

Secvest IP

wireless alarm centre

Installation and operating instructions (UK)

1. Contents

1.	Contents	1
2.	Preface	2
3.	Conformity	2
4.	Meaning of the symbols	3
5.	Important safety information	3
6.	Scope of delivery	7
7.	Compatibility with ABUS products	7
8.	Installation	8
9.	Installation of the backup battery (backup power supply)	9
10.	Display and setting elements	10
11.	Labelling the Secvest IP	14
12.	Putting into operation	14
13.	Enclosed software	15
14.	Configuration of the web server	16
15.	Teaching the wireless components	43
16.	Resetting an alarm	48
17.	Notes on maintenance	49
18.	Technical data	50
19.	Customer service and support	51
20.	Explanation of terms	51

2. Preface

Dear customer,

Many thanks for your purchase of this Secvest IP wireless alarm centre. This product is built according to state-of-the-art technology. 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-sc.com). To ensure safe operation, it is your obligation to observe these instructions! If you have any questions, please contact your local specialist dealer. No part of the product may be changed or modified in any way.

These instructions contain important installation and operation information. Store these instructions in a safe place for future reference. These instructions are part of the product. Bear this in mind if you pass the product on to others.

Disclaimer:

These operating instructions have been produced with the greatest care. Should you discover any missing information or inaccuracies, please contact us under the address shown.

ABUS Security-Center GmbH does not accept any liability for technical and typographical errors, and reserves the right to make changes to the product and operating instructions at any time and without prior warning.

We reserve the right to make changes to these instructions without prior notice. No forms of guarantee are accepted for the contents of this document.

© ABUS Security-Center GmbH & Co. KG, 12/2010

3. Conformity

The declaration of conformity can be ordered from:

ABUS Security-Center GmbH & Co. KG
Linker Kreuthweg 5
86444 Affing
GERMANY
www.abus-sc.com
info@abus-sc.com

4. Meaning of the symbols

Disposal as per directive WEEE 2002/96 EC



At the end of its useful life, dispose of the product according to the applicable legal requirements. Within the EU, the product and its accessories must be collected and disposed of separately. Devices displaying this symbol may not be disposed of as domestic waste. Please contact your dealer or dispose of the products at the local collection point for electronic waste.



This symbol indicates important notes in these operating instructions, which must be observed.



This symbol indicates special tips and notes on the operation of the unit.

5. Important safety information

5.1 Intended use

Only use the device for the purpose which it was designed and built for. Any other use is considered inappropriate.

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

- This three-zone IP wireless alarm centre is used in combination with connected wireless detectors, signallers, actuators and operating units for object surveillance.

5.2 General

Before using the device for the first time, read the following instructions carefully and pay attention to all warnings, even if you are already familiar with electronic devices.



Warning

All guarantee claims become invalid for damage caused by non-compliance with these operating instructions.

We cannot be held liable for resulting damages.



Warning

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

All guarantee claims are invalid in such cases.

Keep this manual in a safe place for future reference.

If you pass on or sell the device, you must also include this user manual. This device has been manufactured in accordance with international safety standards. Inspect the device before putting it into operation. If the device shows signs of damage, do not put it into operation.

5.3 Power supply

- Only operate this device through a power source which supplies the mains power specified on the type plate of the FU3819 power supply unit.
- If you are unsure of the power supply at the installation location, contact your power supply company.
- Only operate this device with the device-specific FU3819 power supply unit.
- This device uses Safety Extra Low Voltage (SELV). The circuits of the switch outputs and the 13.8 V power supply also fall into this voltage range. SELV is a low electrical current that offers special protection against electric shocks based on its low level and insulation compared to higher voltage circuits.



Warning

The installation of additional equipment or modification of the device invalidates your guarantee if not carried out by trained personnel.

Your guarantee is invalidated in the event of improper installation of additional equipment or modifications.

5.4 Overloading/overvoltage

- Avoid overloading of mains sockets, extension cables and adapters as this can result in fires or electric shocks.
- Use overvoltage protection to prevent damage caused by overvoltage (e.g. electrical storms).

5.5 Cables

- Always hold cables by the connector, and do not pull the cable itself.
- Never touch the mains cable with wet hands, as this can lead to a short circuit or electric shock.
- Never position the device, furniture or other heavy items on the cable. Ensure that the cable does not become kinked, especially on the connector and sockets.
- Never knot the cable, and do not tie it to other cables.
- All cables should be laid so that they cannot be stepped on or cause an obstruction.
- A damaged mains cable or power supply unit can cause a fire or electric shock. Check the mains cable from time to time.
- Do not modify or manipulate the mains cable or plug.
- Do not use plug adapters or extension cables that do not conform to the applicable safety standards, and do not make alterations to power supply cables or mains cables.

5.6 Installation location/operating environment

- Install the device on the wall and do not place any objects in front of it.
- The device is not designed for operation in rooms subject to high temperatures or moisture (e.g. bathrooms), or in excessively dusty rooms.
- Operating temperature and ambient humidity:
-10°C to +55°C, maximum 75% relative humidity. The device may only be operated in moderate climate conditions.

Ensure the following:

- Sufficient ventilation must always be guaranteed – leave a gap of at least 10 cm from all sides.
- The device must not be exposed to direct heat sources (e.g. heaters).
- The device must not be exposed to direct sunlight or strong artificial light.
- The device must not be placed in close proximity to magnetic fields (e.g. loudspeakers).
- Naked flames (e.g. candles) must not be placed on or near the device.
- Contact with spraying or dripping water and aggressive liquids must be avoided.
- The device must not be operated in close proximity to water, and must not be submerged under any circumstances (do not place objects containing water on or near the device, such as vases or drinks).
- Foreign objects must not penetrate the device.

- The device must not be exposed to strong variations in temperature, as this can lead to condensation and electrical short circuits.
- The device must not be exposed to excessive jolts or vibrations.

5.7 Care and maintenance

Maintenance is necessary if the device has been damaged. This includes damage to the plug, mains cable and housing, penetration of the interior by liquids or foreign objects, exposure to rain or moisture or when the device does not work properly or has fallen.

- Disconnect the device from the mains power supply before maintenance (e.g. cleaning).
- If smoke develops or unusual noises or odours are detected, then pull the mains plug from the socket immediately and remove the backup battery. In such cases, the device should not be used until it has been inspected by a qualified technician.
- Clean the device housing with a damp cloth.
- Do not use solvents, white spirit or thinners as these can damage the surface of the device.
- Do not use any of the following substances:
 - Salt water, insecticides, solvents containing chlorine or acids (ammonium chloride) or scouring powder.
- Gently rub the surface with a cotton cloth until it is completely dry.

5.8 Accessories

- Only connect devices that are suitable for the intended purpose. Otherwise, hazardous situations or damage to the device can occur.

5.9 Putting into operation

- Observe all safety and operating instructions before putting the device into operation for the first time.
- Only open the housing during installation and when training the wireless components.



Warning

If in doubt, have a specialist technician carry out assembly, installation and connection of the device.

Improper or unprofessional work on the mains power supply puts both you and other persons at risk.

5.10 Children and the device

- Do not allow children access to electrical devices. Never allow children to use electrical devices without supervision. Children may not be able to accurately detect possible risks. Small parts can be life-threatening if swallowed.
- Keep batteries away from small children. Call for medical assistance immediately if a battery is swallowed.
- Keep packaging materials away from children (danger of suffocation).
- This device should not be used by children.

6. Scope of delivery

Individual alarm centre:

1 x Secvest IP wireless alarm centre

1 x FU3919 power supply unit

1 x BT2020 backup battery

1 x 1 metre network cable (TVAC40800)

1 x CD-ROM (installation and operating instructions, Secvest IP Finder, labelling templates)

1 x installation material (4 x wall plugs, 4 x screws)

1 x battery cable

2 x cable clips

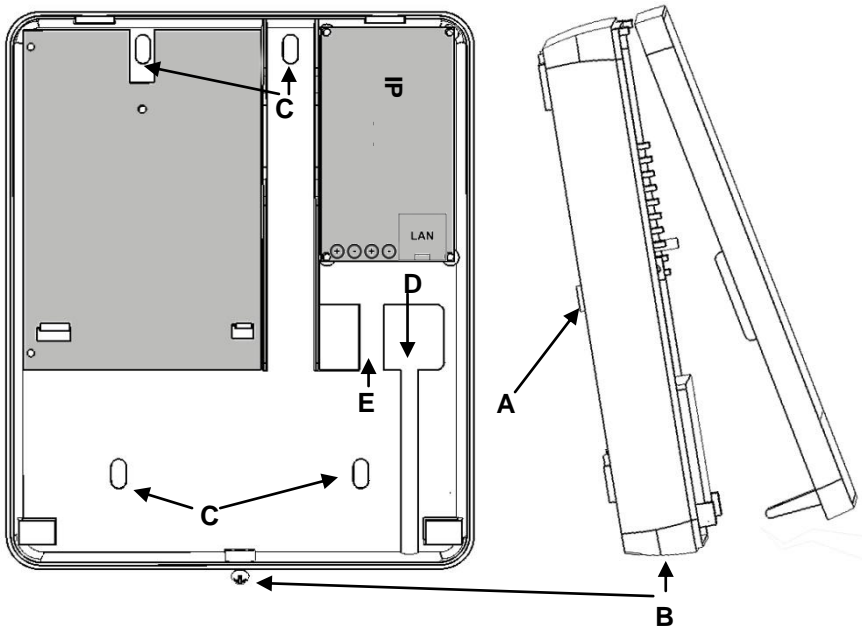
7. Compatibility with ABUS products

Compatible	
CASA10010	IP alarm module
FU59xx	Secvest Key 2WAY wireless cylinder
FU8100	Secvest 2WAY wireless remote control
FU8130	Secvest 2WAY wireless additional lock (7010E)
FU8140	Secvest 2WAY wireless additional lock (7025E)
FU8150	Secvest wireless remote control
FU8200	Secvest 2WAY wireless info module
FU8210	Secvest 2WAY wireless universal module (repeater function)
FU8230	Secvest 2WAY wireless indoor siren
FU8240	Secvest wireless socket
FU8300	Secvest 2WAY wireless panic alarm
FU8305	Secvest 2WAY wireless panic transmitter
FU8310	Secvest 2WAY wireless fire alarm
FU8320W/B	Secvest 2WAY wireless magnetic contact
FU8321W/B	Secvest 2WAY wireless magnetic contact
FU8330	Secvest 2WAY wireless flood detector
FU8340	Secvest 2WAY wireless smoke detector
FU8350	Secvest 2WAY wireless motion detector

FU8360	Secvest 2WAY animal-immune wireless motion detector
FU8370	Secvest 2WAY wireless glass breakage detector
FU8380	Secvest 2WAY wireless vibration detector
FU8390	Secvest 2WAY wireless emergency transmitter
FU841xW/B	FTS 96 E wireless window lock
FU842x	Secvest 2WAY wireless window bar lock (FOS550E)
FU8430	Secvest 2WAY wireless window handle (FG350E)
TVIP41550	PIR network camera

Not compatible	
FU8110	Secvest 2WAY wireless control unit
FU8165	Secvest 2WAY wireless key switch
FU8220	Secvest 2WAY wireless outdoor siren

8. Installation

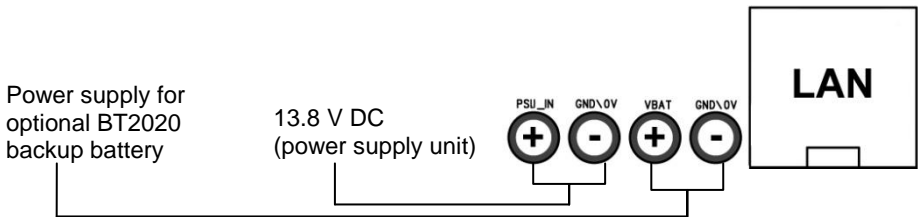


Key:

- A) Wall tamper switch
- B) Housing screw
- C) Fixing holes on base plate
- D) Cable opening
- E) Tension relief (bar for fastening cable to cable clip)

Installation procedure:

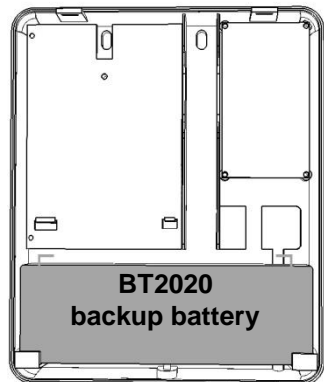
1. Loosen the housing screw on the bottom narrow side and open the housing.
2. Using the back of the housing as a template, mark the drill holes (C).
Drill the holes for the fixing screws.
3. Guide the connection cable through the appropriate opening (D).
4. Connect the power supply to the terminal block with the correct polarity (grey dashed wire is positive).
5. Connect the LAN cable (see following diagram).



6. Fasten the 13.8 V cable and LAN cable to the appropriate tension relief using the supplied cable clips.
7. Fix the housing to the wall.
8. Make sure the spring of the wall tamper switch (A) is positioned correctly.
9. Make the appropriate settings on the web server.
10. Train the wireless components.
11. After training, replace the housing cover and tighten the cover screw.

9. Installation of the backup battery (backup power supply)

1. Disconnect the alarm centre from the power supply.
2. Connect the supplied cable for the battery to the IP module.
Red is the positive terminal and black is the negative terminal. See the installation section for more details.
3. Connect the battery correctly.
4. Insert the battery into the appropriate battery clip and close the housing. See the installation section for more details.







Trained wireless components and programming are not lost in the event of a power failure.








10. Display and setting elements

10.1 Display LEDs

The display consists of 10 LEDs

	<p>Green LED ("Power" LED) for monitoring the power supply</p> <ul style="list-style-type: none"> • Permanently lit: Power supply is OK • Flashing with 1 Hz: Mains power supply failure; only indicated if a backup battery is in use.
	<p>Red LED ("Trouble" LED) for displaying faults</p> <ul style="list-style-type: none"> • Off: No faults • Flashing with 1 Hz: Supervision fault (detector or device is indicated by the channel LED flashing with 1 Hz. If only this LED flashes, this indicates that the alarm centre itself has been tampered with). • Permanently lit: Indicates jamming.
	<p>Blue LEDs ("Channel" LEDs) for detector status display</p> <ul style="list-style-type: none"> • Off: Detector OK (closed) • Permanently lit: Detector is open or has triggered (open); operating units are lit briefly indicating that a wireless signal has been received. • Flashing with 5 Hz: Empty battery on a wireless component • Flashing with 1 Hz: Wireless component has been tampered
	<p>Bottom blue LED lights up: Indicates that this refers to the second caption level (i.e. channels 8–14).</p>

10.2 LED table

		Layer 1		Layer 2			
Zone 1		Lights up/ flashes	Channel 7	Lights up/ flashes	Channel 14	Zone 3	
		Lights up/ flashes	Channel 6	Lights up/ flashes	Channel 13		
		Lights up/ flashes	Channel 5	Lights up/ flashes	Channel 12		
		Lights up/ flashes	Channel 4	Lights up/ flashes	Channel 11		
Operating units <small>(Secvest Key remote control)</small>		Lights up/ flashes	Channel 3	Lights up/ flashes	Channel 10	Zone 2	
		Lights up/ flashes	Channel 2	Lights up/ flashes	Channel 9		
		Lights up/ flashes	Channel 1	Lights up/ flashes	Channel 8		

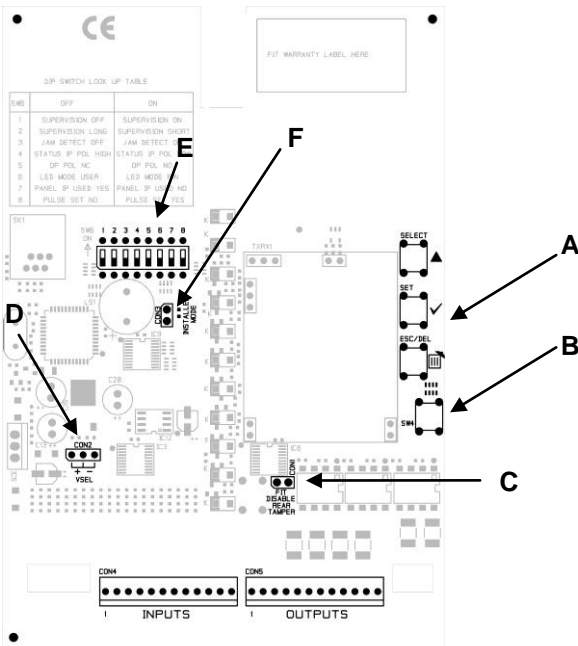
	Does not light up	Lights up
---	-------------------	-----------

10.3 Acoustic signal

The alarm centre can also signal the various states and error messages acoustically:

1 x beep	Centre was deactivated
2 x beep	Centre was activated
8 x beep	System error (tampering, jamming, supervision)

10.4 Setting elements on the wireless PCB



10.4.1 Programming keys (A)

On the right, there are three keys (SELECT, SET, ESC/DEL) for training and programming the wireless components.



10.4.2 Tamper switch

A cover tamper switch (**B**) and a wall tamper switch protect the alarm centre from unauthorised opening and removal from the wall.

10.4.3 CON1

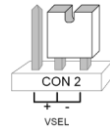
CON1 (**C**) jumper connection “FIT DISABLE TAMP”.

If you set the jumper on both contacts, you deactivate the wall removal contact. (This may be helpful during programming.)



10.4.4 CON2

CON2 (**D**) jumper must be in the “-” position (factory setting).



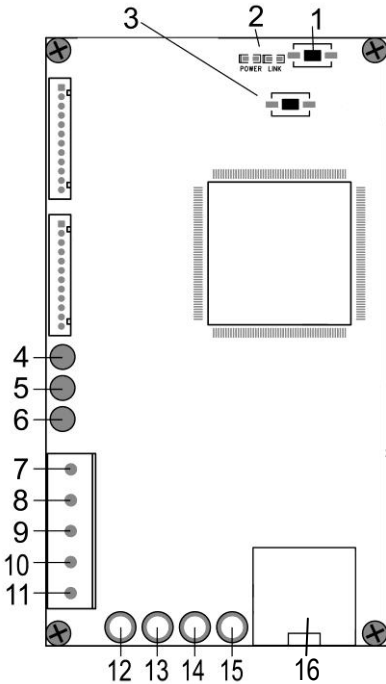
10.4.5 DIP switch SW6

DIP switch SW6 (**E**) is factory-set as follows.

The individual switches of this 8-position DIP switch enable you to choose from the following options. Switch positions 4/5/7/8 must remain in the factory settings to guarantee correct functionality.

Switch	Options	Factory setting	“OFF” position	“ON” position
1	Supervision	ON	Off	On
2	Supervision time	ON	Long 3 hours	Short 20 min
3	Jamming detection	ON	Off	On
4		OFF		
5		ON		
6	LED mode	OFF	Display on	Display off
7		OFF		
8	Acoustic signal	ON	Off	On

10.5 Setting elements and connections on the IP board



- 1. System reset button
- 2. Status LEDs
- 3. Network reset button
- 4. NO
- 5. NC
- 6. COM
- 7. Burglary
- 8. Fire
- 9. Panic
- 10. DSL monitoring
- 11. 0 V
- 12. + terminal for FU3819 power supply unit
- 13. – terminal for FU3819 power supply unit
- 14. + terminal for BT2020 battery connection
- 15. – terminal for BT2020 battery connection
- 16. LAN network connection

10.6 Relay and transistor outputs

The relay output allows wired components to be switched.
Maximum switching power: 1,25A ; 60VDC

The transistor outputs are used for connecting an optional GSM dialler.
Switching power: 1A/200mA

11. Labelling the Secvest IP

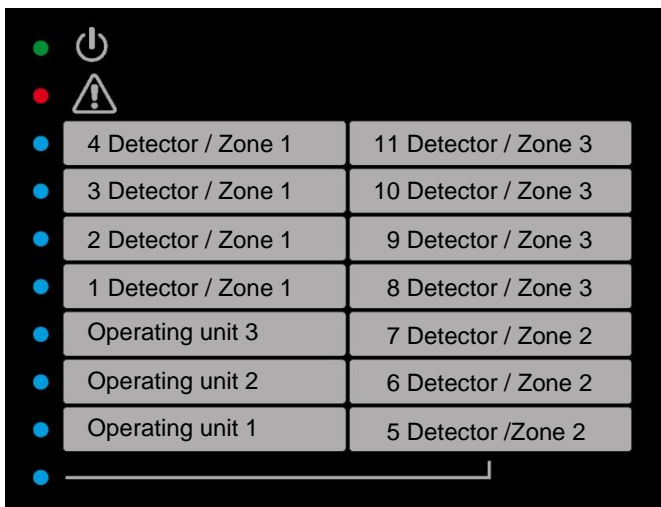
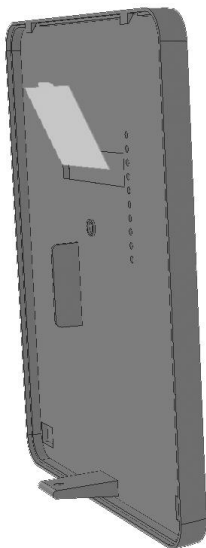
We recommend using the editable PDF on the supplied CD for labelling your Secvest IP, or downloading the PDF for the corresponding product from our website. Labelling the device is very simple. Enter your individual component settings in the PDF and print it out. Insert the cut-out label into the corresponding gap on the inner side of the cover.



We recommend using common, easy-to-understand abbreviations for the detector type (e.g. MC = magnetic contact, MD = motion detector, SD = smoke detector, VD = vibration detector, GD = glass breakage detector, FD = flood detector).

Next, describe the location where the detector is found.

This helps to identify the detector quickly and easily in the event of malfunctions (e.g. empty battery). Remember that the name must correspond to the actual programming.



12. Putting into operation

Connect the alarm centre directly to your computer using a LAN (cross-over) cable, or connect it to your network using a LAN cable. The factory-set IP address on the alarm centre is 192.168.0.50.

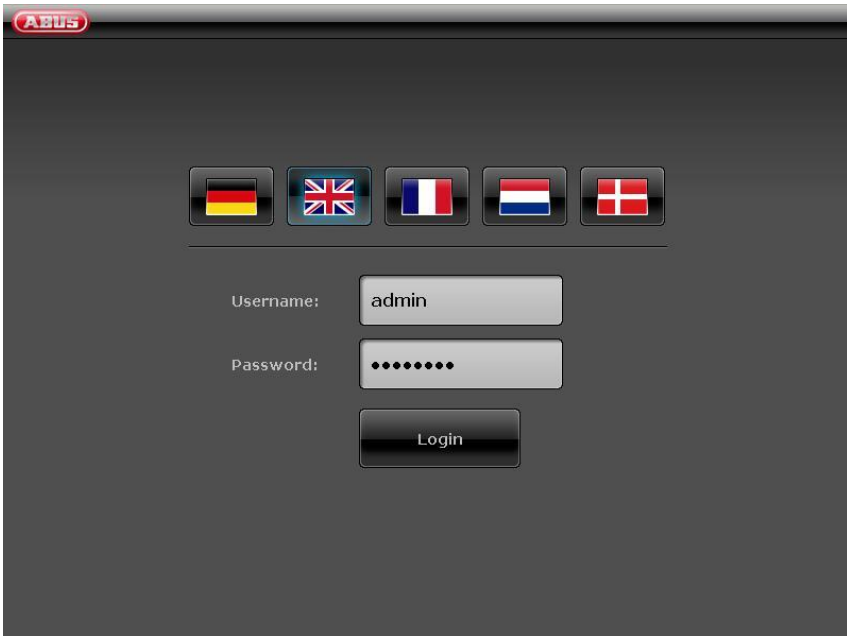
14. Configuration of the web server

When accessing the Secvest IP over your web browser, you can configure the Secvest IP using the integrated web server in the alarm centre.

14.1 Login

In order to change the settings on the Secvest IP using the web server, you must first log in to the web server as follows:

1. Select your language
2. Enter your user name (default: "admin")
3. Enter the password (default: "12345678")
4. Click on "Login"

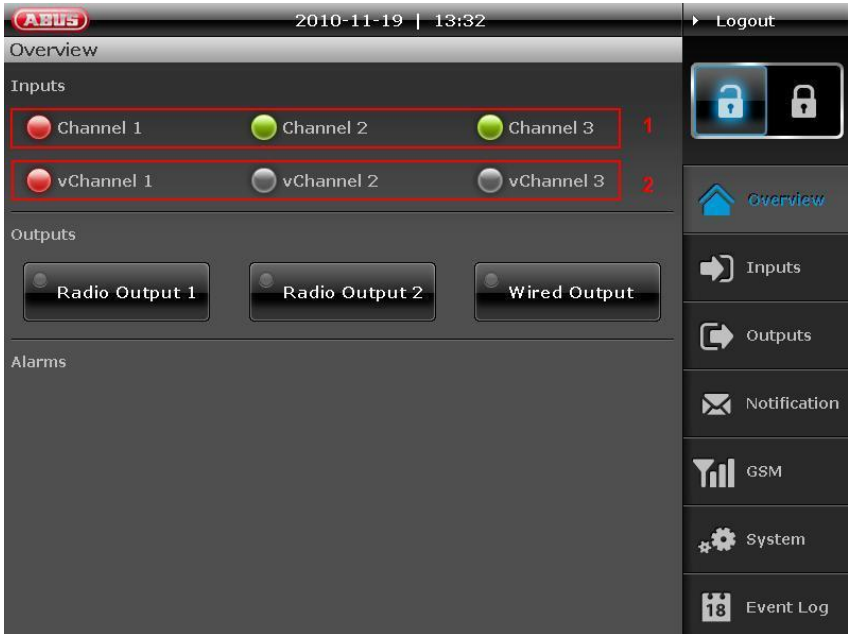


If the user name and password are entered correctly, the "Overview" screen is accessed.

14.2 Overview

The “Overview” screen shows the current status of the Secvest-IP alarm centre, and is divided into **three areas**:

1. Inputs:



In the **Inputs** area, you will see an overview of the state of the three wireless zones (1) and three virtual IP zones (2).

The colour of the respective LED signalises the current status of the zone:

- **Green** indicates that all detectors in the corresponding zone have not been triggered or are closed.
- **Red** indicates that one or more detectors in the corresponding zone have been triggered or are open.
- **Grey** indicates a deactivated or hidden zone, or a zone where no detectors are connected.

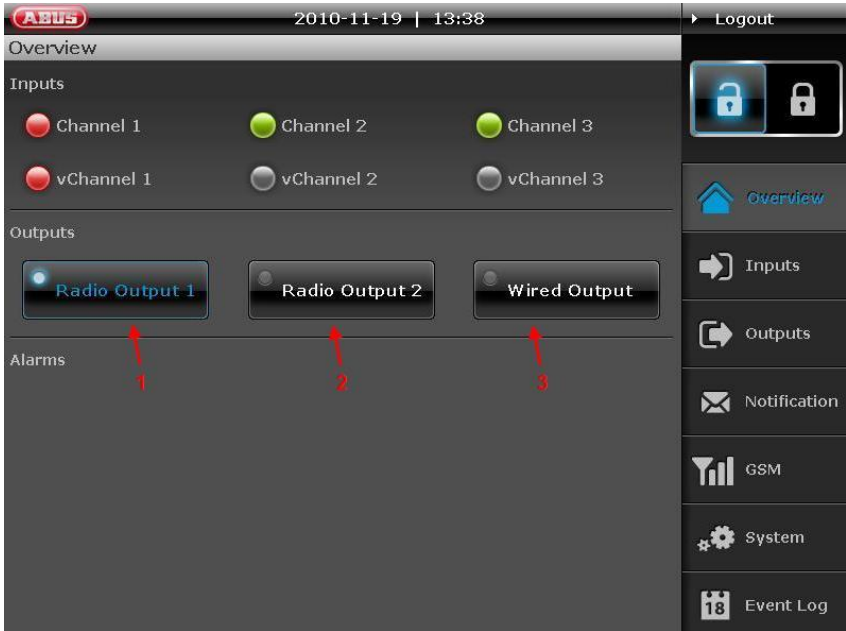
Bypass a channel via the Overview Menu

In the Input area you also can easily bypass a channel. This function allows you to take out one channel with its learned detectors, so that these will not trigger any alarm. If you set bypass for a channel, this will be valid for the next activation of the alarm panel.



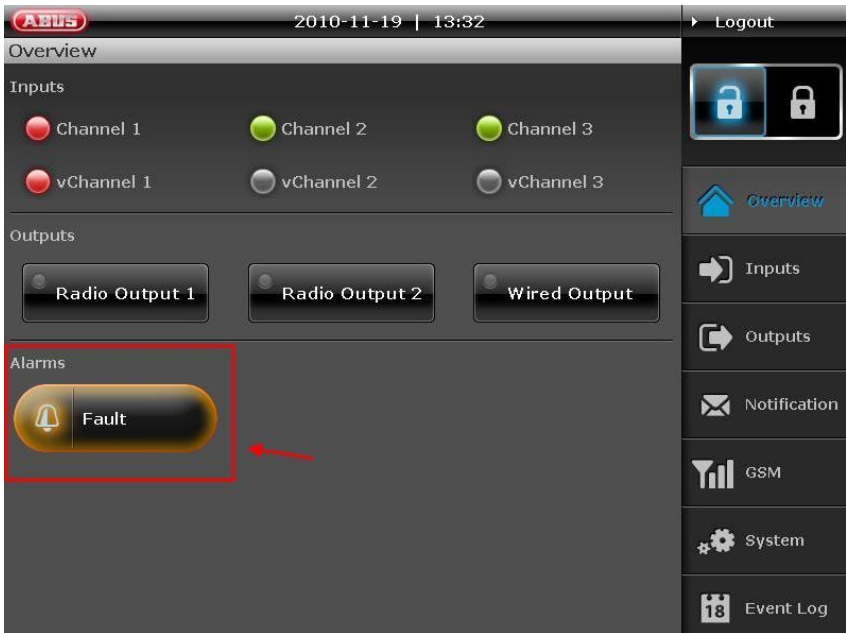
To bypass a channel, click on the **Status-LED** of the channel you want to bypass. (like shown in the screen shot). Tick the bypass button to **“On”** and click **“Apply”**. The Status-LED will turn gray. If you would like to undo the bypass, so click again on the Status LED and choose **“Off”** and also click **“Apply”** to confirm. If you set a channel on Bypass **“On”**, this channel will not detect any alarm for the next activation of the alarm panel. After the next deactivation, the channel will be automatically set on bypass **“Off”**.

2. Outputs:



The **Outputs** area lets you switch the two wireless switching outputs (1 and 2) and the relay output (3). The current status can also be determined at this time. If the LED on the button lights up and the lettering has a blue background, this indicates that the output is currently switched on (see (1)).

3. Alarms:



The **Alarms** area is used to indicate whether any alarms are present (and if so, which ones).

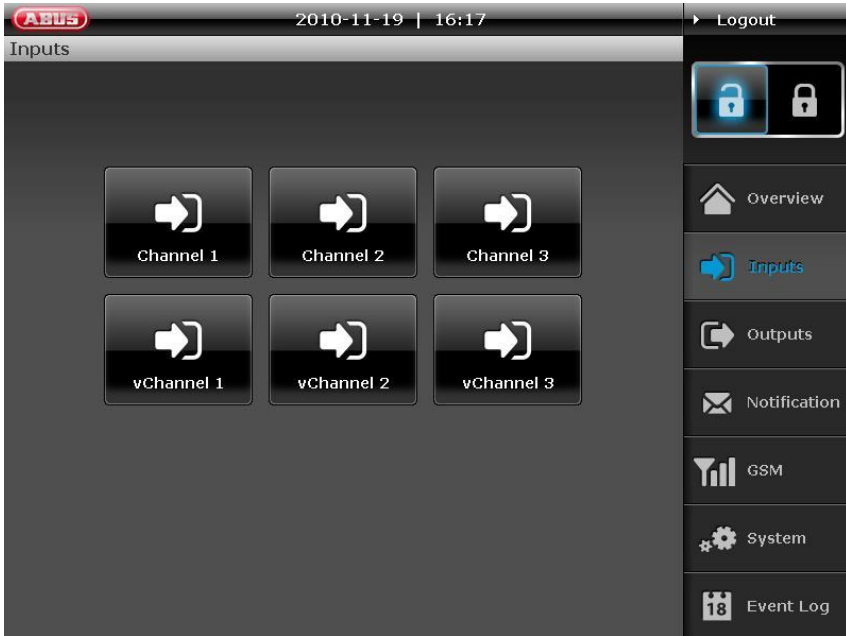
Possible Alarms:

- Burglary
- Fire
- Panic
- Fault
 - Jamming
 - Supervision
 - Tamper
- Technical

14.3 Inputs

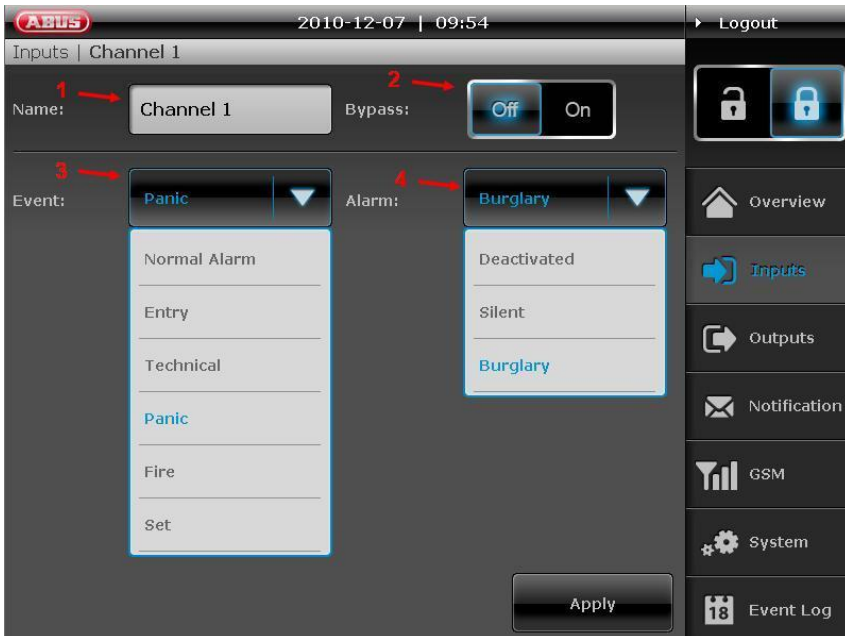
Name the inputs according to the detectors that you want to train. Select the attributes and the associated alarm type.

To go back to a higher level menu from a submenu, press the corresponding buttons on the selection bar on the right.



The following options can be defined:

14.3.1 RF-Inputs



1. **Name:** Name of the zone/specification whose name is used in the zone display in the “Overview” menu.
2. **Bypass (on/off):** The selected zone is hidden (i.e. zones can be deactivated). This function can be used to bypass specific zones and their detectors, when necessary (e.g. when the detector indicates an empty battery or a detector in the zone cannot be connected). The bypass is only activated for one arming procedure, and is then automatically reset.
3. **Event (zone attribute):** Zones can have very different attributes. The assignment is made according to the type of trained detectors on the zone. The detector sends an alarm notification to the alarm centre, which then triggers a reaction depending on the set event properties and alarms.

The following alarm events can be defined:

- **Normal Alarm:** When the alarm centre is activated, this zone triggers a burglar alarm if one of the detectors has been triggered. Good examples for this zone attribute include the training of *motion detectors*, *magnetic contacts* or *PIR network cameras*.
- **Technical:** One of the zones with this attribute triggers a technical alarm when the alarm centre is deactivated and activated. Use this zone type for *flood detectors*, for example.

- **Fire:** This zone always triggers an alarm, irrespective of whether the alarm centre is activated or deactivated. Use this zone attribute when *smoke detectors* have been trained here.
 - **Entry:** If the burglar alarm centre is active, this zone triggers an alarm following a specified delay time (entry delay). This zone attribute can be used for a *magnetic contact* on the entrance door.
 - **Set/Unset:** A zone can be used for activation and deactivation with this zone attribute.
 - **Panic:** This zone always triggers an alarm, irrespective of whether the burglar alarm centre is activated or deactivated. Train *panic detectors* on this zone, for example.
4. **Alarm (alarm reaction of the zone):** Definition of which reaction is triggered by an incoming event.
- **Deactivated:** *Alarm is deactivated*, the event does not trigger an alarm.
 - **Burglary:** *Burglar alarm* – can be signalled by an optical or acoustic signaller. A corresponding alarm notification is also sent by e-mail, depending on the settings.
 - **Fire:** *Fire alarm* – alarm is made by siren as pulsed alarm tone. A corresponding alarm notification is also sent by e-mail, depending on the settings.
 - **Silent:** *Silent alarm* – in the event of a silent alarm, the connected acoustic and optical signalling devices are not activated. The alarm notification is only sent by e-mail, depending on the settings.
 - **Technical:** *Technical alarm* – alarm made by siren. A corresponding alarm notification is also sent by e-mail, depending on the settings.
- To complete the configuration, click **Apply**.

14.3.1.1 Virtual Inputs (vChannel)

In the area of the virtual Inputs you can make all settings regarding the IP devices (e.g. PIR-IP-camera). Like at the RF-Inputs it is possible to bypass these channels and also select the event with the specific alarm.

The screenshot shows the configuration page for a virtual input (vChannel 1) in the ABUS web interface. The page title is "Inputs | vChannel 1". The interface includes a "Logout" button in the top right corner. The main configuration area contains the following fields and controls:

- Name:** A text input field containing "PIR IP", with a red arrow pointing to it labeled "1".
- Bypass:** A toggle switch currently set to "Off", with an "On" option.
- Type:** A dropdown menu showing "PIR IP Camera".
- Event:** A dropdown menu showing "Normal Alarm".
- Alarm:** A dropdown menu showing "Burglary".
- Address:** A text input field containing "192.168.0.12", with a red arrow pointing to it labeled "2".
- Port:** A text input field containing "80", with a red arrow pointing to it labeled "3".
- Username:** A text input field containing "root", with a red arrow pointing to it labeled "4".
- Password:** A password input field with masked characters, with a red arrow pointing to it labeled "5".
- Apply:** A button at the bottom right of the configuration area.

The sidebar menu on the right includes the following items: Overview, Inputs (highlighted in blue), Outputs, Notification, GSM, System, and Event Log.

1. Name the virtual Channels. This is the name which is shown in the overview screen.
2. Please enter here the IP address of the device you wanted to add.
3. Please enter here the network-port of the device you want to add.
4. Please enter here the username of the device you want to add.
5. Please enter here the password of the device you want to add.

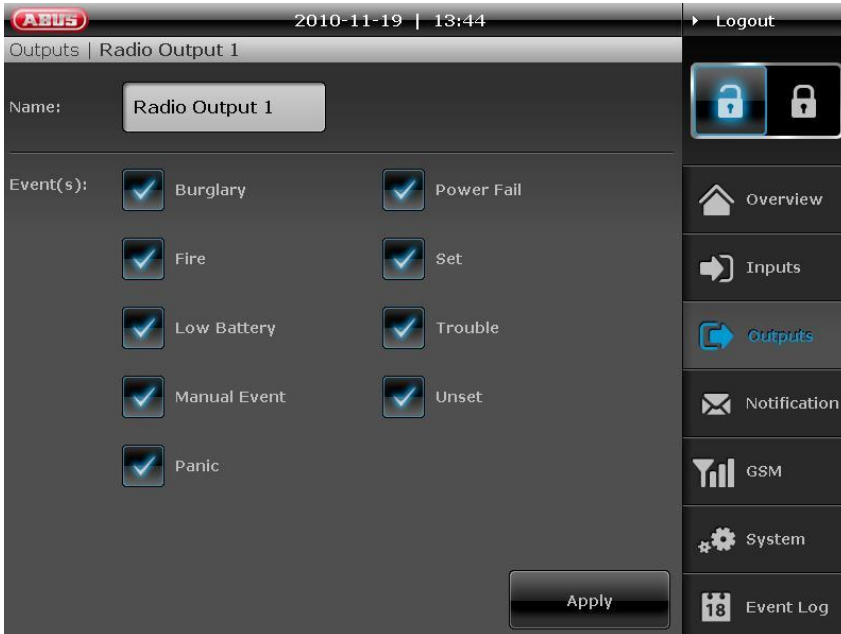
To confirm your settings, please press "Apply"

14.4 Outputs



Name the outputs according to their wireless programming and link them to events.

Example: Radio Output 1, which controls a wireless socket with is connected to a light, this will be switched on in case of an alarm.



By ticking the boxes under “Event(s)”, the user has the option of specifying which events switch the outputs (e.g. so that the light is switched on). The following events can be selected.

- Burglary
- Fire
- Low Battery
- Manual Event (must be ticked on in order to enable manual operation via “Overview”-Screen).
- Panic
- Power Fail
- Set (Radio Output activates, when alarm centre is activated)
- Trouble
- Unset (Radio Output activates, when alarm centre is deactivated)

To complete the configuration, click **Apply**.

14.5 Notification

In this menu, you specify the settings and rules for e-mail notifications.



The “Notification” menu is divided into four areas, which can then be used to adjust the notification function to your own requirements.

1. E-Mail Account

The screenshot shows the 'E-Mail Account' configuration page in the ABUS web interface. The top bar displays the ABUS logo, the date and time '2010-11-19 | 16:19', and a 'Logout' button. The main content area is titled 'Notification | E-Mail Account' and contains the following fields and options:

- Name:** Max Mustermann
- E-Mail:** max.mustermann@
- Outgoing Mail Server:** smtp.web.de
- Port:** 25
- Use authentication
- Username:** max.mustermann@
- Password:** [masked with dots]
- Use secure connection(TLS)

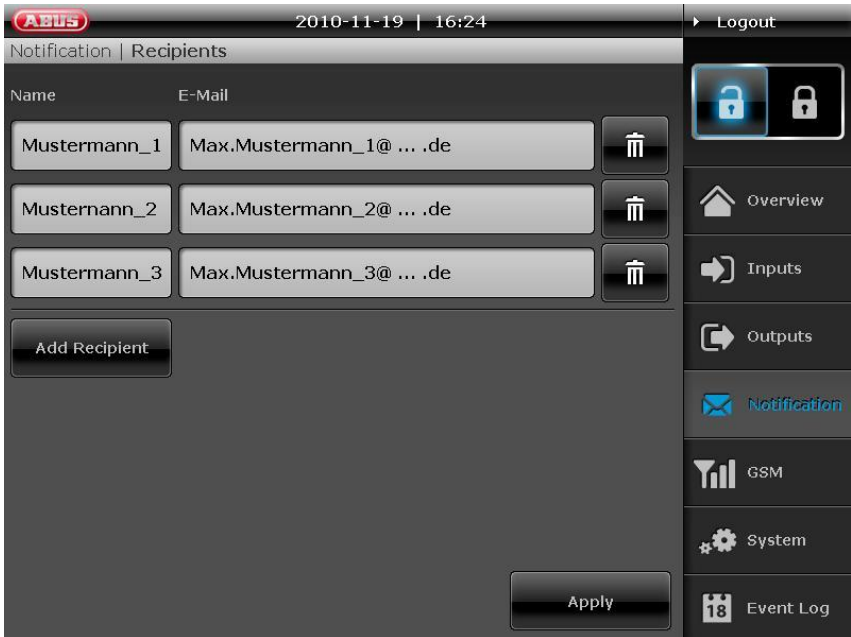
An 'Apply' button is located at the bottom right of the form. On the right side, there is a vertical sidebar with navigation icons and labels: Overview, Inputs, Outputs, Notification (highlighted in blue), GSM, System, and Event Log. At the top of the sidebar, there are two lock icons, one of which is highlighted in blue.

The “E-Mail Account” area is used to enter the data of the account from which notifications are sent in the event of an alarm. Aside from the name and e-mail address, the contact information of the outgoing mail server, user name and password of the e-mail account must be entered. The address of the mail server and the port number can be found on the homepage of your e-mail provider. The settings are saved by clicking **Apply**.

2. Messages

Text messages for the respective event type can be stored under the “Messages” menu item. These messages are then sent automatically to the corresponding e-mail addresses in the event of an alarm. To add a message, click “Add Message”. A subject (e.g. “Burglary!”) and a text (e.g. “A burglary has been committed!”) can now be entered. A message can be deleted by clicking the waste bin icon. After all settings have been made and a message has been set for each event, the settings are then saved by clicking the **Apply** button.

3. Recipients



This menu item is used to enter one or more e-mail addresses where a message is sent in the event of an alarm.

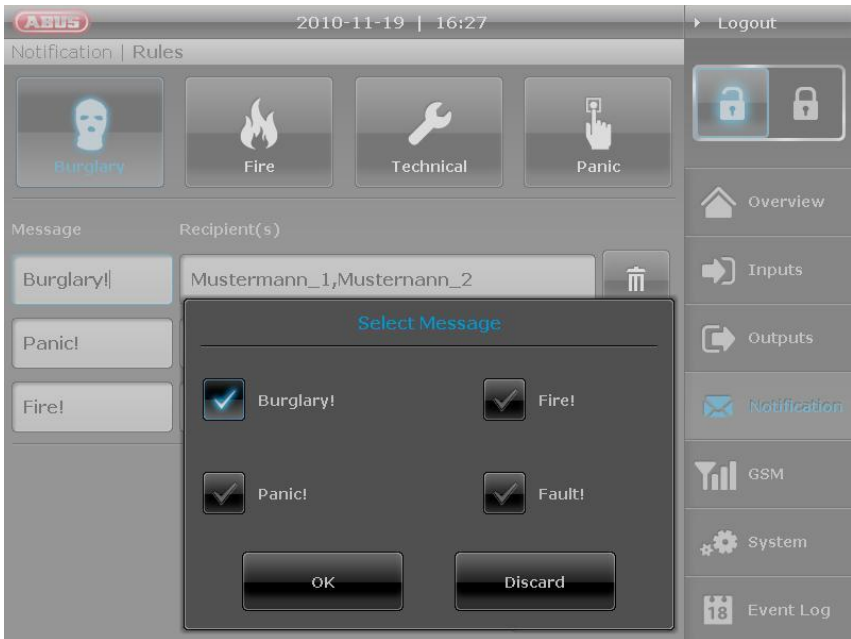
To add a new e-mail address, click on “Add Recipient” and enter the name and e-mail address of the recipient. Repeat this process until all of the required recipients have been entered. Confirm the settings by clicking the **Apply** button.

4. Rules

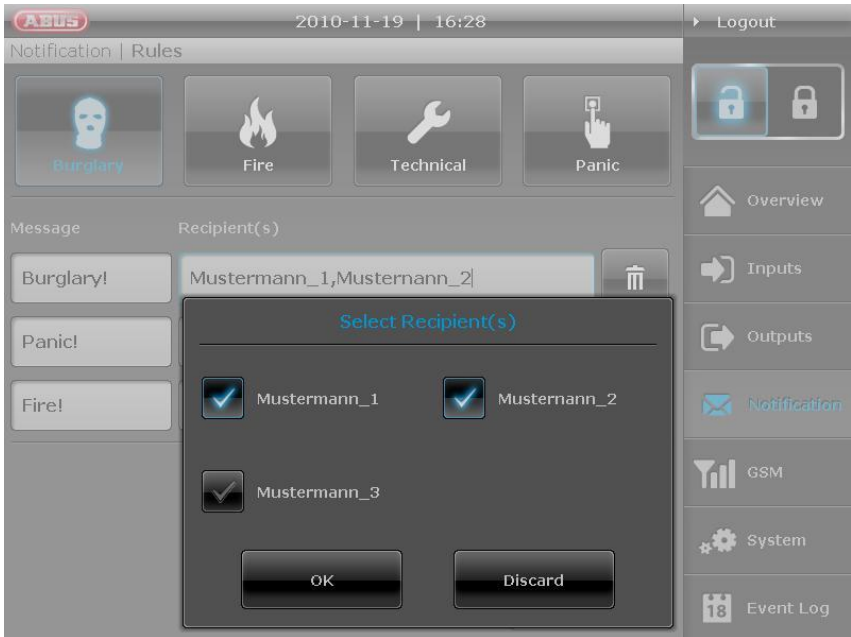
The screenshot displays the 'Rules' configuration page in the ABUS alarm system. At the top, the status bar shows 'ABUS' and the date/time '2010-11-19 | 16:26'. The main interface is divided into a top navigation bar with 'Notification | Rules', a central rule configuration area, and a right-hand sidebar. The central area features four event categories: 'Burglary' (person icon), 'Fire' (flame icon), 'Technical' (wrench icon), and 'Panic' (hand icon). Below these is a table with columns for 'Message' and 'Recipient(s)'. Three rules are listed: 'Burglary!' with recipients 'Mustermann_1, Mustermann_2'; 'Panic!' with recipient 'Mustermann_3'; and 'Fire!' with recipients 'Mustermann_2, Mustermann_3'. Each rule has a trash icon for deletion. An 'Apply' button is at the bottom right. The sidebar on the right includes 'Logout', 'Overview', 'Inputs', 'Outputs', 'Notification' (highlighted), 'GSM', 'System', and 'Event Log'.

This menu item is used to define rules by which a message and one or more recipients are clearly assigned to each event (alarm). Click an event for which a rule should be created (e.g. "Burglary"). A new rule is then created by clicking "Add rule".

Click in the empty message field.



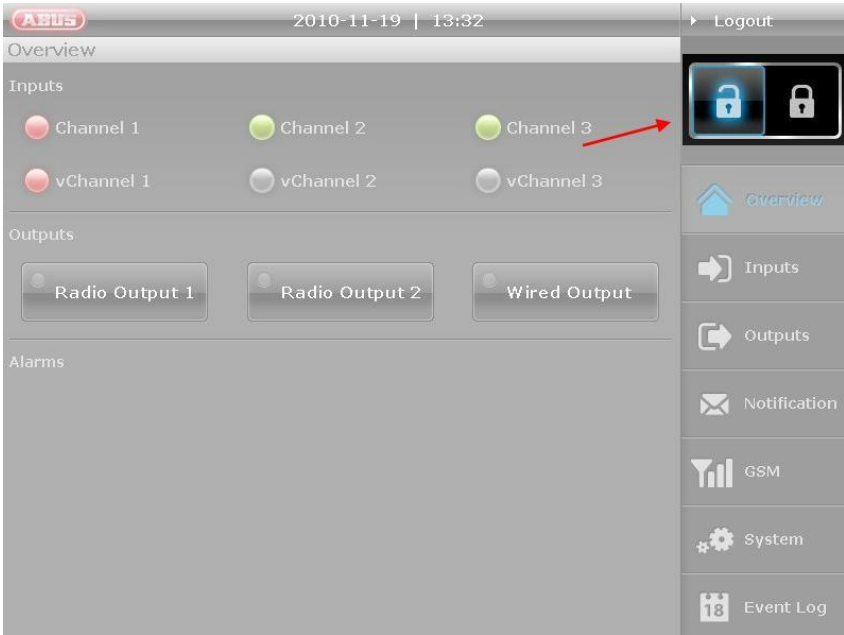
One of the previously saved messages can then be selected and assigned to the “Burglary” event in the window which opens (“Select Message”). Confirm your selection by clicking “OK”. Recipients must now be assigned to the defined message for the “Burglary” event by clicking the empty “Recipients” line.



The recipient can be selected by ticking the box in the window which opens (“Select Recipient(s)”) and then confirmed by clicking “OK”. All changes must be confirmed by clicking “Apply”, otherwise the settings are lost.

14.6 Activating/deactivating the alarm centre

These buttons let you activate/deactivate the control centre (guard mode “on” or “off”).



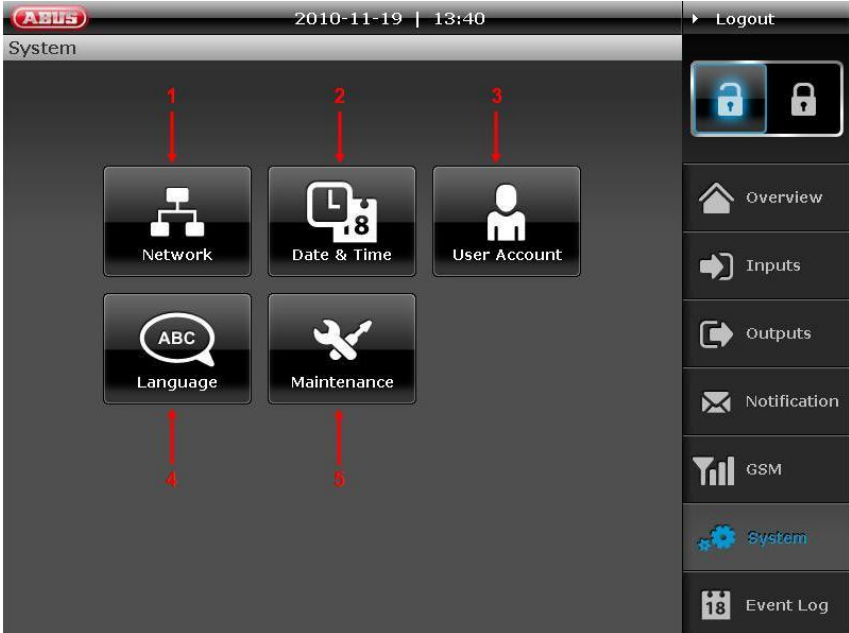
14.7 GSM



Settings can be made here for using an optional GSM dialler (AZ6302) to set up a redundant communication path. To use a GSM dialler, switch GSM to “On”. The transistor outputs are now also controlled. To receive notifications exclusively via GSM, tick the “GSM Only” box. Confirm the settings by clicking the **Apply** button.

14.8 System

This menu item is used to configure the network settings, set the date and time, manage users, change the language and perform maintenance on the alarm centre itself.



1. Network

System | Network

Mode: **Static IP** (dropdown menu open with options: DHCP, Static IP)

IP-Address: 195

Subnet Mask: 255 255 255 0

Gateway: 192 168 0 1

DNS: 192 168 0 1

Port: 10987

Apply

Logout

- Overview
- Inputs
- Outputs
- Notification
- GSM
- System
- Event Log

The “Mode” selection box is used to specify whether the IP address is taken automatically from the DHCP server or is assigned manually by the user via static IP. Select the appropriate setting according to your network properties.

2. Date & Time

System | Date & Time

Mode: **NTP**

Time Zone: (GMT+01:00)Amsterdam, Berlin, Bern, Rome, Vienna

NTP Server: ptbtime1.ptb.de

Date: 2010-11-19

Time: 16:31:54

Apply

Logout

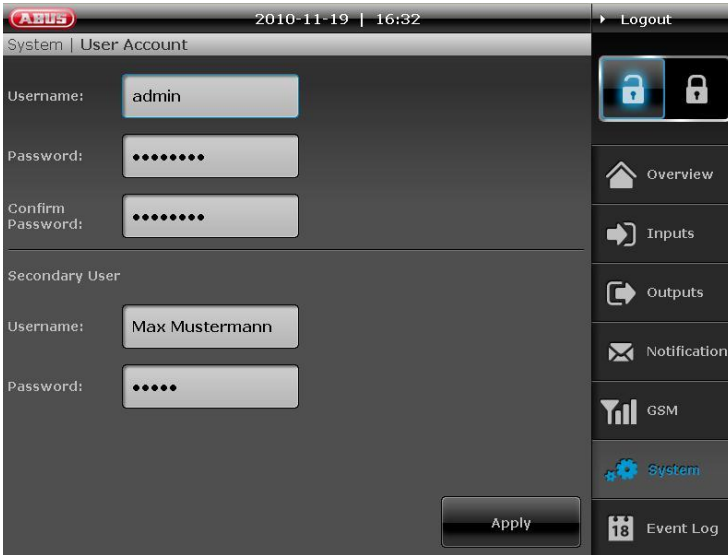
- Overview
- Inputs
- Outputs
- Notification
- GSM
- System
- Event Log

November, 2010						
week	Sun	Mon	Tue	Wed	Thu	Fri
43		1	2	3	4	5
44	7	8	9	10	11	12
45	14	15	16	17	18	19
46	21	22	23	24	25	26
47	28	29	30			

Please click on the date

Set the time and date here.

3. User Account



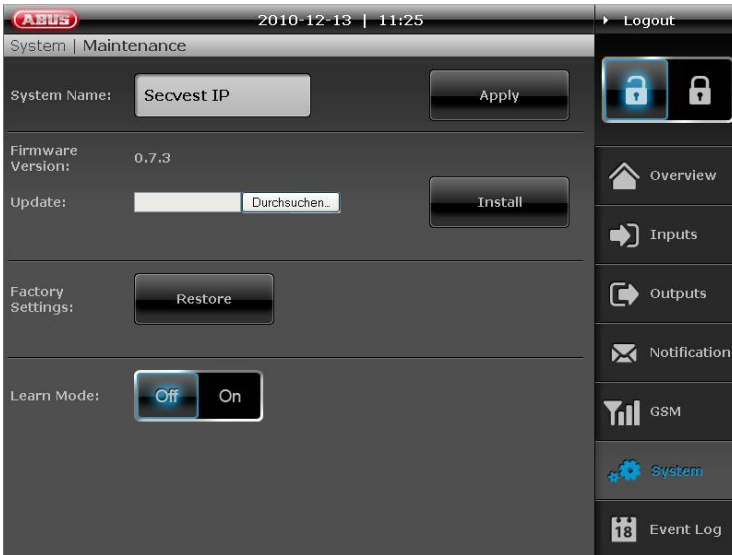
Two user levels can be implemented here. All setting options on the alarm centre are available on the first user level. The second user level only has the option of activating and deactivating the alarm centre or resetting the alarm. This prevents the programming from being able to be changed by every user.

4. Language



The corresponding system language is set here.

5. Maintenance / Learn Mode / Firmware update



The “Maintenance” menu item is used to change the system name, make a firmware update or reset the system to the factory settings.

To update the firmware, click on “Browse” to select the update file on your computer. To start the update, click “Install”. The update process can take several minutes – never terminate the connection between your computer and the Secvest IP during this time. The system is restarted after the update is completed.

The system can be set to “**Learn Mode**”, to deactivate the alarm reaction of the alarm panel. That means that in this mode detectors can be triggered and tested, but the alarm panel does not trigger any alarm. This is especially suitable for teaching the detectors and to maintain wireless components.

14.9 Event Log

This function enables the user to read the event log.

The screenshot displays the ABUS Event Log interface. At the top, it shows the date and time: 2010-11-19 | 16:34. The main area is titled "Event Log" and contains a table of events. The table has two columns: "Date & Time" and "Event(s)". A dropdown menu is open, showing a list of event types: "All Events", "Fault", "Low Battery", "Power Fail", "Fire", and "Technical". Red arrows point to the sort order arrow (1) and the event type dropdown (2). At the bottom, there are three buttons: "Clear", "Save", and "Refresh", each circled in red. The right sidebar contains navigation options: "Logout", "Overview", "Inputs", "Outputs", "Notification", "GSM", and "System".

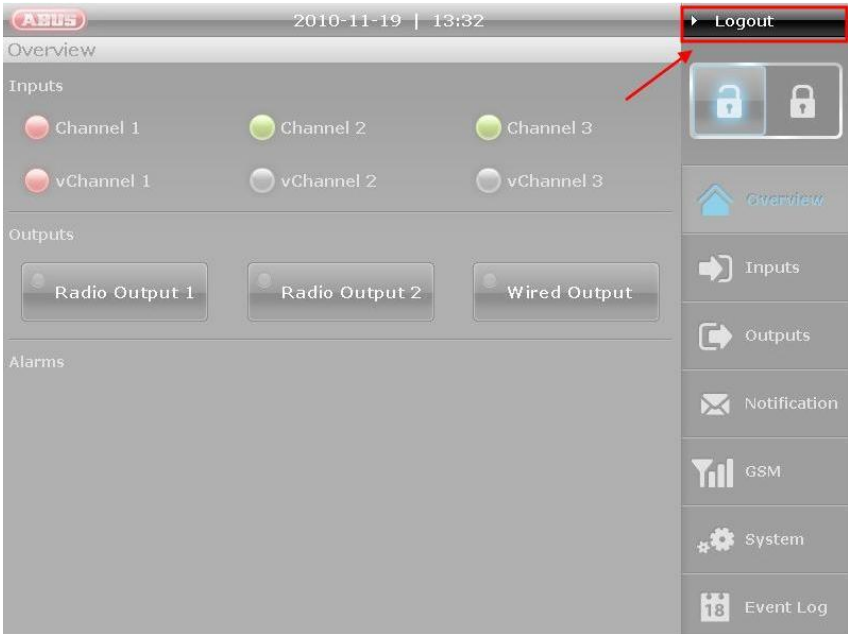
Date & Time	Event(s)
2010-11-19 13:03:05	Fault
2010-11-19 13:03:05	Unset
2010-11-19 11:39:02	Unset
2010-11-19 11:39:02	Unset
2010-11-19 11:38:27	Burglary
2010-11-19 11:38:09	Set
2010-11-19 11:38:09	Set
2010-11-19 11:37:11	Trouble

This log contains the events together with the date and time and event type. The sort sequence can be changed from descending to ascending order using the arrow at the top left (1).

All alarm events are shown as standard. If only one specific event type should be displayed, then select this in the menu at the top right (2).

Additionally, the event log can be deleted ("Clear"), updated ("Refresh") or exported into an external file ("Save").

14.10 Logout



After the configuration is set or operation is finished, click on the **“Logout”** button at the top right of the screen to log out of the Secvest IP web server. This prevents unauthorized persons using this computer from making changes to the alarm centre.

15. Teaching the wireless components

Switching on: Connect the power supply. The alarm centre beeps twice and the top LED (green) lights up. Ensure that the tamper switches on the alarm centre are open. The “Trouble” LED flashes red with 1 Hz if the cover is open. To deactivate the wall temper switch, read the instructions below.

Programming: Press SELECT once to access programming mode. The main menu is accessed. The bottom LED lights up for menu 1.



For teaching wireless components, we suggest to activate the Learn Mode. This can be activated by the web server: System → Maintenance → Learn Mode → ON. In addition we recommend deactivating the wall tamper contact during programming. See the section on deactivating CON1 (C) for more information. Please ensure that the jumper is set according to your wishes after programming is completed.

Press SET once to access the menu – the LED goes out or flashes according to the individual menus.

SELECT



Always **close** programming mode as described below to ensure that the new settings are saved.

Do not disconnect the power supply.

Press ESC/DEL until the alarm centre starts to beep (about once per second). Close the housing and hold down the cover tamper contact SW4 (B) for about 4 seconds until it beeps twice.

The red “Trouble” LED goes out.

SET



ESC/DEL



SW4



If the alarm centre has not yet been mounted to the wall, please keep in mind that the wall tamper switch must also be pressed or deactivated by the “FIT DISABLE TAMP” (CON1 (C)) jumper.

All programmed settings and the data of the trained components are saved in an EEPROM. This data is not lost in the event of a power failure.

15.1 Menu 1 – Training the components



Before starting, consider which detectors should be trained on which zones. Train the detectors in sequence and ensure that only the detectors to be trained emit a signal. Take note of the position and channel where specific detectors have been trained, as this makes subsequent labelling of the Secvest IP easier. Please be also aware, that it is only possible to teach operating units, like the remote control or the Secvest Key, in channel 1 to 3.

Press SELECT (top right) once to access programming mode. The bottom LED (blue) lights up. The **main menu** is accessed.

Press SET **once** to access menu 1. The second LED from the bottom (for channel 1) lights up or flashes. If it lights up, then a component has already been trained on this channel. Press SELECT to access the next channel. If the channel LED flashes, then the channel is free and a wireless component can be trained. Trigger a wireless signal from the components to be trained. Press the corresponding tamper contact of the components to be trained or a trigger. To train a 2WAY wireless remote control, press any button. To train a Secvest Key, insert the battery. Once the first component is trained, the alarm centre beeps twice and the corresponding channel LED lights up. Repeat this operation for additional components. This assigns additional channels. Pay attention to the assignment of the channels to the groups and the maximum number per group.

Group 1	Zone 1	Zone 2	Zone 3
Operating units 1/2/3	Detectors 1/2/3/4	Detectors 5/6/7	Detectors 8/9/10/11
Channels 1–3	Channels 4–7	Channels 8–10	Channels 11–14



Ensure that control devices are trained on the first three channels, followed by detectors from channel 4 onwards. Train detectors of the same type in a group (e.g. group of motion detectors, group of smoke detectors etc.).

When you are finished, press ESC/DEL once. Pressing any other buttons has no effect on the alarm centre at this point. The bottom LED lights up again permanently. The main menu is accessed again.

15.2 Menu 2 – Deleting the components

Press SELECT until the second LED from the bottom lights up.
Press SET **once** to access menu 2.

The LED of a channel with a trained component lights up. Press SELECT repeatedly until the desired channel lights up. Empty channels are indicated by a flashing LED. If the LED of the desired channel lights up, press (beeps once) and hold down ESC/DEL (about 4 seconds) until the alarm centre beeps twice and the channel LED flashes. The component has been deleted. Repeat this as required to delete all the corresponding components.

When you are finished, press ESC/DEL once. Pressing any other buttons has no effect on the alarm centre at this point. The bottom LED lights up again permanently. The main menu is accessed again and LED 2 lights up again.

15.3 Menu 3 – Selecting the channel settings (channel mode)

Explanation:



A detector is triggered (e.g. window is opened) and sends a status notification to the alarm centre. If the window is closed again, then the detector sends another notification of the changed status (closed) to the alarm centre.

If the corresponding channel is activated (detector triggered), then the zone is also opened. If the channel is deactivated (detector inactive) then the zone is also closed (providing all other detectors in this zone are also closed).

Some detectors (e.g. wireless panic alarms) do not send a new notification to the alarm centre after becoming inactive. Resetting of the channel must be made automatically in the alarm centre for these detectors. In order for this to be made automatically, the channel attribute for these detectors must be set to “Impulse”.

Press SELECT until the third LED from the bottom lights up. Press SET once to access menu 3. The alarm centre beeps twice and the LED shows the first occupied channel.

Press SELECT until the LED on the channel to be set lights up. Now press SET – the alarm centre beeps twice again. The LED now indicates the selected setting for the channel:

- “Impulse” is selected when the LED flashes.
- “Permanent” is selected when the LED lights up permanently.

Press SELECT to change the settings. The LED now indicates the selected setting. Press SET again to confirm the changes. The alarm centre beeps twice again and the LED shows the selected channel.

Repeat this process to make the settings for all components.



Note: The following table gives an overview of which components must have the channels set to “Impulse” and “Permanent”:

Permanent	Impulse
FU59xx, FU8100, FU8130, FU8140, FU8150, FU832x, FU8330, FU8370, FU841x, FU842x, FU8430	FU8300, FU8305, FU8310, FU8340, FU8350, FU8360, FU8380, FU8390

When you are finished, press ESC/DEL once. Pressing any other buttons has no effect on the alarm centre at this point. The bottom LED lights up again permanently. The main menu is accessed again and LED 3 lights up again.

15.4 Menu 4 – Displaying the signal strength

Press SELECT until the fourth LED from the bottom lights up. Press SET **once** to access menu 4.

The LEDs then display the last received signal strength for every channel. This happens as follows: First, a channel LED flashes six times and then the signal strength is displayed as a bar between 0 and 8. The corresponding number of LEDs (starting from the bottom) light up. The alarm centre then runs automatically through all of the occupied channels.

This submenu cannot be accessed if no wireless components are trained.

The LEDs show the strength of the received signal. The more LEDs light up (from bottom to top), the stronger the signal. If only two or fewer LEDs light up, the signal is not strong enough for reliable operation.



Before doing this, trigger all detectors and operating units once using the tamper contact or button. Components can also be triggered during the test, which results in the display of the last received signal strength being updated.

The display of the last received signal strength on the channels can be reset manually by pressing SW4 (**B**). Only newly received signals are now displayed.

When you are finished, press ESC/DEL once to access the main menu again.

When you are finished, press ESC/DEL once. Pressing any other buttons has no effect on the alarm centre at this point. The bottom LED lights up again permanently. The main menu is accessed again and LED 4 lights up again.

15.5 Menu 5 – Controlling the wireless indoor siren, wireless info module and wireless socket

In order to be able to use a wireless socket or wireless indoor siren, you must first change the setting to “Activated” in menu 5 (the LED flashes). This is set to “Deactivated” as standard (LED off) in order to prevent unnecessary wireless transmissions when no wireless socket or indoor siren is in use. Press SELECT until the fifth LED from the bottom lights up. Press SET **once** to access menu 5. Press SET again to switch between the activated and deactivated settings.

15.5.1 Wireless indoor siren and wireless info module

Set the indoor siren or info module to training mode. Consult the operating manuals for both components for more information.

Open the alarm centre or cover tamper contact and press SET (also pay attention to the programming information here). Successful training is signalled on both components.



Set the jumper for selecting the partition to “Partition 1”. This must be selected.

15.5.2 Secvest wireless socket

To train the wireless socket:

Set the socket to training mode (orange).

Switch on the output where the socket(s) should be trained using the web server. The socket gives an acoustic feedback on the success of the training process.

Multiple sockets can be trained to one output.

When you are finished, press ESC/DEL once. Pressing any other buttons has no effect on the alarm centre at this point. The bottom LED lights up again permanently. The main menu is accessed again and LED 5 lights up again.

To exit programming mode, press ESC/DEL until the alarm centre starts to beep (about once per second). Close the housing or press and hold down the cover tamper contact (SW4 **(B)**, underneath ESC/DEL) for about 4 seconds until it beeps twice. The data is saved in an EEPROM.

15.6 Menu 6 – Not in use

Option: Switching the display (supervision monitoring displayed on LEDs: yes/no)

15.7 Menu 7 – Not in use

15.8 Menu 8 – Setting the default factory settings

Press SELECT until the eighth LED from the bottom lights up.

Press SET **once** to access menu 8.

All blue LEDs start flashing. This signals that the wireless module is ready to reset itself to the factory settings.

Press and hold down the ESC/DEL button for about 4 seconds until the flashing stops and the alarm centre beeps twice. The factory settings are now restored.

The main menu is accessed again.

To exit programming mode, press ESC/DEL until the alarm centre starts to beep (about once per second). Close the housing or press and hold down the cover tamper contact (SW4, underneath ESC/DEL) for about 4 seconds until it beeps twice. The data is saved in an EEPROM.

16. Resetting an alarm

Alarm centre is **SET** and an alarm has been triggered:

- **Through the web server:**
Press the “Unset” Button
- **Through a wireless remote control:**
Press the “Unset” Button (deactivate) on the remote control. This resets an alarm.



Alarm centre is **UNSET** and an alarm has been triggered:

- **Through the web server:**
Press the “Alarm” button and confirm the reset
→ the alarm will be reset
- **Through a wireless remote control:**
Press the “Set” button (activate) on the remote control.
This resets an alarm when an alarm is present.



17. Notes on maintenance

Set the alarm centre to learn mode when carrying out maintenance. You can then open the alarm centre or teach wireless components (or change the battery) without triggering a tamper alarm.

This is made using the web server: System → Maintenance → Learn Mode → ON

18. Technical data

Display	Status LEDs
Number of wireless zones	3 wireless zones, 11 detectors (4/3/4)
Number of virtual IP zones	3
Wireless control devices	Max. 3 (Remote Control, Secvest Key)
Switching outputs	1 x relay, 4 x transistor
Expandable (wireless)	Yes (by max. 8 detectors via max. 1x IP alarm module)
Event log	Yes (alarm notifications; can be called up via web interface)
Integrated siren	No
Communication/alarming	E-mail
Remote maintenance	Yes
Programming	Via integrated web server
Operation	Via Secvest Key, wireless remote control, local PC or online via browser or iPhone application
Languages	DE, UK, NL, FR, DK
Tamper detection	Yes
Wireless frequency	868.6625 MHz
Wireless output	Max. 10 mW
Range: Transmission	Ca. 30 m (indoors)/ca. 100 m (outdoors)
Range: Reception	Ca. 30 m (indoors)/ca. 100 m (outdoors)
Modulation	FM
Bandwidth	Narrow band
Encryption	Yes (wireless)
DSL monitoring	Yes
Supported browsers	Safari, Mozilla Firefox, Google Chrome
Supported software	iPhone application
Network connection	RJ45 Ethernet 10/100 Base-T
Network protocols	TCP/IP, DHCP, SMTP, DNS, NTP, HTTP
Access protection	User name, password
Power supply	13.8 V DC, power supply unit (FU3819)
Battery type	12 V, 1.2 Ah (BT2020)
Power consumption	Max. 1,4A
Backup power supply	Yes
Max. run time under emergency power	ca. 5 hours
Power supply monitoring	Yes
Backup	Reverse polarity protection
Housing material	ABS
Protection class	IP34
Factory-set IP address	192.168.0.50
Installation location	With optimally adjusted conditions for wireless performance Environmental conditions
Operating temperature	-10°C to +55°C, max. 75% humidity (non- condensing)
Dimensions (W x H x D)	193 x 233 x 45 mm
Weight	760 g
Environment class	II

19. Customer service and support

End consumer: Please consult your dealer or installer if you have any questions.

Dealers/installers: Consult our website for product support information:
www.abus-sc.com

ABUS Security-Center GmbH & Co. KG
Linker Kreuthweg 5
86444 Affing
GERMANY
www.abus-sc.com
info@abus-sc.com

20. Explanation of terms

- ✓ **Jamming:** Interference of the wireless frequency.
- ✓ **Supervision:** The availability of the detectors is monitored (i.e. is there a wireless connection: yes/no).
- ✓ **LAN:** **Local Area Network**
 - Direct connection of the Secvest IP alarm centre to a PC
→ Cross-over cable (certain lines are swapped).
 - Connection of the Secvest IP alarm centre through a switch
→ Patch cable required (all wires looped 1:1).
- ✓ **APP:** **Application**
→ Usually a small program on modern mobile phones (e.g. iPhone).
- ✓ **NO:** **Normally Open** (the detector contact is open when idle and triggers as soon as the circuit is closed).
- ✓ **NC:** **Normally Closed** (the detector contact is closed when idle and open when activated).