ▲ or ▼ to scroll through each day of the week. Press ◀ or ▶ to specify Yes or No.

Event Actions

Press ▲ or ▼ to scroll through each partition, and ◀ or ▶ to select No (no action), Full (full set), Part (part set) or Unset.

Event Exceptions

Choose the exceptions (set up using Add Exception) that you want to apply to the event. Press ▲ or ▼ to scroll through the list of programmed exceptions. Press ◀ or ▶ to specify Yes (the exception applies to the event) or No.

Warning Time

Specify the period (in minutes) you want the control unit to sound the warning tone before the start of a setting event. Enter between 1 and 30 minutes. The default is 10. There is no specific warning indication for an unset event. The warning tone sounds at the keypads and loudspeakers allocated to the partition(s) specified in the event. At the beginning of the warning time, the control unit activates any outputs of type Autoset Warning. At the end of the period, the control unit stops the warning tone, sets the affected partition(s) without any delay and deactivates any outputs of type Autoset Warning.

Warning Tone

Press ▲ or ▼ to choose between Audible or Silent. When Silent, the control unit will NOT sound a warning tone for the event (although the warning timer will still operate).

If a warning tone is due from more than one event at the same time, and any of the tones is set to "Audible", the tone will be audible.

Edit Event

Use System Config – Calendar Set – Edit Event to edit individual parts of an event.

Delete Event

Use System Config – Calendar Set – Delete Event to delete an event.

Add Exception

Use System Config – Calendar Set – Add Exception to create an exception. During the time specified by the exception, none of the events that have the exception will take place. When you add an exception, the control unit guides you through the following steps:

Name

Enter up to 12 characters or press ✔ to leave the default name. Check APPENDIX C on page 43 for details of how to enter text.

Exception Start Time

Specify the time you want the exception to start, then ✔ to display the next prompt. The time “00:00” is midnight, at the beginning of a new day.

Exception Start Date

Specify the date you want the exception to start (for example, 31/12 for 31st December).

Exception End Time

Specify the time you want the exception to end.

Exception End Date

Specify the date you want the exception to end.

Edit Exception

Use System Config – Calendar Set – Edit Exception to edit individual parts of an exception.

Delete Exception

Use System Config – Calendar Set – Delete Exception to delete an exception.

Deferring calendar setting

During the calendar set warning time, a user can interrupt the setting process. To do this, the user must enter the access code at a keypad that has a display, then do one of the following:

- Press ◀ or ▶ to see details of which partitions or part of the system is about to set.
- Press ✘ to allow the setting event to proceed.
- Press ✔ to defer setting for 30 minutes. Note that the user must belong to the partition that is due to be set.
- Press the ☰ key to gain access to the setting menu to set another partition that is not involved in the current setting event. Note that if the user is allocated to a single partition, that partition may start setting immediately.

If a user defers a setting event, the control unit halts the warning timer, and defers setting 30 minutes from the start of the warning time. At that time, the control unit starts counting down the warning timer again.

The user can defer setting in this way a total of three times. After the third deferral, the control unit sets the system.

Note that deferring setting does not defer any unsetting events.

Setting faults – Force Set

If there is a fault that would normally prevent the system from setting, a calendar set event will also fail. Before the time of a setting event, the control unit starts the calendar set warning tone as usual, but at the setting time, the control unit will not set the system. The control unit will log the failure as "set fail". At the same time, the control unit will activate any output programmed as type Set Fail.

> Note that if an installer assigns zones the Force Set Omit attribute, the control unit will omit those zones if they are active during a scheduled setting event.

4.13.4 Defining contacts

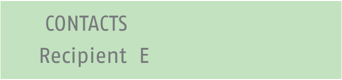
You can use System Config – Contacts to edit the Contacts List, which is a list of up to 12 contacts (by default named Recipient A-L). Contacts are used for outgoing communications, such as those for reporting alarms by speech call or SMS message.

> **Note:**
>
> - You cannot edit contacts that the installer has used for communications to an Alarms Receiving Centre (ARC).
> - Unless you are sure of what you are doing, it is recommended that you liaise with your installer before editing the Contacts List.

To edit the Contacts List:

1. Select System Config – Contacts.

   The first recipient (contact) you are able to edit is displayed:

   ```
    CONTACTS
   Recipient  E
   ```

2. Press ▲ or ▼ followed by ✔ to select the recipient you want to edit.

3. Press ▲ or ▼ followed by ✔ to select one of the following options:

   Name

   Select this to edit the name of the recipient. See Appendix C, page 43 for details of how to enter text.

   Tel No 1

   The first telephone number of the recipient.

   Tel No 2

   The second telephone number of the recipient.

Note: The Email and IP Address settings are not used, as email addresses (for emailed alarms) and IP addresses (for ARC reporting over the internet) are configured and used by ABUS Cloud.

Press ✔ when you have finished editing the setting, and if required, select another setting to edit.

4. Press ✘ several times to exit.

4.13.5 Editing Outputs

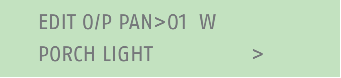
You can use System Config – Edit Outputs to edit the on and off times of any output the installer has configured as "User Defined".

Note: User-defined outputs can be activated or deactivated at any time using Outputs On/Off (see page 33).

To edit an output:

1. Select System Config – Edit Outputs.

   The first output you are able to edit is displayed:



```
EDIT O/P PAN>01  W
PORCH LIGHT           >
```

   The top line shows the address and type of the output. In the above example, the address is PAN>01 and the type is W (wired). The output type is displayed for control units that have built-in radio and wired outputs. The bottom line shows the name of the output.

2. Press ▲ or ▼ followed by ✔ to select the output you want to edit.

3. Press ▲ or ▼ followed by ✔ to select the setting to change:

   Name

   You can edit the name of the output. See Appendix C, page 43 for details of how to enter text.

   Latched

   Use ▲ or ▼ followed by ✔ to select Yes or No. When set to No, the output changes state when activated, but then returns to the normal state again after the period specified by On Time (see below). When set to Yes, the output changes state every time a user operates the output, or according to a schedule if you specify On Time, Off Time and Days (see below).

   On Time/Off Time/Days

   If Latched is set to No, use On Time to specify the number of seconds you want the output to remain active. If you specify zero seconds, the output will not operate.

   You can use On Time, Off Time and Days to specify a schedule for the output to activate and deactivate automatically. Use On Time and Off Time to specify the time you want the output to activate and deactivate. Use Days to specify the days of the week you want the output to operate (Use ▲ or ▼ to display each day, then ▶ or ◀ to choose Yes or No).

Note: If a user activates the output while it is deactivated, the output stays activated until the control unit reaches the next off time. If a user de-activates the output while it is activated, the output deactivates until the control unit reaches the next on time. Leave On Time, Off Time and Days without values if you want the output to act as a simple on/off switch.

4. Press ✔ when you have finished editing On Time/Off Time/Days.

4.13.6 Managing remote controls

You can use System Config – Remotes to specify the functions that can be carried out using remote controls. The System Config – Remotes menu contains the following options:

Edit

Used to edit the programming of the buttons, such as the buttons used to set or unset the system, or operate outputs.

Delete

Deletes a selected remote control.

Delete All

Deletes all remote controls.

Unset

Enables or disables the ability for all remote controls to unset the system.

HUA Function

Enables or disables the ability for remote controls to generate Hold-Up Alarms (HUAs).

These options are described next.

Editing the programming of the buttons

You can use System Config – Remotes – Edit to re-program the "*" button after the devices have been assigned to a user.

The button can be programmed to:

- Set a selected part set (only the partition the remote control is assigned to).
- Operate an output configured as "User Defined" by the installer.

To re-program the button on a remote control:

1. Select System Config – Remotes – Edit.

   The following is displayed:

   ```
   EDIT REMOTE
   Press Remote button
   ```

2. **EITHER:**

   a. Press the button on the remote control you want to re-program. Hold down the button until you see the transmit LED flash.

   OR (if you do not have the remote control):

   a. Press ✔ at the "Press Remote Button" prompt.

   b. Use ▲ or ▼ followed by ✔ to select the remote control you want to re-program.

   c. The display lists the first button on the remote control:

```
RM002:User 002
Button *
```

   The top line of the display shows the identity of the remote control, the button you pressed or selected, and the name of the owner. For example:

```
RM002,*:User 002
*Part Set
```

3. Use ▲ or ▼ followed by ✔ to choose the function for the button.

Note: The unset button can only be used to unset some or all partitions allocated to the user. See Unset, Unset All and Unset, Partitions below.

No Action

For the button to have no action.

Part Set

To part set B/C/D. This applies only to the partition assigned to the remote control. Use ▲ or ▼ followed by ✔ to select the part set.

Output

To operate a user-defined output. Use ▲ or ▼ followed by ✔ to select the output, then use ▲ or ▼ followed by ✔ to select the output mode:

- On – Switches the output on.
- Off – Switches the output off.
- Toggle – Changes the state of the output each time you press the button.

4. Press ✘ repeatedly to exit.

Deleting remote Controls

You may want to delete a remote control if is lost or you want to reassign it to another user. You must delete a remote control before you can reassign it to another user.

The System Config – Remotes menu provides two options for deleting remote controls:

Delete

This allows you to delete a specific remote control (see below).

Delete All

This deletes all remote controls that the system learnt. You should use this option only if you are sure you want to delete all remote controls.

To delete a specific remote control:

1. Select System Config – Remotes – Delete.

   The following is displayed:

   ```
   DELETE REMOTE
   Press Remote Button
   ```

2. Press the button on the remote control you want to delete. Alternatively, if you do not have the remote control, press ✔, then use ▲ or ▼ to choose the remote control, followed by ✔. A message similar to the following is displayed:

   ```
   RM001:User 002
   Are you sure?
   ```

3. Press ✔ to delete the remote control.

Enabling or disabling unsetting

You can use System Config – Remotes – Unset to enable or disable the ability for all remote controls to unset the system. By default, remote controls are able to unset the system, but you may want to change this for security reasons.

After selecting Unset, use ▲ or ▼ to to select Enabled or Disabled, followed by ✔.

Disabling Unset does not affect the ability for remote controls to set the system.

Enabling or disabling HUA functions

You can use System Config – Remotes – HUA Function to enable or disable the ability for a remote control to generate Hold-Up Alarms (HUAs).

Note: The installer must first enable this feature by configuring "Basic" confirmation mode.

After selecting HUA Function, use ▲ or ▼ to select Enabled or Disabled, followed by ✔.

Switching outputs on/off

Master and admin users can use Outputs On/Off to switch outputs on or off as follows:

1. Select Outputs On/Off.

   The display shows the first in a list of any outputs allocated for your use. For example:

   ```
   O/P PAN>01 W
   PORCH LIGHT      Off
   ```

   The top line shows the address and type of the output. In the above example, the address is PAN>01 and the type is W (wired). The output type is displayed for control units that have built-in radio and wired outputs. The bottom line shows the name of the output (which may be the same as the address) and whether the output is currently on or off.

2. Press▲ or ▼ to select the output.

3. Press ▶ or ◀ to switch the output on or off. Outputs operated via radio may take several seconds to change state.

4. Press ✘ repeatedly to exit.

4.13.7 Using the About options

If you are a master or admin user, you can use the About option to find information about the system you are using. The About menu contains the following options:

Panel

This gives:

- The control unit model.
- The control unit's software (firmware) and bootloader version number.
- The installed languages and their versions.

Cloud

This gives information about the connection to the ABUS Cloud.

Expanders

For each expander, this gives the expander's address, its type and the version of software (firmware) installed.

Keypads

For each keypad, this gives the keypad's address and the version of software (firmware) installed.

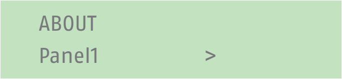
Comms

This gives information about any plug-on communications module fitted and the control unit's Ethernet connection. If required, please ask your installer for details about the information displayed.

To use the About option:

1. Select About.

   The following is displayed:



```
ABOUT
Panel1          >
```

2. Press ▲ or ▼ followed by ✔ to select the option you require.

3. If applicable, press ▲ or ▼ followed by ✔ to select the sub-option.

4. If applicable, press ▶ or ◀ to display further information.

5. Press ✘ repeatedly to exit.

4.13.8 Generating a Secoris App pairing code

You can use the Pair App option to generate a pairing code for the Secoris App. The app allows you to monitor and control your alarm system over the internet from your mobile phone or tablet.

The pairing code uniquely pairs your app with your panel and user code. This ensures that any actions you carry out using the app will affect only your panel, and are logged against your user code.

You are prompted to enter the code when you first open the app. The pairing code lasts for 15 minutes.

5. TERMS AND DEFINITIONS

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.

Alarm panel

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

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.

Alarm zone

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

Set components

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

Set/unset

"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.

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).

Bidirectional 2-way wireless (2 WAY)

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

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)

Coding of wireless signals

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

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.

Danger alarm system

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

Danger detector

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

Display

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

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.

6. DECLARATIONS OF COMPLIANCE

for the ESEZ60500 Alarm Panel System

Standards with which the alarm panel claims compliance

Security level: EN50131-1 Grade 2, VSÖ class GS-N

Environmental class II

If the alarm panel has been installed correctly, the Secoris will be compliant with EN50131 Grade 2 or VSÖ class GS-N.

The Secoris 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 (integrated SP2 [ATS2] communicator) is compliant with EN50136-1:2012 as an SP2 (ATS2) communicator.

At Grade 2 the integrated SP2 (ATS2) communicator provides a compliant communicator for the Secoris on the condition that

a) it is installed as specified in the installation instructions

b) the connected PSTN, LAN and GSM work normally

c) the alarm receiving centre has the right equipment

The ESM060010 PSTN module can be used as a supplementary communicator for Grade 2.

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.

APPENDIX A – USER TYPES

Master User	This user is able to carry out all user actions. A master user can, for example, set or unset the system and access all options in the user menus, including the ability to add or delete other users. A master user can edit any user's name, and for all but other master users, edit a user's type and partitions (if applicable). All master users always belong to all partitions. There is always (at least) one master user (User 001), which cannot be deleted by any user.
Admin	This user is similar to a master user, but is limited to one or more partitions. Admin users can set or unset the system and have access to most options in the user menu. They can add, delete or edit other users (including admin users) belonging to the same partition(s), but cannot add, edit or delete master users. Admin users can assign other users to any of the partitions that the admin user belongs to.
Normal user	A normal user can set and unset the system, but has access to a limited number of user options and may be limited to one or more partitions. A normal user can, for example, omit zones, change their own access code, view the log and operate outputs, but cannot add or delete users.
Partition user	A partition user is similar to a normal user, but has the added restriction that they must set and unset their allocated partitions from keypads that are also assigned to those partitions.
Duress Code	A duress code user can set or unset the system, but whenever the access code is used, the control unit can, for example, notify the Alarm Receiving Centre (ARC). A duress code has no access to the user menu and cannot have a remote control. **Note:** The Installer must program your system to provide this feature, and you must agree with your alarm installer and the ARC what action the ARC should take on receiving a duress message.
Guard	A guard user can only unset the system when it is in alarm and set it again. A guard user has no access to the user menu. A guard user can be allocated to one or more partitions, which are the only parts of the system that they can set and unset.
Set Only	This type of user can be allocated to one or more partitions and is able to set the system, but not unset it. A set-only user has no access to the user menu.
Set / Unset	This type of user can be allocated to one or more partition and is able to set and unset the system. A Set/Unset User has no access to the user menu.
Shunt Code	This type of user code is used only for activating and deactivating shunt groups When the user's access code is used, all zones in the shunt group assigned to this user are shunted.
Easy Set	This type of user sets or unsets all partitions allocated to the user. When the user's access code or remote control is used: • if any partition assigned to the user is currently set, all are unset. • if all partitions assigned to the user are currently unset, all are set (even if there are alerts present). No partitions are set if any has an active zone.

BMS	This is designed to give third-party systems permission to perform actions that would normally be performed by a normal user, such as setting and unsetting. A remote password is automatically generated and displayed when you create this user, which the third-party system requires.
Level-4	This type of user can be created only by the installer, and is able to update the firmware and language files at the control unit using the web interface. There can be only one level-4 user. The level-4 user cannot set or unset the system, and is able to use the user menu only to change their own name and access code (to access the web interface).

APPENDIX B – USER MENU MAP

Menu Option			Master	Admin	Normal	Partition	Guard	Set Only	Set/Unset	BMS	Duress	Easy Set	Shunt	Level-4	Keypad	Webserver	Chapter
Omit Zones			✓	✓	✓	✓				✓		✓			✓		4.9
Shunt Group			✓	✓											✓	✓	4.10
Users	Add User		✓	✓											✓	✓	4.8.3
	Edit User	Name	✓	✓										✓	✓	✓	4.8.4 - 4.8.6
		Type (not U001)	✓	✓											✓	✓	
		Partitions (not U001)	✓	✓											✓	✓	
		Code	✓	✓	✓	✓		✓	✓			✓			✓	✓	
		Remote	✓	✓	✓	✓						✓			✓		
		Hold Up Alarm	✓	✓	✓	✓						✓		✓	✓		
		Remote Password								✓					✓	✓	
		Medical Pedant	✓	✓	✓	✓									✓		
		Social Pedant	✓	✓	✓	✓									✓		
		App access	✓	✓	✓	✓									✓		
	Delete User		✓	✓											✓		4.8.7
View Log			✓	✓	✓	✓						✓			✓	✓	4.11
Test	Siren & Sounders	Ext. Radio Sirens	✓	✓											✓		4.12.1
			✓	✓											✓		
		Loudspeakers	✓	✓											✓		
		On-board Sounder	✓	✓											✓		
		Wired Keypads	✓	✓											✓		
		Internal Sounders	✓	✓											✓		
	Wired Keypad		✓	✓											✓		4.12.2
	Walk Test	Chime	✓	✓											✓		4.12.3
		System	✓	✓											✓		
		Partitions	✓	✓											✓		
		Zones	✓	✓											✓		
		Signal Strength	✓	✓											✓	✓	
	Outputs		✓	✓											✓		4.12.4
	Pedants		✓	✓											✓		
	Remotes		✓	✓											✓		4.12.5
	User HUAs		✓	✓											✓		4.12.6
	ARC Reporting		✓	✓											✓		4.12.7
	Network		✓	✓											✓		4.12.8

Menu Option				Master	Admin	Normal	Partition	Guard	Set Only	Set/Unset	BMS	Duress	Easy Set	Shunt	Level-4	Keypad	Webserver	Chapter
System Config	Facilities on/off	Chime		✔	✔	✔	✔						✔			✔		4.13.1
		Remote Access		✔												✔		
		Level 4 Update		✔	✔	✔	✔						✔			✔		
		Activity Monitor		✔	✔											✔		
	Set Date & Time			✔												✔		4.13.2
	Calendar Set	Add Event		✔	✔											✔		4.13.3
		Edit Event	Event Name	✔	✔											✔		
			Event time	✔	✔											✔		
			Event day	✔	✔											✔		
			Ward/ Paritions	✔	✔											✔		
			Exceptions	✔	✔											✔		
			Warning time	✔	✔											✔		
			Warning tone	✔	✔											✔		
		Delete Event		✔	✔											✔		
		Add Exception		✔	✔											✔		
		Edit Exception	Exception Name	✔	✔											✔		
			Exception Start Time	✔	✔											✔		
			Exception Start Date	✔	✔											✔		
			Exception End Time	✔	✔											✔		
			Exception End Date	✔	✔											✔		
		Delete Exception		✔	✔											✔		
		Force Set		✔	✔											✔		
	Contacts			✔												✔		4.13.4
	Edit Outputs			✔	✔											✔		4.13.5
	Remotes			✔	✔											✔		4.13.6
Outputs On/Off				✔	✔	✔	✔						✔			✔		
About	Panel			✔	✔											✔	✔	4.13.7
	Cloud			✔	✔											✔	✔	
	Expanders			✔	✔											✔	✔	
	Keypads			✔	✔											✔	✔	
	Comms			✔	✔											✔	✔	
Pair App				✔	✔	✔	✔	✔	✔		✔	✔	✔			✔		4.13.8

APPENDIX C – ENTERING TEXT

You can use the numeric (1-9), * and # keys to enter numbers and text.

Press a key one or more times to obtain the letter you require. For example, to enter a "B", press the "2" key twice, or to enter an "C", press "2" three times. The bottom line of the display shows the character you are about to insert and the other characters available using that key. Wait a moment before each new letter.

Press # to change between capitals and lower case letters. Press 0 to enter a space or other characters such as "&", "@" and "/".

Press ▲ to move the cursor left, or ▼ to move the cursor to the right.

Press ◀ to remove letters to the left of the cursor. Press ▶ to insert a space.

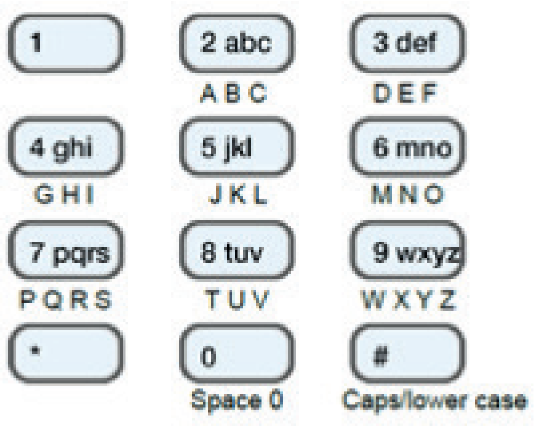


Figure 2: Letters assigned to keys

7. NOTES

Für weitere Hilfe steht unser Support-Team für Sie zur Verfügung: support@abus-sc.com
Our Support Team will be happy to help you with any further questions:
support@abus-sc.com

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

Issue 1