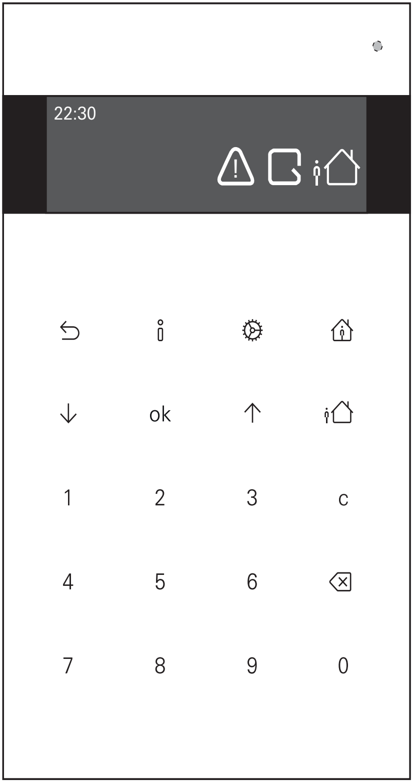
Gira security system
Alarm Connect

GIRA

Operating instructions
Wireless operating unit

→

Display and button assignment



Key: see the drop-down menu on the last page!

Table of contents

Security instructions

Change administrator PIN

Administrator PIN

The factory-assigned Administrator PIN (0001) must be changed by the main user or main person responsible for the Alarm Connect security system the first time the system is used.

If disregarded, there is a risk of misuse by unauthorised third parties.

Assigning or changing the PIN

The PIN assignment or change made on the wireless operating unit can only be done **after** the project is put into commission.

1. Press the ⚙ key and enter the factory-assigned Administrator PIN (0001).
2. With the ↓ key, navigate to "Extended Menu", then confirm by pressing the **OK** key.
3. Use the key ↓ to navigate to "User Management" and confirm with **OK**. The Administrator always comes first in the user list.
4. Select the Administrator and confirm with **OK**.
5. Select ↓ menu item "Change PIN" and confirm with **OK**.
6. Enter a new four-digit PIN.
7. Confirm with the new PIN.
8. Press the ⚙ key to exit the menu.

Sleep mode

Sleep mode

The control panel of the wireless operating unit changes to sleep mode after about 30 seconds.
Before you want to take action (turn on the power, go to the menu or info page, trigger the alarm, etc.), you can quit the sleep mode by pressing the **OK** button; i.e. the display is switched on.

General

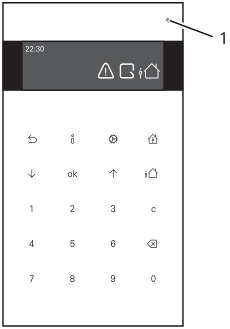
Wireless operating unit with 12-V power supply
We recommend operating the wireless control unit with the DC 12 V flush-mounted power supply (Item No. 5219 00), because all functions are then fully available.

Wireless operating unit without 12-V power supply
The wireless control unit is only supplied with power via the four internal batteries. In order to spare the battery capacity and increase the service life, the following functions are only available to a limited extent:

- Permanent illumination of the display is not possible.
- In sleep mode, alarm and fault messages are only signaled by the flashing status LED (three-second interval).

The following describes the wireless control unit with 12-V power supply and the setting "Display continously on" (also see page 31).

The Status LED



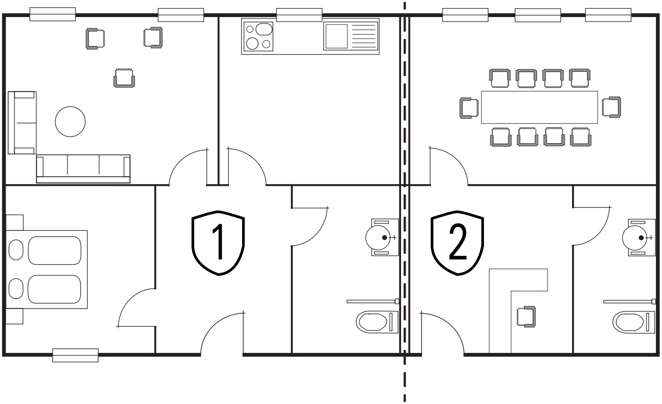
1 Status LED

Depending on the switching condition of the security area, the colours of the status LED have the following meanings:

Switching condition	LED	Meaning
Inactive	green	Everything ok
	yellow	Fault (e. g. tampering, battery low, etc.)
	red	Alarm (e. g. panic alarm, fire alarm, etc.)
Internally armed	green	Everything ok
	yellow	Fault (e. g. empty battery)
	red	Alarm (e. g. intruder, tampering, panic, etc.)
Externally armed	green	Neutral status display (normative default)

Security area

The Gira Alarm Connect security system has a maximum of four security areas. One feature of the security area is the monitoring of completed buildings or areas, each of which can be separately armed or disarmed. Unauthorised intrusion into an armed security area triggers an alarm.
Example: An object with two independent security areas (each security area has a separate entrance). The alarm control unit Connect is located in Security area 1.



Security area 1, (main security area): Main apartment with separate entrance

Security area 2
Office with separate entrance

When activating, a distinction is made between "internal activation" and "external activation".

What does "Activated internally" mean (🏠)?

"Activated internally" means that a security area is activated and people are **in the** security area. This corresponds to the so-called perimeter monitoring. Internal activation takes place, for example, on the wireless operating unit within the security area. Devices with the setting "active when externally armed" (e.g. wireless motion detectors) do **not** trigger an alarm when a detected event occurs. Devices with the setting "active when internally and externally armed" (e.g. wireless magnetic contact) trigger an alarm when a detected event occurs.

What does "Externally armed" mean (🏠)?

"Externally armed" means that a security area is armed and that **no one** is in the security area. This corresponds to the so-called indoor and perimeter monitoring. In the case of "Externally armed", a distinction is also made between the inevitability factor and the lock function.

Inevitability factor

External activation is implemented by means of the activation device (key switch/VdS **outside** of the security area). When the security area is activated, access to the security area is blocked by means of a blocking element. It is only possible to enter the security area if it has previously been deactivated using the activation device. A built-in door module implements the inevitability factor. **To avoid false alarms, the inevitability factor is recommended.**

Gateway function

External arming is carried out with the aid of the wireless control unit (**within** the security area) and correspondingly configured detectors. In this case, after entering the PIN, a defined exit delay begins during which the security area must be exited. When entering the security area, the entry delay ensures that the security area can be disarmed without first triggering an alarm.

Alarm forwarding

Alarm and alarm forwarding

Please note the following for the topic "Alarm and alarm forwarding":

- Alarm forwarding can be activated in the project and thus transferred to other security areas or remotely (e.g. via telephone) to outside persons or facilities.
- Without activated alarm forwarding or remote alarming, the alarm triggering is limited to the security area in which the alarm was triggered.

Detailed information on the topic of "alarm forwarding" and "remote alarming" can be found in the system description of the Alarm Connect security system.

Switch the security area to armed/disarmed

PIN entry

The following always applies when entering the PIN:
After entering the 4-digit PIN, the wireless control unit generates a positive or a negative acknowledgment tone as feedback.

✓ In addition, a long acknowledgment tone can be heard = PIN is correct.

✕ In addition, three short acknowledgment tones are audible = PIN is incorrect.

Arm the security area

Keep the following in mind when arming the security area:

- Close all windows and doors.
- Check on the info page whether open detectors or faults or messages are displayed (also see page 16 and page 17).
- Clear and acknowledge the faults, if necessary, going in the order they are listed.

I am at home - switch on "internally arm"

1. Press the 🏠 key and enter the user PIN.

✓ PIN correct: The 🏠 symbol appears on the Display and the 🏠 button lights up constinously yellow. The security area is switched to "Internally armed".

You can now move freely in the security area. If you still unintentionally open a secure window for example, the pre-alarm (signal tone) will sound on the wireless operating unit so that you have enough time to disarm the security area.

Disarm

1. Press the 🏠 key and enter the user PIN.

✓ PIN correct: Erase the 🏠 symbol in the display and the 🏠 button. The security area is disarmed.

I am not home - Activate "Externally armed”

Activate "Externally armed" with the gateway function

1. Press the 🏠 key and enter the user PIN.

✓ PIN correct: The 🏠 symbol appears on the display and the exit delay is activated.

2. Leave the security area before the exit delay expires and close the door.

Arming successful

✓ A long acknowledgment tone can be heard: The exit delay has expired and the safety area is now armed.

Arming unsuccessful

✕ Three short acknowledgment tones are audible: The exit delay has expired and the safety area is **not** armed. Check on the info page to see what has prevented the arming process (e.g. fault, open detector, etc).

Disarm

1. When entering the "Externally armed" security area, a pre-alarm (signal tone for the duration of the entry delay) is triggered first.
2. Enter the user PIN before the exit delay period is over. If you do not disarm the security area before the exit delay is over, an alarm is triggered.

Activate "Externally armed" with inevitability factor

Switching "external arming" on or off takes place **outside** of the security area on a key switch.

1. Leave the security area, close the door and lock it.
2. Switch the security area to "Externally armed" on the key switch.

Disarm

Disarm the security area on the key switch and enter the security area.

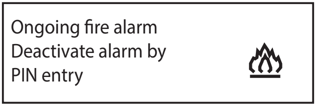
Manual alarms

Trigger alarm

Requirement: The alarm types have been activated and configured in the project.
The following alarms can be manually triggered using a three-digit code on the wireless operating unit:

- Panic alarm (factory code: 110)
- Fire alarm (factory code: 112)
- Service call (factory code: 777)

Regardless of the alarm type, the following always applies:
Enter the code for the desired alarm and confirm with the **OK** button. The corresponding alarm is activated and shown in the display (example: 112 + **OK** = fire alarm).



Ongoing fire alarm
Deactivate alarm by
PIN entry

Deactivate alarm

1. Enter the PIN.
✓ PIN correct: the alarm is deactivated.
2. Press the ℹ button: alarm type and source are displayed.
3. Confirm the message by entering a PIN.

When do I trigger the panic alarm?

Trigger the panic alarm if you are in the security area and there is sudden danger (e. g. from an intruder).

When do I trigger the fire alarm?

Trigger the fire alarm if you detect a fire and can not extinguish it yourself. The fire alarm alerts all other people in the security area.
Get yourself to safety immediately and inform the fire department.

When do I send out a service call?

Trigger the service call if you need help. The service call--according to the configuration--gives a notification, for example, that there are people in other security areas.

The presence alarm

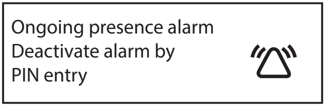
Requirement: The presence alarm function has been activated and configured in the project.

The security area user must confirm his presence within a defined time window by entering the code (factory code: 111) on the wireless control unit. If no confirmation is entered, the presence alarm is triggered.
If "Externally armed" is set in the security area, this function is automatically deactivated.

1. Enter the code and confirm with the **OK** button.

✓ Code is correct: confirmation for the time window has been made.

If no confirmation is entered within the time window, the presence alarm is triggered and the following display appears:



Ongoing presence alarm
Deactivate alarm by
PIN entry

Information page

On the information page, all current messages (alarms, faults, etc.) are displayed according to the following priority:

- Messages from another security area
- Messages about active faults that need to be cleared.
- Messages about ignored faults that must be acknowledged
- Open detectors

The i-LED

The ℹLED indicates if a message is available or if it still must be acknowledged.

ℹ LED	Meaning
off	No messages available.
flashes yellow	New, unread messages are available.
lights up yellow	Messages have already been read.
lights up green	Info page turned on.

Example

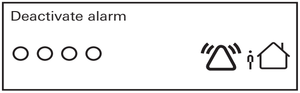
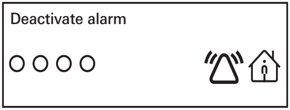
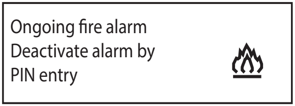
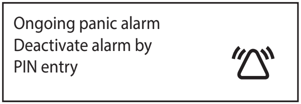
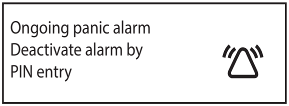
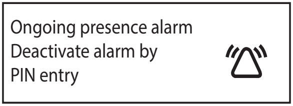
The batteries have to be changed on a wireless magnetic contact.

1. The ℹ-LED flashes yellow. Press the ℹ button: "Low battery" is displayed.
2. Open the housing of the wireless magnetic contact. The tampering contact is triggered.
3. Change the batteries in the wireless magnetic contact according to the instructions for use and close the housing again.
4. Press the ℹ button and go to the info page.
5. Acknowledge the message using the Administrator PIN.

✓ PIN correct: the message was acknowledged successfully and deleted from the info page.

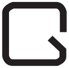
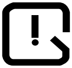
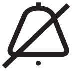
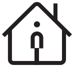
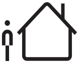
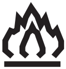
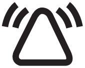
Alarm messages on the display

An active alarm message can only be deactivated by entering a PIN.
The following alarm messages could be shown in the display:

Message	Meaning
 Deactivate alarm ○○○○	**Intruder alarm under "Externally armed"**
 Deactivate alarm ○○○○	**Intruder alarm under "Internally armed"**
 Ongoing fire alarm Deactivate alarm by PIN entry	**Fire alarm**
 Ongoing panic alarm Deactivate alarm by PIN entry	**Panic alarm**
 Ongoing panic alarm Deactivate alarm by PIN entry	**Service alarm**
 Ongoing presence alarm Deactivate alarm by PIN entry	**Presence alarm**

Symbols on the display

Messages from the personal security area are shown on the display via the following symbols. Depending on the message, the symbols may appear alone or in combination.

Symbol	Meaning
	**Alarm device open** By pressing the ℹ button, the open detectors are displayed on the info page
	**Alarm device open with Bypass** "Bypass" function, see page 25.
	**Doorbell switched off** "Doorbell" function, see page 27.
	**Internally armed** The security area is switched to "Internally armed".
	**Externally armed** The security area is switched to "Externally armed".
	**Fire alarm** An active fire alarm is available or the message of an ignored fire alarm must be acknowledged on the info page.
	**Alarm** An alarm message must be acknowledged on the info page.

Symbol	Meaning
⚠	**Fault or technical message** An active fault or technical message is available or the message must be acknowledged on the info page. In addition, a signal tone (every 60 sec.) can be heard. Deactivate the signal tone by pressing any key.

Cause of the fault message	What do I have to do?
Wireless malfunction	Contact the professional company.
Weak battery	Replace the battery on the corresponding device .
Battery weak on the alarm control unit	After replenishing the power supply, wait approx. two hours (charging time of the battery pack). Display despite power supply and wait time: The battery pack is defective; contact the professional company.
Power failure	Check the fuse in distribution box. If necessary, contact the network provider or professional company.
Error - transmission path 1 or 2	Contact the professional company.
Error - telephone connection	Check the telephone connection. As required, contact your telephone provider or the professional company.
Error - mobile communications connection	Check the mobile phone card balance. If necessary, contact the network provider or the professional company.
Error - Network connection	Check the network connection. If necessary, contact the professional company.
Error - NTP time server	Check the network connection. If necessary, contact the professional company.
Error - IP module	Contact the professional company.
Tamper alarm	Check the corresponding device.
Tamper alarm due to false PIN	Enter the correct PIN.

Device monitoring alarm	Check if the device is available and within range of the control unit or the wireless repeater. The batteries might be dead. Contact the professional company.

Messages from another security area

Messages from other security areas are only shown in the display when alarm forwarding is activated.

Symbol	Number	Meaning
⊞	Not visible	The security area is either disarmed or switched to "Internally armed".
⊞ 2	Visible	The security area with the corresponding number is switched to "Externally armed".
⊞ 2	Visible, blinking	An alarm was triggered in the security area with the corresponding number. The alarm can only be turned off and acknowledged in the corresponding security area.

Change the batteries in the wireless operating unit

⚠ WARNING

Explosion hazard in case of improper handling of batteries.
Do not throw batteries into the fire, and do not recharge batteries, as this may result in a risk of explosion.

! Replacing the battery

Replace the battery as soon as the "low battery" display appears in the display of the wireless operating unit. Always change out all four batteries. Mixing new and used batteries is not permitted, as this can lead to functional damage to the wireless control unit.

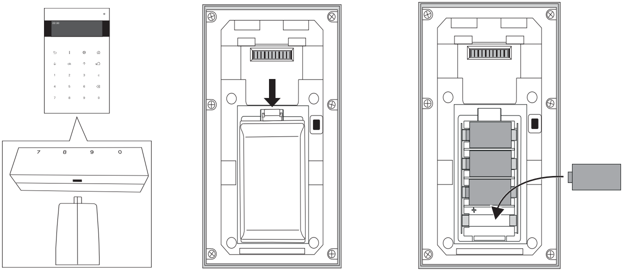
ℹ "Low battery" display

As soon as the wireless operating unit or another device reports "low battery" status, this is shown in the Display of the wireless operating unit (the ⚠ symbol appears and the ℹ button glows yellow). Press the ℹ button: the information page shows which device is showing "low battery". Use the key ↓ to check for further messages.

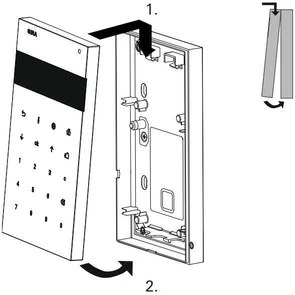
1. The wireless operating unit reports "low battery". Detach the wireless operating unit from the mounting frame using the unlocking tool (included with the alarm control unit Connect). The tamper alarm is triggered.
2. Open the lid to the battery compartment and remove all batteries.

Replacing the battery

3. Only use new and unused batteries of the same type. **Observe polarity!**



4. Attach the wireless operating unit to the mounting frame (attach from above and screw on from below) until you hear a click. Acknowledge all messages on the info page.



Technical data

Battery

Type:	CR 123A, lithium
Capacity:	> 1.4 Ah
Voltage:	DC 3 V
Quantity:	4

Settings menu

Who can access the settings menu?

Varying rights when accessing the settings menu

When accessing the settings menu, a distinction is made between the following user roles:

- Administrator (full access).
- Installer (access only after Administrator's approval).
- User without administrator rights (no full access).

Further information regarding the access rights of the individual user roles can be found in the overview on the next page.

Installer's temporary activation

The "installer" is required for the duration of the installation and maintenance of the Alarm Connect security system.

For safety reasons, the installer must be activated by the administrator on the wireless operating unit (normative specification). Deactivation of the installer takes place automatically when the security area is armed. The PIN for the installer is assigned in the GPA and can only be changed there.

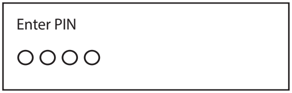
Overview of access rights

	Administrator	Installer	User
1 Bypass*	x	x	-
2 Button lock 30 seconds	x	x	x
3 Display brightness	x	x	x
4 Doorbell*	x	x	x
5 Service info*	x	x	x
6 Event memory	x	x	x
7 Extended menu	x	x	-
7.1 Date and time	x	x	-
7.2 Time display on the operation unit	x	x	-
7.3 Volume	x	x	-
7.4 Backlight	x	x	-
7.5 User management	x	x	-
7.6 Device management	x	x	-
7.7 Test run	x	x	-
7.8 Language selection	x	x	-
7.9 Software version	x	x	-
7.10 Resetting the operating unit	x	x	-

* Only visible if activated in the project.

Pull up the settings menu

1. Press the ⚙ button: The following display appears:



Enter PIN

○○○○

2. Enter the PIN.

✓ PIN correct: the settings menu opens.

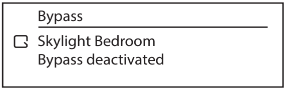
1 Enable/disable Bypass

When is the "Bypass" function required?
The "Bypass" function is always required if you want to switch the security area to "armed" despite the detector being open or the presence of an active fault message.
The example of a wireless magnetic contact on the roof window of a bedroom shows how you can activate Bypass and then arm the security area.

Device with activated Bypass

Note the following:
A device with activated Bypass is ignored by the Alarm control unit Connect.
Devices with activated Bypass always present a safety risk, since the security area can be entered at this point without triggering an alarm.
The "bypassing" of an open detector or an active fault message can only be activated by an administrator on the wireless operating unit.

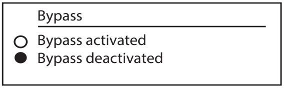
1. 1. Enter the administrator PIN and pull up the settings menu. The menu item "Bypass" displays.
2. Press the **OK** button. Next, the bypassable devices and messages (open detectors, devices with dead batteries, etc.) are displayed.
3. Use the arrow key to navigate to the device to be bypassed.



Bypass

Skylight Bedroom
Bypass deactivated

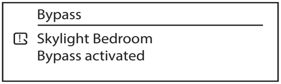
4. Press the **OK** button again. The following display appears:



Bypass

○ Bypass activated
● Bypass deactivated

5. With the ↑ key, select "Bypass activated" and press **ok** to confirm. The following display appears:

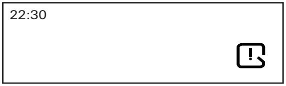


Bypass

Skylight Bedroom
Bypass activated

Repeat steps 4 to 7 for all devices or messages that are preventing arming.

6. Press the ⚙ key to exit the menu. The following display appears:



22:30

7. If faults were bypassed, the fault messages must be acknowledged on the info page.
8. The security area can now be armed, despite the detector being open.

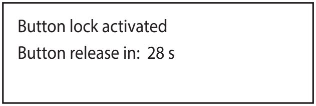
Disarming the security area will automatically disable the bypass.

2 Activate the button lock

Button lock

The button lock is used, for example, when the user wishes to clean the surface of the wireless operating unit, e.g. with a damp cloth, without accidentally pressing a button. The button lock is automatically disabled after 30 seconds.

1. Pull up the settings menu and press the ↓ key to navigate to menu item "Button lock 30 seconds".
2. Press the **OK** button. The button lock is automatically activated and the following display appears:



Button lock activated

Button release in: 28 s

3 Switch off the "Doorbell" or switch it on again

The "Doorbell" function is used to ensure that the wireless operating unit emits a signal tone to indicate when a corresponding configured wireless magnetic contact (e.g. a shop door) is opened in a disarmed security area. Turn off the doorbell function, for example, when the door will be temporarily opened more frequently (e.g. an open house or similar) and the signal tone disturbs you.

1. Pull up the settings menu and press the ↓ key to navigate to menu item "Doorbell".
2. Press **OK** and open the menu item.
3. Activate or deactivate the doorbell (default setting: activated). Confirm changes with the **ok** button. The setting selected here applies only to this wireless operating unit.
4. Press the ⚙ key to exit the menu. The deactivated doorbell is indicated by 🔕 in the display.

4 Set the Display brightness

1. Pull up the settings menu and press the ↓ key to navigate to menu item "display brightness".
2. Press **OK** and open the menu item.
3. Press the ↓ and ↑ keys to set the brightness and then confirm with **[ok]**.
4. Press the ⚙ key to exit the menu.

5 Service information

Requirement: The contact details were stored in the project.

1. Pull up the settings menu and press the ↓ key to navigate to menu item "service information".
2. Press **OK** and open the menu item.
   Here you'll find contact information of the professional company that installed the Alarm Connect security system.

6 Pull up all saved events

The event memory stores the last 250 events (alarms, fault messages, faults, etc.). The event memory can not be deleted.

1. Pull up the settings menu and press the ↓ key to navigate to menu item "event memory".
2. Press **OK** and open the menu item.
3. Press the ↓ and ↑ keys to navigate through the event memory list.
4. Press the ⚙ key to exit the menu.

7 Pull up the extended menu

1. Pull up the settings menu and press the ↓ key to navigate to menu item "extended menu".
2. Press the **OK** button and pull up the extended menu.

7.1 Change the date and time

ℹ **Changing the date and time**

The date and time can only be permanently changed on the wireless operating unit if this function has been activated in the GPA (Alarm system -> Basic settings -> Region and time) by the installer. In addition, the NTP time server must be deactivated under [Project Settings] -> [General] -> [Date and time]!

1. Pull up the extended menu and press the ↓ key to navigate to the submenu "Date and time".
2. Press **OK** and open the menu item.
3. The date and time are changed by number and confirmed by pressing **ok**.

7.2 Show or hide the time in the display

1. Pull up the extended menu and press the ↓ key to navigate to the submenu "Operating unit time display".
2. Press **OK** and open the menu item.
3. Select "enabled" or "disabled" and confirm the selection with the **OK** button. Factory default: **enabled**.
4. Press the ⚙ key to exit the menu.

7.3 Change the volume of the signal tones

Signal tones on the wireless operating unit

The volume of the signal tones for the following functions can be set on the wireless operating unit:

- **Alarms**
- **Note and acknowledgment** (entry and exit delay/positive and negative acknowledgment/fault message)
- **Doorbell**
- **Button actuation and PIN entry**

1. Pull up the extended menu and press the ↓ key to navigate to the submenu "Volume".
2. Press **OK** button and open the list of functions.
3. Press the ↓ key of the function to be changed and press **OK** to confirm.
4. Press the ↓ and ↑ keys to set the volume and confirm with **ok** .
5. Press the ⚙ key to exit the menu.

7.4 Change the switch-off delay of the backlight/permanently switch on or off the display

1. Pull up the extended menu and press the ↓ key to navigate to the submenu "Backlight".
2. Press **OK** and open the menu item. Press the ↓ key and select one or both of the submenus.

Switch-off delay
This determines after how many seconds (from 10 to 240 seconds) the backlight is switched off automatically.
The time is changed using the ↓ and ↑ keys and then confirmed with the **OK** key. Factory default: **30 seconds**

Display continuously on (only possible with connection to the power supply)
Select "enabled" or "disabled" and confirm the selection with the **OK** button. Factory default: **disabled**.
As soon as the display is permanently switched on, the switch-off delay only applies to the background illumination of the buttons on the control panel.

7.5 Assign, change or reset the user PIN and deactivate or activate users

The stored user names are shown in the submenu "User management".

Assign or change user PIN

The following users need their own four-digit PIN:

- The Administrator.
- The installer (can only change the PIN in the GPA).
- Any user with or without administrator rights.
- The security guard (only if alarm forwarding to a security service has been activated in the project).

1. Pull up the extended menu and press the ↓ key to navigate to the submenu "User management", then confirm by pressing **OK**.
2. Press the ↓ key and select a user; then press **ok** to confirm.
3. Press the ↓ key to navigate to "Change PIN" and confirm with **ok**.
4. nter a 4-digit PIN that has not yet been assigned.
5. Confirm with the new PIN.

Reset the User PIN

1. Repeat steps 1 to 2 in the chapter "Assigning a user PIN".
2. Press the ↓ key to navigate to "Reset PIN" and confirm with **ok**.
3. Confirm with an Administrator PIN.

Deactivating or reactivating the user

1. Repeat steps 1 to 2 in the chapter "Assigning a user PIN".
2. Press the ↓ key to navigate to "User status" and confirm with **ok**.
3. Select "enabled" or "disabled" and confirm the selection with the **OK** button.

7.6 Deactivating or reactivating the wireless hand-held transmitter

Requirement: at least one wireless hand-held transmitter is connected to the Alarm control unit Connect).

1. Pull up the extended menu and press the ↓ key to navigate to the submenu "Device management" then confirm **by pressing** OK. The list of wireless hand-held transmitters is displayed.
2. Press the ↓ key and select a wireless hand-held transmitter; then press **ok** to confirm.
3. Select "enabled" or "disabled" and confirm the selection with the **OK** button.
4. Press the ⚙ key to exit the menu.

7.7 Change the menu and the display language

1. Pull up the extended menu and press the ↓ key to navigate to the submenu "Language selection" , then press **OK** to confirm. The list of languages will be displayed. Factory default: **German**.
2. Press the ↓ key to select another language and confirm with **ok**. The following languages are available: German, English

7.8 Carry out the test operation

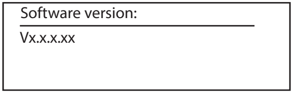
Activate and deactivate the test mode

Detailed information on the topic of "test mode" can be found in the system description of the Alarm Connect security system.

1. Disarm all security areas.
2. Remove the housing cover (see BDA of the alarm control unit Connect). The tamper alarm is triggered.
3. Pull up the extended menu and press the ↓ key to navigate to the submenu "Test mode" , then press **OK** to confirm.
4. Activate the test mode and press **OK** to confirm.
5. Carry out the test operation. Deactivation takes place in the same way.

7.9 Check the software version of the wireless operating unit

1. Pull up the extended menu and press the ↓ key to navigate to the submenu item "Software version".
2. Press the **ok** button. The software version is displayed.



Software version:

Vx.x.x.xx

7.10 Resetting the wireless operating unit

You can reset all local settings (e. g. set display brightness, volume, etc.) in the central system.

1. Pull up the extended menu and press the ↓ key to navigate to the submenu "Reset operating unit" , then press **OK** to confirm.
2. Enter the PIN.

All local settings are reset to factory settings.
The connection to the Alarm control unit Connect remains in place.

What do you do if...

the PIN is not accepted when the PIN is assigned?
When the PIN is assigned, only 4-digit PINs may be assigned that are not yet assigned in the system. The PIN might already be taken. Select another PIN.

... the PIN is not accepted when entered?
When entering a PIN, only 4-digit PINs stored in the system may be used. You might not have permission for this security area.
Contact a user with administrative rights.

Note the following: You can enter an incorrect PIN five times in a row without triggering an alarm. After the sixth incorrect entry, "Tamper alarm due to incorrect PIN" will be triggered. If a valid PIN is entered, the alarm will be deactivated again.

...manually no alarm can be triggered?
The manual alarms have been activated and configured in the project.
Contact the professional company and have the appropriate alarm activated and configured in the project.

... the menu item "Bypass" is not visible?
The menu item "Bypass" is only visible to users with administrator rights and if the bypass function has been activated in the project. Contact a user with administrator rights or contact the professional company and have the bypass function activated.

... the extended menu can not be pulled up?

- You might not have permission to access the extended menu with your PIN. Contact a user with administrative rights.
- Check to see if another security area is armed. In this case, access to the extended menu is not possible. Disarm any other security area.

Licence agreement

LICENSEAGREEMENT

Contents:

I. Usage of Gira security system Alarm Connect Software License Agreement

Hereafter, the terms of contract between the Gira, Giersiepen GmbH & Co KG, Dahlienstraße 12, 42477 Radevormwald („Licensor“) and you („Licensee“) as a user of a Gira security system Alarm Connect (consisting of the hardware and the associated Firmware) are explained for the usage of the contractual object software.

You are declaring your consent with the terms of this agreement through the acceptance of this agreement and by installing the Gira security system Alarm Connect or the operationalization of Gira security system Alarm Connect.

1 Contractual Object

This agreement is applicable for the software of a Gira security system Alarm Connect provided to the licensee by the licensor. Namely, this comes to include the installation and update tools software as well as the provided written or electronic documentation. This software for Gira security system Alarm Connect (also subsequently referred to as Alarm Connect) will be preinstalled on the units for the licensee.

Important Notice about Open Source Software:

The Alarm Connect Software contains open source software components (hereafter referred to as „OSS"). An overview as to the included OSS in the Alarm Connect software is documented in Part II of this document and the complete license text is included in Part III. This license agreement can be accessed from http://www.legal.gira.com/AlarmConnect_license_en_v1.rtf

The licensee is permitted to use the OSS according to the concerned license agreement of the respective OSS. The license agreement of the respective OSS takes precedence to the specified license in part I with regard to the usage of the OSS.

Provided that the OSS license agreement necessitates the provision of OSS source code, the licensor will submit an offer for the delivery of the corresponding source codes to the licensee and third parties on request within 36 months after conclusion of contract against payment of the shipping costs after invoicing by the Licensor.

2 Rights of Usage of Gira Alarm Connect Software

2.1 The licensor allows the licensee the non-exclusive (not an exclusive), non-transferable and non-sublicense right, without time limitation, to use the Alarm Connect software on the Alarm Connect central unit and the Alarm Connect keypad pursuant this agreement in the valid version of the documentation (the documentation is in printed form or will be made available as online help or online documentation) for the named reasons and scope of application.

2.2 The licensee is not permitted to use, copy, edit or transfer Alarm Connect software either completely or partially in another manner as described in this contract or documentation. The creation of one (1) copy, which is made for archiving or backing up purposes, is excluded.

2.3 The licensee is not permitted to reverse engineer Alarm Connect software or to transform it in another form. Such techniques include disassembling (conversion of binary coded machine commands of an executable program in a human-readable assembly language) or decompiling (conversion of binary coded machine or assembly commands in source code in the form of high-level language commands) unless such use is exceptionally permitted by reason of the limitations of copyright law.

2.4 The licensee is not permitted to transfer Alarm Connect Software with or without payment without the consent of the licensor. The licensee agrees to use the Alarm Connect Software solely for the purpose of the right of use within this usage license.

The licensee is only permitted to transfer the Alarm Connect software and the license key for the usage of the software to third parties, if (i) the licensee has removed the Alarm Connect software, backup copies, and the required license key from the licensee's system by either deletion or deinstallation, and (ii) before the transfer and use, the third party has committed itself to Gira in the conformity of the terms of use. Before transferring Alarm Connect unit, the licensee will explicitly notify the third party about the terms of use.

The licensee's right to individual use lapses when transferred to third parties.

2.5 The licensee is not permitted to rent out, lease or grant sublicenses Alarm Connect Software, which were granted to the licensee within the framework of this agreement of the granted rights of use.

2.6 The licensee requires the licensor's prior written consent, if the licensee intends to develop and distribute which is derived from Alarm Connect Software.

2.7 The mechanisms of Alarm Connect Software's license management and copy protection are not allowed to be analyzed, published, circumvented, or deactivated.

2.8 All rights not explicitly granted to the licensee in this agreement explicitly remain with the licensor.

3 Changes by the Licensor

The licensor retains the right to expand upon, improve or modify, at any time and without notice, the Alarm Connect Software including documentation. These actions can be alternatively conducted by a third party. This license agreement is applicable pursuant to later versions of the software.

4 Guarantee for Alarm Connect Software

4.1 The Alarm Connect Software and the documentation (either provided in printed form or, as well, as online documentation) will be provided to the licensee as amended. The period of the guarantee for the Alarm Connect Software is 24 months. Guarantee compliance will be performed through the sending of a replacement. The legal right to withdraw remains unaffected. The restrictions of the guarantee rights do not apply if the licensee is a consumer pursuant § 13 BGB.

The Licensor does not provide any guarantee for the included OSS in the Alarm Connect software. This does not affect the guarantee for the Alarm Connect software as a whole or more specifically the functioning of the OSS within the Alarm Connect software.

4.2 The guarantee does not include errors arising from improper usage or other causes outside the sphere of influence of the licensors.

5 Liability

The licensor is not liable for damages arising from lost profit, loss of files or other financial losses, which occured within the framework of using Alarm Connect software. This limitation of liability applies for all claims of damages by the licensee regardless of legal basis. Liability is limited in amount to the product’s purchase price. This limitation of liability does not apply to damages which have caused by intent or gross negligence on behalf of the licensor, the licensor’s agent or other persons who aided in the fulfilling of the contract.

Furthermore, the exclusion of liability does not apply for damages arising from injury to life, limb and health and for assumed guaranties (guarantee liability) by the licensor.

Claims from the licensees remain unaffected from the exclusion of liability, which. Such obligations are significant contractual duties. Their breaching would put the purpose of the contract into danger and, therefore, the contractual partner places its trust in its fulfillment.

6 Data Protection

Through conclusion of these license agreements, you agree to the validity of Gira’s data protection
notices in its valid version respectively.

Please refer to http://www.gira.de/impressum/datenschutz.html

7 Applicable Law und Jurisdiction

This contract is subject to the laws of the Federal Republic of Germany under exclusion of the UN Convention on Contracts for the International Sale of Goods (CISG). This choice of law enables the consumer the application of the law of country of the consumer's habitual residence; under the law, that country may not deviate from the agreement.

The jurisdiction is the competent court of the licensor's location. This does not apply if the licensee is not a merchant, not a legal entity under public law and a special fund under public law, or, insofar, the licensee does not have a general jurisdiction within the Federal Republic of Germany.

8 Collateral Agreements and Changes to the Contract

Collateral agreements und changes to contract require to be in written for validity. This license agreement is issued both in German and English. Thereby, the English version serves only as information. In case of an unclarity or should disputes arise from the contract, the German version is binding the version.

9 No participation in the Consumer arbitration (Verbraucherschlichtung) pursuant VSBG

The licensor does not participate in the consumer arbitration
(Verbraucherschlichtung) at a consumer arbitration office
(Verbraucherschlichtungsstelle) pursuant consumer arbitration law
(Verbraucherstreitbeilegungsgesetz (VSBG)).

- End of Segment I. –

II. List of Open Source Software in Gira security Alarm Connect Software

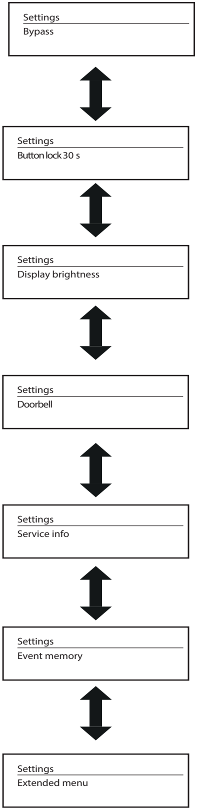
Software package	SW version	Source	License type
avahi	0.6.31	http://www.avahi.org/download	LGPLv2.1+
boost	1.65.1	http://downloads.sourceforge.net/project/boost/boost/1.65.1	BSL-1.0
busybox	1.23.2	http://www.busybox.net/downloads	GPLv2
bzip2	1.0.6	http://www.bzip.org/1.0.6	bzip2 license
codesynthesisxsd	3.3.0	https://downloads.ise.de	GPLv2 FLOSS
dbus	1.8.20	http://dbus.freedesktop.org/releases/dbus	AFLv2.1 or GPLv2+
dosfstools	3.0.28	https://github.com/dosfstools/dosfstools/releases/download/v3.0.28	GPLv3+
dropbear	2015.67	http://matt.ucc.asn.au/dropbear/releases	MIT, BSD-2c-like, BSD-2c
eeprog	0.7.6	http://www.codesink.org/download	GPLv2+
expat	2.1.0	http://downloads.sourceforge.net/project/expat/expat/2.1.0	MIT
fatfs	all	http://elm-chan.org/fsw/ff/00index_e.html	1-clause BSD
gdb	7.8.2	http://ftp.gnu.org/pub/gnu/gdb	GPLv2+ LGPLv2+ GPLv3+ LGPLv3+
htop	1.0.3	http://hisham.hm/htop/releases/1.0.3	GPLv2
infozip	3.0	ftp://ftp.info-zip.org/pub/infozip/src	Info-ZIP v2007-Mar-4
iostat	2.2	http://www.linuxinsight.com/files	GPLv2
json-spirit	4.06	https://downloads.ise.de	MIT
kmod	2.2.10	https://www.kernel.org/pub/linux/utils/kernel/kmod	LGPLv2.1+
libdeamon	0.14	http://0pointer.de/lennart/projects/libdaemon	LGPLv2.1+
libffi	3.1	ftp://sourceware.org/pub/libffi	MIT

libglib2	2.44.1	http://ftp.gnome.org/pub/gnome/sources/glib/2.44	LGPLv2.1+
libpcap	1.7.4	http://www.tcpdump.org/release	BSD-3c
libupnp	1.6.19	http://downloads.sourceforge.net/project/pupnp/pupnp/libUPnP%201.6.19	BSD-3c
libxmlsec1	1.2.18	http://www.aleksey.com/xmlsec/download	MIT
libxml2	2.9.2	ftp://xmlsoft.org/libxml2	MIT
libxslt	1.1.28	ftp://xmlsoft.org/libxslt	MIT
linux	3.2.20	https://github.com/torvalds/linux/blob/master/COPYING	GPLv2 with Linux-syscall-note
log4cplus	1.1.2	http://downloads.sourceforge.net/project/log4cplus/log4cplus-stable/1.1.2	Apache-2.0
memtester	4.3.0	http://pyropus.ca/software/memtester/old-versions	GPLv2
mtd	1.5.2	ftp://ftp.infradead.org/pub/mtd-utils	GPLv2
ncurses	5.9	http://ftp.gnu.org/pub/gnu/ncurses	MIT with advertising clause
netcat	0.7.1	http://downloads.sourceforge.net/project/netcat/netcat/0.7.1	GPLv2+
openssl	1.0.2p	http://www.openssl.org/source	OpenSSL or SSLeay
pcre	8.37	ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre	BSD-3c
popt	1.16	http://anduin.linuxfromscratch.org/sources/BLFS/svn/p	MIT
screen	4.2.1	http://ftp.gnu.org/pub/gnu/screen	GPLv3+
ser2net	2.10.0	http://downloads.sourceforge.net/project/ser2net/ser2net	GPLv2+
sftpserver	openssh-6.0p1	http://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable	BSD-3c BSD-2c Public Domain
socat	2.0.0-b8	http://www.dest-unreach.org/socat/download	GPLv2
tcpdump	4.7.4	http://www.tcpdump.org/release	BSD-3c

tree	1.6.0	http://mama.indstate.edu/users/ice/tree/src	GPLv2+
uboot	2010.06	https://github.com/u-boot/u-boot/blob/master/Licenses/README	GPLv2
uboot-tools	2015.04	ftp://ftp.denx.de/pub/u-boot	GPLv2+
util-linux	2.26.2	https://www.kernel.org/pub/linux/utils/util-linux/v2.26	GPLv2+, BSD-4c, libblkid and libmount LGPLv2.1+, libuuid BSD-3c
websocketpp	0.7.0	https://github.com/zaphoyd/websocketpp	BSD
xerces	3.1.2	http://archive.apache.org/dist/xerces/c/3/sources	Apache-2.0
zeromq	4.0.5	http://download.zeromq.org	LGPLv3+ with exceptions
zlib	1.2.8	http://downloads.sourceforge.net/project/libpng/zlib/1.2.8	zlib license

Brief overview

Settings menu



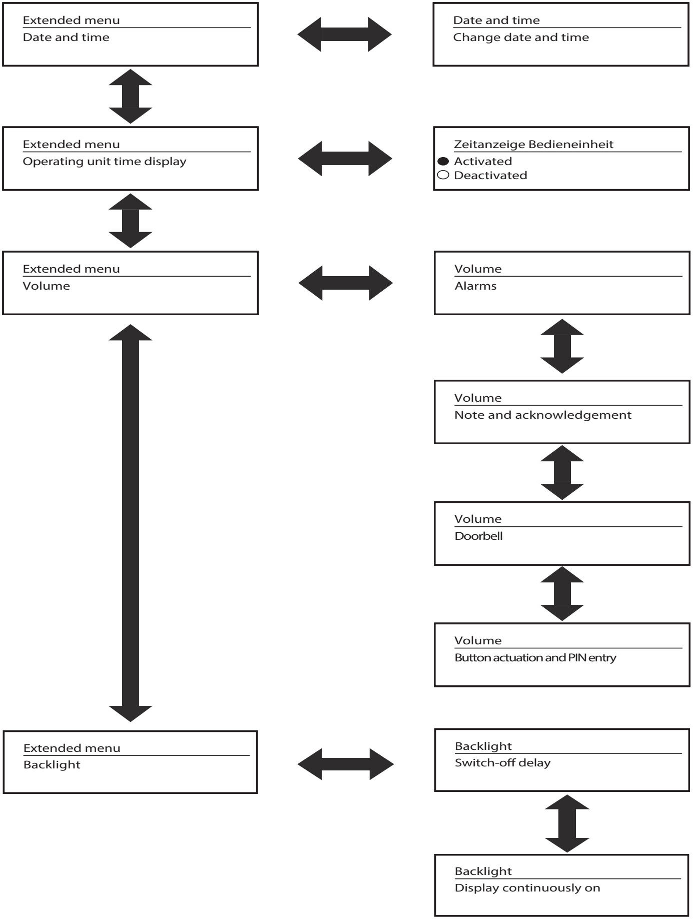
Function must be activated at the project. Only visible for Administrator / Installer.

Function must be activated at the project.
Then visible for all.

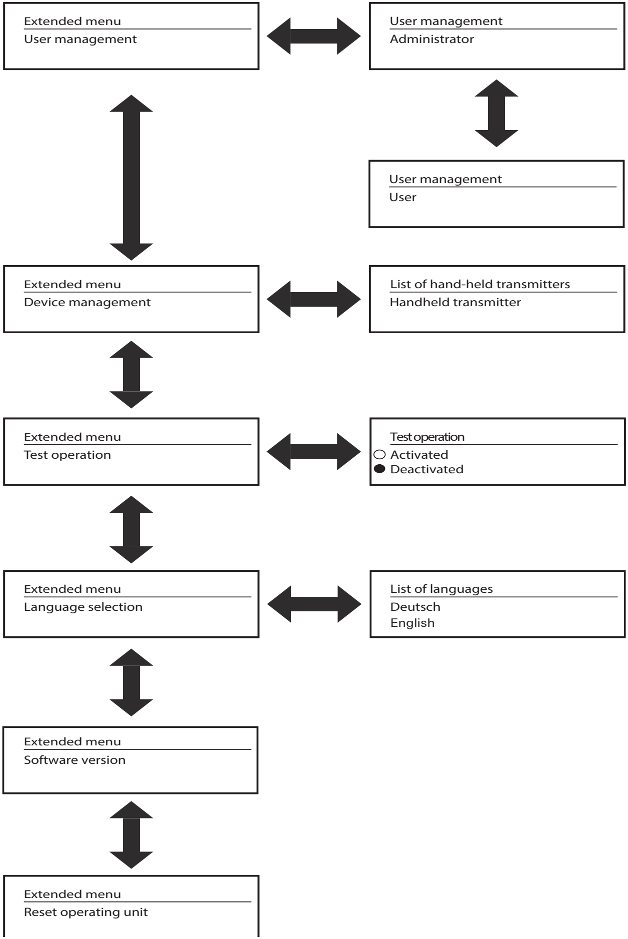
Display only visible if corresponding date are stored in the project.

Only visible for Administrator / Installer.

Extended menu



Brief overview — Extended Menu



Symbol	Meaning
◻	Detector open — also see page 18
◻!	Detector open with Bypass — also see page 18 and page 25
🔕	Doorbell switched off — also see page 27
🚨	Alarm — also see page 18
🔥	Fire alarm — also see page 18
⚠	Fault/Technical message — also see page 19
1:2 3:4	Message from another security area — also see page 20
⌂	Status display: "Internally armed" — also see page 18
i⌂	Status display: "Externally armed" — also see page 18
√	Positive feedback — also see page 11
X	Negative feedback — also see page 11

Button	Meaning
↩	- Settings menu/Info page: Jump back to the level/leave the view
i	Pull up the info page — also see page 16
⚙	Pull up the settings menu — also see page 23
⌂	Switch on "Internally armed" — also see page 12
↓	Navigate down
ok	Confirm entry/selection
↑	Navigate up
i⌂	Switch on "Externally armed" — also see page 13
C	- In case of PIN entry: Cancel - In case of "Internally armed" or "Externally armed", switch to: Cancel
⌫	- Settings menu/Info page: Jump back to the level/leave the view - In case of PIN entry: delete individual numbers)
0-9	Numbers for PIN or code entry

←

Gira
Giersiepen GmbH & Co KG
Electrical installation
systems
P.O. Box 1220
42461 Radevormwald
Germany
Phone: +49 2195 602 - 0
Fax: +49 2195 602 - 191
info@gira.com
www.gira.de

10863913 27/18

Legal notice
Picture credits:
schmitz Visuelle
Kommunikation, Title

GIRA