interlogix
A UTC Fire & Security Company

Advisor Advanced Manager Manual

P/N 1069043 • REV 4.0 • ISS 09MAY11

Trademarks and patents

Interlogix, Advisor Advanced name and logo are trademarks of UTC Fire & Security.

Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.

Manufacturer

UTC Fire & Security Americas Corporation, Inc.
1275 Red Fox Rd., Arden Hills, MN 55112-6943, USA

Authorized EU manufacturing representative:
UTC Fire & Security B.V.
Kelvinstraat 7, 6003 DH Weert, Netherlands

Certification

CE

EN 50131-1 System requirements
EN 50131-3 Control and indicating equipment
EN 50131-6 Power Supplies
EN 50136-1-1 Alarm systems -Alarm Transmission systems
PSTN transmission path: ATS Class 2
IP transmission path: ATS Class 4
Security Grade 2, Environmental class II

Tested and certified by Telefication B.V.

European Union directives

1999/5/EC (R&TTE directive): Hereby, UTC Fire & Security declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

2002/96/EC (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info.

Contact information

www.utcfireandsecurity.com or www.interlogix.com

Customer support

www.interlogix.com/customer-support

Content

Important information

This manual explains how to use the Advisor Advanced system if you are responsible for managing the system. There is also a shorter user guide available that explains everyday usage. To use this documentation effectively, you should have a basic knowledge of alarm systems.

Read these instructions and all ancillary documentation entirely before operating this product.

Note: A qualified installer, complying with all applicable codes, should perform whatever hardware installation is required.

Typographical conventions

This manual uses certain notational and typographical conventions to make it easier for you to identify important information.

Table 1: Notational and typographical conventions

Item	Description
Keys	Capitalized, for example “press Enter”.
Note	Notes alert you to information that can save you time and effort.
Caution	Cautions identify conditions or practices that may result in damage to the equipment or other property.
❑	Check boxes let you indicate whether a particular option is available or not. The installer can provide details on the available options.
[IP]	This text identifies menus and options specific only for Advisor Advanced-IP panels.

Important note

This manual provides information for all Advisor Advanced control panels in all variations. “Advisor Advanced control panel” refers to any variant of the Advisor Advanced, unless specifically stated otherwise.

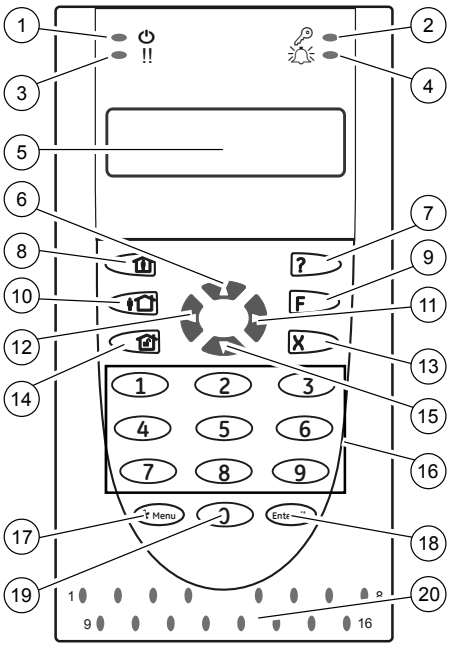
Table 2: List of panel variants [1]

Model	Enclosure	Dimensions (mm)	Power supply (A)	Weight (kg) [2]
ATS1000A-SM	Metal	250 x 250 x 86	1	2.8
ATS1000A-MM	Metal	315 x 388 x 85	1	5.2
ATS1000A-IP-MM	Metal	315 x 388 x 85	1	5.2
ATS1000A-LP	Plastic	257 x 400 x 112	1	2.6
ATS1000A-IP-LP	Plastic	257 x 400 x 112	1	2.6
ATS2000A-MM	Metal	315 x 388 x 85	2	5.2
ATS2000A-IP-MM	Metal	315 x 388 x 85	2	5.2

[1] Not all variants may be available.
[2] Weight does not include batteries.

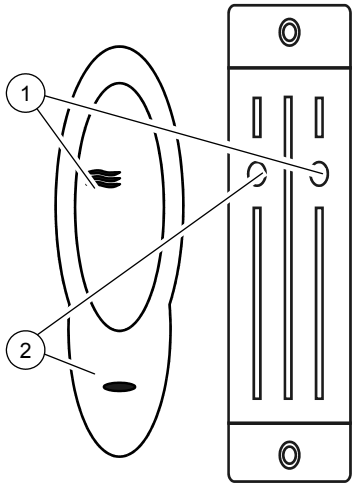
Keypads and readers

Figure 1: The keypad



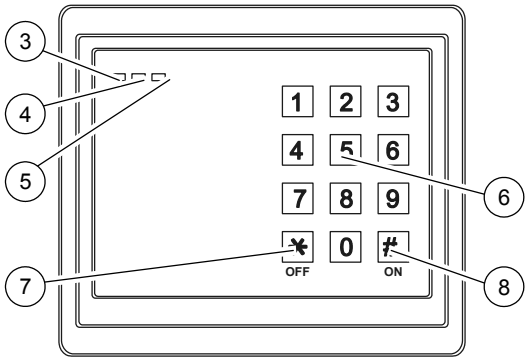
1.	AC mains LED	Green on: AC mains supply on
2.	Access LED	Blue flashes: card read
3.	Fault LED	Yellow on: system fault active Yellow flashing: general alert (EN 50131)
4.	Alarm LED	Red on: alarm condition active
5.	LCD display	Displays messages
6.	▲ / Up	Scroll up in the menus Change value Delete
7.	? / Help	Show help Enables/disables word library
8.	Partset	Part set an area
9.	F / Function	Show active zones / faults Expand text
10.	On	Full set an area
11.	► / Right	Enter the selected menu Move cursor right
12.	◄ / Left	Return to the previous menu Move cursor left
13.	X / Clear	Exits the current user function
14.	Off	Unset an area
15.	▼ / Down	Scroll down in the menus Change value Backspace
16.	Alphanumeric keys	Keys 1 to 9, alphanumerical data
17.	Menu	Request entry to the menus
18.	Enter	Complete the step Enter the selected menu entry
19.	0	Key 0 Toggle selection
20.	Area LEDs 1 to 16	On: area set Off: area unset Flashing: area alarm condition

Figure 2: ATS1190/ATS1192 readers



1.	Blue LED	Access granted
2.	Red LED	On: area set Flashing: general alert (EN 50131)
3.	Dual LED	Green on: AC mains supply on Green flashing: AC mains supply off, or unlocked while unset Red on: all areas set Red flashing: unlocked while set
4.	Yellow LED	On: All zones are in normal state Flashing: general alert (EN 50131)
5.	Red LED	Flashing: alarm
6.	Numeric keys	Keys 0 to 9, numerical data
7.	Off	Unset an area
8.	On	Full set an area

Figure 3: ATS1197 reader with keypad



The LCD display

Messages are displayed on the liquid crystal display (LCD) on the keypad. They guide you through the menu options and possible problems of the Advisor Advanced system. The display is also used to show information you have entered on the keypad.

The first line of the display shows system information and scrolls if there are more characters than can be displayed, depending on the arming station type. The second line or last line of the display shows instructions and characters you enter on the keypad.

```
    UTC F&S
TUE 29 Apr 08:55
```

Your system might display a custom message instead of the one shown above if it has been programmed to do so, for example:

```
 Main warehouse
TUE 29 Apr 08:55
```

The LEDs

The LEDs on the Advisor Advanced keypad and the information shown on the display allow you to determine the system status at a glance. Not all LEDs are available on all arming stations.

Area LEDs

The area LEDs, one for each of the possible security areas, indicate the status of the particular area. The status of the area LED can be:

- On: The area is unoccupied and set.
- Off: The area is occupied and the security system has been set to allow normal access.
- Blinking: An alarm has occurred in the area while the area was unset (LED flashes slow), or an alarm has occurred in the area while the area was set (LED flashes fast).

System alarm LEDs (available on some arming stations only)

The system alarm LEDs indicate a breach of security. One of the system alarm LEDs flashes when an alarm has occurred (the area's set LED also flashes to indicate the location of the alarm). Alarm LEDs operate as follows:

- Unset alarm: Flashes when an alarm has occurred in an occupied area, and the area was unset.
- 24-hour alarm: Flashes when an alarm has occurred in an area where a zone has been programmed for 24-hour alarm.
- Set alarm: Flashes when an alarm has occurred in a set area.
- Tamper alarm: Flashes when an alarm has occurred due to tamper.

System faults (available on some arming stations only)

System faults are displayed on the arming station keypads if the arming station has an LCD fitted and/or has "System faults" LEDs. Fault LEDs operate as follows:

- Comms fail: When there is a failure in the communications between the Advisor Advanced control panel and a central station.
- RAS fail: When a remote arming station is offline.
- DGP fail: When a data gathering panel is offline.
- Battery fail: When the auxiliary battery power is found to be low.

- Trouble: When there is a trouble in the system (RAS fail, low battery, etc).

General alert indicator (EN 50131)

To comply with the EN 50131, this indicator is enabled if the system is unset and the screen saver is active. The alert indicator flashes in case of any fault, alarm, or pending alarm.

Screen saver

Some installations require the use of a screen saver.

The screen saver prevents unauthorized users from viewing details about the security system status. The screen saver is deactivated on entering a valid user code or presenting a valid badge.

When the screen saver is active, only a general alert message can be displayed.

User identification

All users of the Advisor Advanced system need a PIN and/or a card that is set up in a user account. A PIN is unique code and has between 4 and 10 digits. It is a combination of numbers between 0 and 9.

PINs and/or card details are part of the setup of a user account. The user account is set up to allow users to perform specific tasks, such as set or unset the system. These task or options are defined in user groups.

Predefined users

There are two predefined users in the system:

- Installer is used to enter the Advisor Advanced system configuration. It has user group “Installer group” assigned.
- Supervisor is used to grant access for a service engineer. It has user group “Supervisor group” assigned. The default PIN is 1122.

Note: If the PIN length is configured for more than four digits, zeroes are added to the default PIN values. For example, if the system is configured for a six-digit PIN, the supervisor PIN is 112200.

User groups

A user group allows users to control the Advisor Advanced system alarm options (also called alarm control). This provides flexibility when determining a user’s access to, and control of, the system.

A user can have more than one user group assigned. In this case, if any of those groups grants permission to a particular option, the user has this permission.

For example: A user has two user groups assigned: “R&D” and “Managers”. If “Managers” user group allows inhibiting but the “R&D” group does not, the user is able to inhibit a zone.

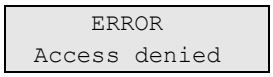
Note: The system always includes an installer group. This group can be assigned to only one user, the default installer user.

Using a PIN and/or a badge

When you enter your PIN on the Advisor Advanced keypad, each key pressed is indicated by * on the display.

If you enter the wrong PIN, or present a card with a PIN that is not valid at the particular keypad, the keypad beeps quickly seven times. Correct a wrong code by pressing Clear and enter the correct code. If you access a menu and do not press any key for three minutes, the system time out function automatically exits from the menu. It is good practice to exit the menu using the Clear button rather than using this time out facility. If someone else uses the menu before it times out, the option used is logged against your user account.

Users can only access the menu options enabled for the user groups assigned to the user account. When they try to access an option that they are not authorised to access, they get the message:



See also: “7 Users” on page 28.

Duress

The duress function activates a silent signal to alert security personnel. If you are asked, under threat, to breach your system security (for example, forced to unset the system), this function lets you do so while at the same time activating the system duress facility. However, your Advisor Advanced system must be programmed to use this function.

You use a duress digit in conjunction with your PIN. There are three methods for entering a duress code.

Table 3: Duress methods

Option	Description	Example	Available
Increment last digit	The duress code is your PIN with the last digit of your PIN incremented by one (1)	Example: PIN = 1234, duress code = 1235. If the last digit of your PIN is 9, then the duress digit becomes 0. Example: PIN = 2349, duress code = 2340.	❑
Add last digit	The duress code is a code with an additional digit “5” at the end	Example: PIN = 1234, duress code = 12345	❑
Add first digit	The duress code is a code with an additional digit “5” on the beginning	Example: PIN = 1234, duress code = 51234	❑

To activate duress, provide an allowed key sequence indicated in “Common key sequences” on page 44.

To reset the duress alarm, enter a valid PIN or card with PIN.

Notes

- If duress was activated under conditions that are no longer valid (a false alarm), and it has been reset, you must contact your central station company to ensure that they take no further action.
- Using your PIN with the duress digit still activates the options configured for your user group.

Door access

If programmed, it is possible to get access through a particular door using the keypad or the reader assigned to the door.

Provide an allowed key sequence indicated in “Common key sequences” on page 44.

Set and unset the system

When to set

The security system should be set if you are the last person to leave the premises (or your area), for example at the end of the day. When set, any security device detecting intruders activates an alarm.

When to part set

In case you are still on the premises (or in your area) it is possible to perform a part set of it. For example, you can secure your garage using part set while you remain in the house. If there is an alarm, the external siren is not activated. Notification to the central station may happen depending on system configuration settings. Contact your installer for more information.

You can use part set for perimeter protection, for example when you secure your house at night but stay inside. You can move inside of the house, but if someone tries to enter without unset, this triggers an alarm without external siren activation. Notification to the central station may be sent depending on system configuration settings. Your installer can provide details.

If there are more part sets available in the system, you will be prompted to choose an appropriate set to part set:

```
1>Part set 1
2 Part set 2
```

When to unset

If the area you want to enter is set, you must first unset the alarm system before you can enter as otherwise you will trigger an alarm. Depending on system configuration you may be able to tell when an area is set because the LED on the keypad is lit red. If the screen saver is enabled, only the Mains LED will be lit. Once a valid code is entered, the system status will be shown.

In most cases an entry beeper sounds indicating that the system needs to be unset or an alarm will occur.

The time limit to leave the premises once set

Once you have set the system, you must leave the premises (or area) within a pre-set time (“exit time”) as otherwise you will set off the alarm. The manager of the system needs to inform everyone about this time limit.

Normally, you will hear a beeper during the time allowed to leave the building.

Make sure you know which route to take when leaving the premises.

The time limit when unset

Once the system is set, you have to unset the area within a pre-set time (“entry time”) as otherwise you will set off the alarm. The manager of the system needs to inform everyone about this time limit.

You will normally hear a beeper during the time allowed to unset.

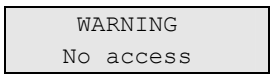
Unset when there is an alarm

If there is an alarm condition while you are unsetting the system, the alarm is reset. You must then find out what caused the alarm and make sure it does not happen again. See “What to do when there is an alarm” on page 16.

Unsetting while the system is in alarm is described in “Resetting an alarm” on page 17.

Use menu “3 View logs” on page 24” to list recent alarms.

When you cannot set or unset



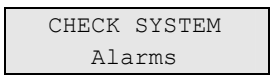
You might not be authorised to set/unset specific areas on the premises because:

- Your keypad has been programmed to set/unset specific areas of the premises only. Make sure you know which keypad to use if there is more than one present of the premises.
- Your PIN and/or card have been programmed to set/unset only specific areas of the premises. Make sure you know which areas you are authorised to set/unset.
- Your alarm system might have more than one control panel. If so, each will have been programmed to set/unset only specific areas of the premises. Make sure you use the correct keypad for the areas you want to set/unset.

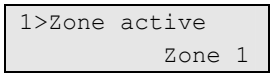
Active zones

You cannot set an area if it has a zone that is open, such as the magnetic contacts of a door or window. So, before setting, make sure that all doors and windows are properly closed.

If a zone is open when you try to set, you get the message:



All the active zones are listed:



Setting the areas is now disallowed. If the indicated zones have to stay open (for example, you need to leave a window open), the problem may be resolved using one of the following methods:

- Cancel the setting using the Clear button. Log on to the menu and inhibit the zone if it should remain active. See “1 Inhibit zones” on page 22 for more information. After active zone is inhibited, attempt the setting procedure again.
- Inhibit the zone from the set menu. This is only allowed if you have the proper options available. It only works on zones that are allowed to inhibit. Press Off to inhibit.

  ```
  >1 Zone 1
  ----------------
  ```

  ```
     Inhibited
       Alarms
  ```

  If any more zones are active, this step may be repeated.
- Use forced set.

  You can activate forced set only if you have the proper options available. The system configuration also needs to include this option. Forced set is an automatic inhibiting of open zones and some faults. The conditions for inhibiting and uninhibiting items are configured in the system. The manager must inform users when they are allowed to use forced set.

  To activate forced set, press On. All open zones and faults are inhibited, and the appropriate warning is displayed. See “Inhibited zones and faults” below.

Active faults

```
  CHECK SYSTEM
     Faults
```

You cannot set an area if certain system faults are present. The list of faults preventing setting the system is defined by the installer. It is possible to temporarily disable these warnings in the same way as for active zones (see above). The manager must inform users whether or not they are authorized to disable faults in this way.

Inhibited zones and faults

If there are inhibited faults or zones, it is necessary to confirm information about it.

```
    WARNING
   Inhibited
```

All the inhibited zones and faults are listed:

```
1>Inhibited
          Zone 1
```

```
2>Battery fault
       Inhibited
```

- Press Enter to confirm the warning. After this the setting procedure continues.

— or —

- Cancel the setting using the Clear button. After you have determined which zones are active, check these and resolve the problem (for example, close the door). Attempt the setting procedure again.

Note: If you do not cancel the setting, after fixing the problem the setting procedure is continued automatically, and you can raise an alarm when you proceed to the exit after closing the zone.

The manager of the system must inform users which keypads they can use, and which areas they can set and unset.

Set areas via LCD keypad

To set areas via LCD keypad:

1. Provide an allowed key sequence indicated in “Common key sequences” on page 44.
2. If prompted, choose areas. See “Areas displayed during set and unset” on page 15 for more information.

   If there are inhibited or isolated zones in selected areas, they are listed on the display.
3. If you want to continue setting, press Enter. Otherwise, press Clear to cancel the set process.

   See “1 Inhibit zones” on page 22 and “2 Isolate” on page 23 for more information.

   The exit tone sounds. This may be a continuous tone or an intermittent tone.
4. Exit the premises using the designated entry/exit route.

   The exit tone switches off.

   When an area is set, its LED lights up red.

   If programmed, after a delay the screen saver is engaged, and LEDs are extinguished.

Part set areas via LCD keypad

To part set areas via LCD keypad:

1. Provide an allowed key sequence indicated in “Common key sequences” on page 44.
2. If prompted, choose the appropriate part set.
3. If prompted, choose areas. See “Areas displayed during set and unset” on page 15 for more information.

   If there are inhibited or isolated zones in selected areas, they are listed on the display.
4. If you want to continue setting, press Enter. Otherwise, press Clear to cancel the set process.

   See “1 Inhibit zones” on page 22 and “2 Isolate” on page 23 for more information.

   If programmed, the exit tone sounds. This may be a continuous tone or an intermittent tone.

   The exit tone switches off.

   When an area is partially set, its LED lights up red.

   If programmed, after a delay the screen saver is engaged, and LEDs are extinguished.

Unset areas via LCD keypad

To unset areas via LCD keypad:

1. Enter the premises using the designated entry/exit route.

   An intermittent entry tone starts.
2. Provide an allowed key sequence indicated in “Common key sequences” on page 44.
3. If prompted, choose areas. See “Areas displayed during set and unset” on page 15 for more information.

   The entry buzzer stops and the areas are unset.

   LEDs are extinguished, and the time and date is displayed.

Set areas via keypad without LCD

To set areas via keypad without LCD:

1. Provide an allowed key sequence indicated in “Common key sequences” on page 44.

   If the operation is not possible, the keypad beeps seven times. See “When you cannot set or unset” on page 10 for more information.

The exit tone sounds. This may be a continuous tone or an intermittent tone.

2. Exit the premises using the designated entry/exit route.

   The exit tone switches off.

   When an area is set, its LED lights up red.

   If programmed, after a delay the screen saver is engaged, and LEDs are extinguished.

Unset areas via keypad without LCD

To unset areas via keypad without LCD:

1. Enter the premises using the designated entry/exit route.

   An intermittent entry tone starts.

2. Provide an allowed key sequence indicated in “Common key sequences” on page 44.

   The entry buzzer stops and the areas are unset.

   LEDs are extinguished.

Autoset

The system can be configured so that the premises are set automatically at a particular time and a day of the week.

Before the autoset begins, the warning time starts. The system may warn the users by a sound. The following message is displayed:

```
      INFO
  Auto setting
```

Depending on system settings and user privileges, you can postpone or cancel the autoset during the warning time. To do this, press Clear and enter you PIN.

If you are authorized to postpone the autoset, you will be asked to choose the appropriate autoset delay.

```
Retry time
    >15 minutes<
```

Choose one of the following:

- Off: Cancel the autoset.
- 15 min, 30 min, 1 h, 2 h, 3 h, 4 h: Set an appropriate time period to delay the autoset.

Areas displayed during set and unset

If your system has not been programmed to display the areas assigned to your PIN on the LCD, those areas are automatically set/unset (provided all zones were normal).

The area LEDs illuminate when the set or unset procedure is successful.

If the areas assigned to your PIN are displayed, any of those areas that are unset will be listed, for example:

```
0>  All
1 * Office
```

Each area in the list has an indicator that describes its status. The following area statuses are available.

Table 4: Area statuses

Indicator	Area status
Space	Ready to set
?	Not ready to set
x	Exit time
!	Alarm
*	Set
−	Part set 1
=	Part set 2

You now have the following options.

Table 5: Area list options

Option	Action	Note
Set / unset all areas	Press 0 — or — select “0 All”, and then press Enter (or Right)	For example, the user is allowed to arm areas 1, 4, and 5. He presses On, PIN, Enter, 0. It causes that areas 1, 4, and 5 are arming.
Select / deselect areas to set / unset	Enter area numbers — or — select particular areas using Up, Down, and Enter (or Right) keys	When any of areas is selected, the first line “0 All” changes to “0+Selected”.
Set / unset selected areas	Press 0 — or — select “0+Selected”, and then press Enter (or Right)	For example, the user is allowed to arm areas 1, 4, and 5. He presses On, PIN, Enter, 1, 4, 0. It causes that areas 1 and 4 are starting to arm.
Cancel	Press Clear	Exit and return to the original display. Areas that are already set/unset, keep their state.

The area LEDs illuminate when the set/unset procedure is successful.

What to do when there is an alarm

When there is an alarm, the LED of the area in alarm and the alarm LED flashes on the keypad. If the screen saver is active, the LEDs start flashing when a user code has been entered. The time and date message is no longer displayed.

An area can have several zones associated with it. When there is an alarm, it is important that you know exactly which zone is causing the alarm so that you can quickly deal with it.

What happens when there is an alarm

There are different types of alarm and they occur under different situations.

Alarm

An alarm is raised if:

- The area is set and one of its zones has been activated. For example, a door lock has been forced open causing a siren to sound.
- The area is unset and a 24 Hour zone was activated. Examples: a hold-up button is activated, or a tamper switch is open.

The exact type of alarm signal depends on how the system has been programmed (strobes, sirens etc.) The LED on the keypad flashes quickly. The area LED on the panel identifies the location of the alarm.

When programmed, the alarm is sent to the central station.

System alarm

This alarm can occur at any time. The exact type of alarm signal depends on how the system has been programmed (strobes, sirens etc.) It occurs when the security equipment (such as the panel) has been tampered with, or detects a fault.

You can only reset a system alarm if your PIN has been authorised to do so, and only after the fault is restored.

When programmed, the central station is contacted automatically by the system.

Viewing an alarm

After disarm, all the alarms are listed on the screen.

```
Alarm
     Pending >0<
```

```
Zone 1
     Pending >0<
```

The first screen shows the type of the alarm. The second shows the source of the alarm. The second line shows if there are more alarms for this source.

Resetting an alarm

To switch off sirens or bells, you must unset the appropriate area.

If an alarm is active, the reset procedure is the same as for a standard unset. After the system is unset, you are prompted to confirm the alarms. This is possible only if the problem has been resolved.

Acknowledging the alarm

If you are permitted, you can acknowledge the alarm by pressing Off.

The alarm cannot be acknowledged if its cause is still active, for example, if there is a zone tamper. The fault should be fixed prior to acknowledging the alarm caused by this fault.

All alarms must be confirmed. A counter during the alarm confirmation process indicates the number of outstanding alarms to still be confirmed. If you don't confirm the alarms after the unset, you are prompted to do so before next set or after the next unset, until all alarms are acknowledged.

Performing a walk test

If the system is programmed for user walk tests, sometimes while setting the area, the system may ask you to perform the area walk test. To pass the walk test, you need to go to all the zones displayed. The system lists all zones still to be tested.

The necessity of the walk test depends on:

- System settings
- Activity of the programmed zones in last 4 hours

You can perform the walk test manually using “8.2 Walk test” menu (described on page 33).

Problems that can occur

There is a faulty zone

A faulty zone continues to cause an alarm until it is isolated from the system (see “2 Isolate” on page 23 for more information).

As soon as the faulty zone is isolated or the problem has been resolved, the alarm is reset automatically.

Your PIN does not work when you try to acknowledge an alarm

There are two possible reasons why your PIN may not work when you attempt to acknowledge an alarm:

- You can only acknowledge an alarm for an area if your PIN is assigned to it. If it is not and you try to acknowledge an alarm, you might set/unset the area instead.
- You cannot acknowledge a system alarm unless your PIN is authorised to do so.

The keypad does not respond to key presses

The keypad may not respond to key presses even when there is no fault in the system. The keypad is locked after a wrong PIN is entered three or more times.

When you press a key on a locked keypad, it beeps seven times.

After 2 minutes the keypad becomes available again.

Further information about alarms

If the alarm conditions are no longer valid, and the alarm has been reset, you must contact your central station company to ensure that they take no further action.

If you are unable to reset an alarm because of a faulty zone, refer to the section “2 Isolate” on page 23.

You can only reset an alarm for an area that is assigned to your PIN. If you are unable to reset the alarm, ensure that the flashing area LED is for an area you can disarm with your PIN. If not, your attempt to reset the alarm results in arming/disarming your system.

The system can be programmed in such a way that certain alarms (like tamper alarms) require a specific action from your installer. “Engineer reset req” appears in the display and a code is shown. Pass this information to your installer. See also “8.7 Engineer reset” on page 35.

Common tasks

Inhibiting / uninhibiting zones

To inhibit or uninhibit zones, use menu “1 Inhibit zones” described on page 22.

Isolating / deisolating zones

To isolate or deisolate zones, use menu “2 Isolate” described on page 23.

Listing events

To view system events, use menu “3 View logs” described on page 24.

Viewing panel status

To view the status of the panel, use menu “4 Panel status” described on page 25.

Changing own PIN

To change your own PIN, use menu “5 Change PIN” described on page 26.

Changing own reporting settings

To change particular SMS and voice reporting settings, for example, phone number, use menu “6 SMS & Voice” described on page 27.

Managing users

To create, modify, and delete users, use menu “7 Users” described on page 28.

Service functions

Service functions are described in the section “8 Service” on page 32.

Installer access

The system can be configured so that the default supervisor user must grant access for the installer / service engineer to enter the Installer menu. Use the option “8.8 Service In” described on page 35.

Calendar

Calendar lets you to define schedules and actions assigned to particular days, for example, automatic arming on holidays. See “9 Calendar” on page 36.

The Advisor Advanced menu

The Advisor Advanced system uses a menu structure to present the various options and commands available. The availability of these depends on system configuration and on the permissions in your user group. You may not always see all the items described in this manual.

If you access the menu and do not press any key for three minutes, the system time out function automatically exits from the menu. It is good practice to make sure you exit the menu using the Clear button rather than this time out facility. If someone else uses the menu before it times out, the options used will be logged against your user account.

If you attempt to select an option that is not authorised in your user account, the display shows the message:

```
    ERROR
Access denied
```

Although you might be authorised to access a menu option, you might not be allowed to access all the information it provides. You are only allowed to access information for the areas assigned to your user account.

How the menu option sections are organised in this manual

Menu options are numbered in the Advisor Advanced system. This numbering system is also used in this manual, so menu option 1 “Inhibit zones” is topic “1 Inhibit zones”.

The menu number also refers to the key sequence that can be pressed to enter the menu. For example, if you want to enter menu “7.2 Walk test”, you can press 7, then 2 after entering the menu system.

Access menu

Before commencing, ensure that the welcome screen is shown on the display.

```
   UTC F&S
TUE 29 Apr 08:55
```

Provide an allowed key sequence indicated in “Common key sequences” on page 44.

From the display you can now:

Option	Action	Result
Change the selection	Press Up or Down	Select previous or next menu option

Option	Action	Result
Enter the menu option	Enter menu option number — or — Press Enter or RIGHT to enter the selected one	Jump to a specific menu option
Show help	Press HELP	Display a description of the selected menu entry (if available)
Exit a menu option	Press LEFT or Clear	Exit the menu option

1 Inhibit zones

The “inhibit” function is used to inhibit zones and exclude them from the security system until the next unset.

There may be occasions when you want to inhibit a zone. For example, if you want to leave a window open when the system is set. By inhibiting the zone associated with the window, when you set the system you will not activate an alarm.

Note: It is also possible to inhibit active zones while setting an area. See “Active zones” on page 10 for more information.

Enter the “Inhibit zones” menu to inhibit or uninhibit zones. What happens next depends on whether or not there are active zones:

All zones are normal

You can inhibit normal zones if you know their zone number.

```
1>Zone 1
     Uninhibited
```

1. Press Up or Down to scroll through the zones.
2. Press the zone number, or use Enter to select a zone.
3. Change the zone state using Up and Down.
4. Confirm the changes by pressing Enter.
5. Press Clear twice to exit programming.

Active zones

When one or more zones are active, the system displays:

```
1>Zone 1
         Active
```

The active zones are listed one by one.

1. Press the Up and Down buttons to scroll through the zones.
2. To inhibit the selected zone, press Enter. The confirmation is displayed:

   ```
   1>Zone 1
          Inhibited
   ```

3. If you do not have rights to inhibit the selected zone, the following warning is displayed:

   ```
      WARNING
    No access
   ```

4. Press Clear to exit programming.

2 Isolate

The isolate function is used to isolate zones or devices, and exclude them from the security system.

Note: Isolated devices do not raise tampers or faults, but still remain operational.

You do this, for example, when a zone is faulty or broken. By isolating it, you stop it from causing an alarm until the problem has been resolved.

This differs from inhibiting a zone, because an isolated zone is not automatically deisolated when the system is unset.

2.1 Isolate zones

Enter the “Isolate zones” menu to isolate or deisolate zones. What happens next depends on whether or not there are active faults:

All zones are normal

You can isolate normal zones if you know their zone number.

```
1>Zone 1
      Deisolated
```

1. Press Up or Down to scroll through the zones.
2. Press the zone number, or press Enter to selected a zone for editing.
3. Press Up and Down to change the zone state.
4. Confirm the changes by pressing Enter.
5. Press Clear twice to exit programming.

Active zones

When one or more zones are active, the system displays:

```
1>Zone 1
         Active
```

The active zones are listed one by one.

1. Press Up and Down to scroll through the zones.
2. To isolate the zone, press Enter. The confirmation is displayed:

   ```
   1>Zone 1
           Isolated
   ```

3. Press Clear to exit programming.

2.2 Isolate DGP / 2.3 Isolate RAS

Isolating a DGP or RAS works the same way as isolating a zone, except the devices remain operational.

3 View logs

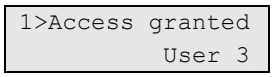
The “View logs” list provides you with a quick alarm history. It is a fast and easy way to determine where alarms have happened. This information is useful when you have had to reset an alarm without checking its cause immediately.

To view messages, select one of the following message types.

Table 6: Log message types

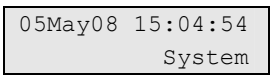
Option	Description
3.1 All	All events
3.2 Mandatory	Only events that are considered as mandatory by EN50131-1 (set/part set/unset, alarms, hold-up, tamper, fault, user change, engineer reset etc.)
3.3 Non mandatory	Events other than mandatory events mentioned above
3.4 Installer	Events caused by the installer (programming mode, PC connection etc.)
3.5 Access	Access events, like access granted and access denied

The display shows where the event occurred.



You can now:

- Scan recent alarms. Press Up or Down.
- View details. Press Enter.



- Exit history. Exit the alarm history and return to the initial display. Press Clear.

Note: You cannot see events from the area if you don't have permission for the area, or if the keypad is not programmed for access to the area.

4 Panel status

The "Panel status" function lists zones that are in alarm or tamper alarm, zones that are inhibited or active, plus system alarms.

There are menu options that display each of these conditions separately. However, this option can be used to check on all zones that need attention.

If you are allowed, you can see the panel current status using the “4 Panel status” menu.

The following data can be viewed:

Table 7: Panel status data

Option	Description
4.1 View open zones	Displays zones that are not in normal state. The top line shows the zone that is not in normal state. The bottom line shows the zone status.
4.2 Alarms	Displays and lets you to acknowledge pending alarms.
4.3 Faults	Displays active faults.

5 Change PIN

If you are allowed, you can change your PIN using “Change PIN” menu.

The PIN policy in the Advisor Advanced system can be configured in one of the following ways:

- PINs are generated by the system. The user can request a new PIN generation, but PINs cannot be entered manually or edited.

  The PIN is generated when pressing Enter in this menu. Once generated the code is then displayed.

- PINs are entered manually.

  If you are allowed to do it, you can enter the unique PIN you want to have.

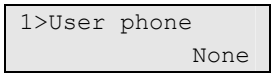
  Pressing Enter lets you enter or edit a PIN.

  To confirm the PIN, enter it again.

  PINs must be unique. A PIN cannot be assigned to more than one user. The system does accept entry of PINs that are already in use.

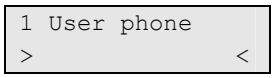
See also “7.n.2 Change PIN” on page 29 for details.

6 SMS & Voice



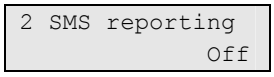
The SMS & Voice menu contains configuration menus for SMS and voice reporting. This menu allows you to change only your own settings.

6.1 User phone



The User phone menu allows you to set your personal phone number.

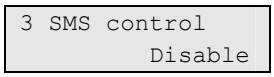
6.2 SMS reporting



The SMS reporting menu allows you to enable or disable SMS reporting to you.

This option is editable only if you belong to a user group that has SMS reporting privilege enabled.

6.3 SMS control



The SMS control menu allows you to see whether you have a possibility to send SMS commands.

See “Appendix A. SMS control” on page 57 for more information on SMS control.

7 Users

```
0>Add user
2 Supervisor
```

Use the “Users” menu to add, edit, or delete users of the Advisor Advanced system. Up to 50 users can be programmed.

For each user, the system records these options:

- Number (a panel ID between 1 and 50)
- Name
- PIN

  Note: Your user group might not allow you to program PINs. If it does allow use of this option, there may still be restrictions on which user groups you are allowed to update.
- Card ID number
- User group that determines options the user can access
- Language

There are two predefined users in the system. See “Predefined users” on page 5.

User data lock

If the system is configured as EN 50131 compliant, it does not allow you to modify the other existing user [to modify existing users]. The new user can be configured only when added, and the existing user can be only removed. The supervisor can only modify own settings, and other users can modify their own settings.

After the new user is added via menu “7.0 Add user” below, the supervisor can configure this user. After the modification is done and the supervisor is going to exit the user menu, the following confirmation request appears:

```
Lock user data?
        >Cancel<
```

Choose OK to confirm the new user configuration. After it, only this user is able to modify own settings.

Otherwise, choose Cancel to return to the user configuration.

7.0 Add user

Use to add a user. If the user is created successfully, the following message appears:

```
      INFO
   User added
```

The new user is given the default name “User N” and placed on the end of the user list. You can now start editing the user details for the new user.

7.n Edit user

Select a user to edit.

The following options can be configured.

7.n.1 User name

```
1 User name
>User 6        <
```

Press Enter to edit the name, or Clear to exit.

The default user name is “User N”, where N is the user number.

The name can have up to 16 characters.

7.n.2 Change PIN

```
1>PIN code
     ***********
```

The PINs policy in the Advisor Advanced system can be configured in one of the following ways:

- PINs are generated by the system. The user can request a new PIN, but PINs cannot be entered manually or edited.

  A PIN is generated by selecting Yes and pressing Enter in this menu. The generated PIN will show until Enter is pressed again.

- PINs are entered manually.

  Pressing Enter lets you enter or edit the PIN of the selected user.

Contact the system installer to set the PIN change mode.

PIN length is programmable in Advisor Advanced system. The number of available PINs varies from 10000 (for 4-digit PINs) to 10000000000 (for 10-digit PINs).

No PINs are reserved for system use. Any PIN can be generated or entered for use. The system will not accept generate or accept entry of PINs already in use.

7.n.3 User card

```
3>User card
      **********
```

The “User card” menu allows you to enter the user card number. Press Enter and present the card to the keypad. This is only possible on LCD keypads with integrated readers.

7.n.4 Language

```
4>Language
      ENGLISH UK
```

The Advisor Advanced system can display menus in the preferred language of each user.

The language is switched after user authorization.

7.n.5 User groups

```
1>Not set
2 Not set
```

Use the “User groups” menu to assign user groups to the selected user. A user can have up to 16 user groups assigned.

To change a user group assignment, select the appropriate slot.

If the selected slot is empty (the user group is not assigned), you are prompted to select one of the available user groups.

```
02>Supervisor G>
03 Area 1
```

Select the appropriate user group to assign to the selected user.

If the selected slot already contains an assigned user group, you are moved to the “Change UG” menu.

```
1>Change UG
    User Group 3
```

Now you can take one of the following actions:

- Change the assigned group: press 1, or Enter, or Right to go to the user group list and select a group.

  — or —

- Delete the assigned group: press 2, or go the next menu entry and press Enter.

For more information on user groups see “User groups” on page 5.

7.n.6 SMS & Voice

```
1>User phone
            None
```

The SMS & Voice menu contains configuration menus for SMS and voice reporting.

7.n.6.1 User phone

```
1 User phone
>             <
```

The User phone menu allows you to set the user’s phone number.

7.n.6.2 SMS reporting

```
2 SMS reporting
             Off
```

The SMS reporting menu allows you to enable or disable SMS reporting for the selected user.

7.n.6.3 SMS control

```
3 SMS control
         Disable
```

The SMS control menu allows you to enable or disable SMS control for the selected user.

See “Appendix A. SMS control” on page 57 for more information on SMS control.

7.n.7 Remove user

To remove a user, select a user using the cursor, or by entering the user number, and go to the “Remove user” menu.

The display shows:

```
6 Remove user
        >Cancel<
```

Choose Ok and press Enter. This removes the user.

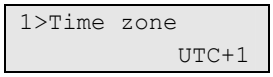
Repeat this to delete other users, or press Clear to exit and return to the higher menu level.

Note: You cannot delete a user unless your user group authorizes you to do so.

8 Service

The “Service” menu allows performing the maintenance tasks described below.

8.1 Time&date



The “Time&date” menu allows you to set the system time and date, as well as set up daylight saving time.

The following options are available.

Table 8: Time & date menu options

Option	Note
8.1.1 Time zone	The system time zone.
8.1.2 Date	Date format is DD-MM-YYYY.
8.1.3 Time	Time format is 24 hours.
8.1.4 Daylight saving time beginning month	The DST start month.
8.1.5 Daylight saving time beginning week	The DST start week. The available options are: disabled, 1st week, 2nd week, 3rd week, 4th week, last week.
8.1.6 Daylight saving time ending month	As above.
8.1.7 Daylight saving time ending week	As above.
8.1.8 Set correction	Allows configuring time correction if necessary.
8.1.8.1 Mode	The following correction modes are available: **None:** Time correction is disabled. **Manual:** The user performs necessary time correction. **NTP:** Time correction is made automatically by NTP server (IP models only).
8.1.8.2 Time/7days	This submenu allows setting the time correction that is performed each 7 days of panel work. Maximum value is 5 min 40 s. Positive value means the clock is set forward, negative — backward.

The daylight saving time always toggles on Sunday at 2:00.

Note: The Advisor Advanced system time has a 24-hour format.

8.2 Walk test

```
  Walk test
 in progress
```

Walk test allows the user to test all detectors in the selected areas.

To perform the walk test:

1. Enter the menu.

   The display lists all zones to be tested.

   ```
   1>Zone 1
        Need Active
   ```

2. Walk along all detection points and make sure the detector is activated either by walking in front of it or by opening a door or window.

   Each activated zone is removed from the list on the display.

3. Return to the keypad and verify the result.

If the test is passed, the following message is displayed:

```
  Walk test OK
  Press Enter
```

Otherwise, there still is a list of untested zones. Contact the installer if you are unable to pass the walk test.

See also “Performing a walk test” on page 17 for more information.

8.3 Manual test

```
01>CS 1
02 CS 2
```

The “Manual test” option allows you to test the central station reporting. Select the central station. The panel now tries to establish a connection with the selected central station.

The call progress status is shown on the display.

8.4 Sirens test

```
1>Internal siren
2 External siren
```

The “Sirens test” menu allows you to test internal and external sirens as well as strobes.

Note: this function works only with certain settings programmed. Please contact system installer to confirm that this function is available.

Table 9 below shows the options available for siren testing.

Table 9: Siren test options

Menu	Description
8.4.1 Internal siren	Toggle the state of the internal siren
8.4.2 External siren	Toggle the state of the external siren
8.4.3 Strobe	Toggle the state of the strobe

Enter the appropriate menu and press Enter to activate the output. Press Enter again to deactivate it. Press Clear to exit from the menu.

8.5 Communication

```
1>CS
2 PC connection
```

The “Communication” menu is used to change the phone number for voice communication, and to initialize the communication with a PC.

8.5.1 CS (central station)

```
01>CS 1
02 CS 2
```

Advisor Advanced allows you to change phone numbers for central stations that are programmed for voice communication.

8.5.1.n Select central station

```
1>Phone
```

Select central station to change the phone number.

8.5.1.n.1 Phone

```
1 Phone
>              <
```

Every central station reports to one telephone number. The phone number can contain up to 20 digits. The following special characters are available:

- P: Pause (3 s). Press 6 twice to enter.
- T: Waiting for dial tone. Press 7 twice to enter.

Note: Only voice communication phone numbers can be changed.

8.5.2 PC connection

```
01>PC conn 1
02 PC conn 2
```

The “PC connection” menu allows connecting to a PC from the panel. Select the appropriate PC connection to activate.

8.5.3 Credit

```
3>Credit
------------
```

Enter Credit menu to receive the GSM account state.

8.6 Doorbell

```
1>Area 1
          Enable
```

The “Doorbell” menu allows you to enable or disable doorbells for selected areas.

Note: If the doorbell is set to auto in system settings, the doorbell in the area may automatically become enabled or disabled when the area is armed or disarmed. Please contact the installer for more information.

8.7 Engineer reset

Some events require an engineer. You must perform the engineer reset (using the “Engineer reset” menu) when it is required by system.

To do an engineer reset:

1. Note the engineer code that is displayed in the engineer reset request.
2. Contact your installer and give him the engineer code.

   The installer will give you the resulting required for the reset.
3. Go to the “Eng. reset“ menu and enter the code given by the installer.

8.8 Service In

```
8>Service In
         Enable?
```

Certain regulations prohibit the installer from accessing the menus without permission from the manager (or supervisor). In this case the manager must use the “Service In” menu to allow the installer to log on to the system menus. Log on permission is granted for a specific time period.

Note: Once the installer enters the installer menu, he can stay in programming mode with no time limit.

9 Calendar

```
1>Actions
             >>>
```

The Calendar lets you to configure an automatic execution of specific actions at particular time and date. Panel settings can be automatically adjusted according to the schedule.

The Calendar functionality is based on actions. Every action has the following settings:

- Name
- Start time - day time to trigger the action on
- Condition filter - an additional filter that must be active to enable the action
- Activation - enabled, disabled, or disabled temporarily
- User function - see “User programmable functions” on page 43.

The actions can be grouped into Action lists, which can contain up to 8 actions.

This menu let you to configure schedule Exceptions. Exceptions represent particular time periods when everyday actions are expanded or substituted by other actions. An example of exception is a holiday, when the premises must stay set for 24 hour.

Finally, this menu provides a Schedule configuration possibility. The Schedule allows configuration of actions taken on a weekly basis.

9.1 Actions

```
01>Action 1
02 Action 2
```

There are 64 programmable actions in the Advisor Advanced system. Each action can be programmed with a number of options. Before going any further, select the action to program.

9.1.n Select action

```
1>Name
        Action 1
```

Select an action to program.

Action settings

9.1.n.1 Action name

```
1 Name
>Action 1      <
```

Every action can be programmed with a name to identify it.

Use the Action name screen to enter or edit the action name. The action name can contain up to 16 characters.

9.1.n.2 Start time

```
2 Start time
         >00:00<
```

Provide the time of the day in 24-hour HH:MM format when the selected action is performed.

9.1.n.3 Action filter

```
00>Not used
01 Internal Sire
```

Assign an additional condition filter to the action.

If this Action filter is deactivated, the action is disabled. If no condition filter is assigned, the action is executed unconditionally.

9.1.n.4 Active

```
4 Active
           >Off<
```

The Active action menu allows you to disable or enable the action permanently.

9.1.n.5 Function

```
5 Function
              >>>
```

The Function menu lets you to assign a user programmable function that should be executed during this action.

User function programming is described in “User programmable functions” on page 43.

9.2 Action lists

```
01>Action list 1
02 Action list 2
```

Action lists are used to group configured actions. An action list can contain up to 8 actions. Action list provides a name as a common description for these actions, as well as the possibility to enable or disable all of them in one menu.

9.2.n Select action list

```
1>Name
   Action list 1
```

Select an action list to program. There are 32 action lists available in the system.

Action list settings

9.2.n.1 Action list name

```
1 Name
>Action list 1 <
```

Every action list can be programmed with a name to identify it.

Use the Action list name screen to enter or edit the action list name. The action list name can contain up to 16 characters.

9.2.n.2 Active

```
4 Active
           >Off<
```

The Active action list menu allows you to disable or enable all actions in this action list permanently.

9.2.n.3 Action list

```
1>Action 1
2 Not set
```

Choose previously configured actions to configure the action list.

An action list can contain up to 8 actions.

Choose “Action” to select an action.

Choose “Remove” to remove an action from the action list.

9.3 Exceptions

```
01>Exception 1
02 Exception 2
```

Exceptions represent particular time periods when everyday actions are expanded or substituted by other actions. An example of exception is a holiday, when the premises must stay set for 24 hour.

9.3.n Select exception

```
1>Name
     Exception 1
```

Select an exception to program. There are 64 exceptions available in the system.

Exception settings

9.3.n.1 Exception name

```
1 Name
>Exception 1   <
```

Every exception can be programmed with a name to identify it.

Use the Exception name screen to enter or edit the exception name. Exception name can contain up to 16 characters.

9.3.n.2 Start date

```
2 Start date
         >01.01<
```

Enter the first day of the exception in DD.MM format.

9.3.n.3 Stop date

```
3 Stop date
         >01.01<
```

Enter the last day of the exception in DD.MM format.

9.3.n.4 Substitute

```
4 Substitute
            >On<
```

If the Substitute option is set to On, only actions and action lists assigned to this exception are performed during the exception time. If the option is set to Off, the exception actions are executed together with the other actions that must occur at the configured time.

9.3.n.5 Active

```
5Active
           >Off<
```

The Exception activation menu allows you to disable or enable the exception permanently.

9.3.n.6 Actions

```
1>Action 1
2 Not set
```

Choose previously configured actions to configure the exception.

An exception can contain up to 4 actions.

Choose “Action” to select an action.

Choose “Remove” to remove an action from the exception.

9.3.n.7 Action lists

```
1>Not set
2 Not set
```

Choose previously configured actions to configure the exception.

An exception can contain up to 4 action lists.

Choose “Action list” to select an action.

Choose “Remove” to remove an action list from the exception.

9.4 Schedules

```
01>Schedule 1
02 Schedule 2
```

Schedules are timed sets of actions with a weekly structure. Each schedule can contain actions and action lists assigned to particular days of the week.

9.4.n Select schedule

```
1>Name
      Schedule 1
```

Select a schedule to program. There can be up to 4 schedules in the system.

Schedule settings

9.4.n.1 Schedule name

```
1 Name
>Schedule 1    <
```

Every schedule can be programmed with a name to identify it.

Use the Schedule name screen to enter or edit the schedule name. Schedule name can contain up to 16 characters.

9.4.n.2 Week days

```
1>Monday
2 Tuesday
```

The Week days menu allows you to assing actions and action lists to each day of the week.

Choose a day of the week to assign actions and action lists.

```
1>Actions
2 Action lists
```

Go to the Actions submenu to assign or remove actions for the selected day of the week. Edit the list as it is described in “9.3.n.6 Actions” on page 39.

Go to the Action lists submenu to assign or remove action lists for the selected day of the week. Edit the list as it is described in “9.3.n.7 Action lists” on page 40.

9.4.n.3 Exceptions

```
1>Not set
2 Not set
```

You can assign up to 32 exceptions to the schedule. See “9.3 Exceptions” on page 38 for more details.

9.4.n.4 View

```
1>Current view
2 Date view
```

Use the View menu to see actions, action plans, and exceptions provided by the selected schedule for the particular day.

Note: Availability of submenus described below depend on the presence of the particular actions, action lists, and exceptions in this menu. For example, if no action is scheduled for the current day, menu 7.4.n.4.1.1 Actions is not shown.

This menu also allows users to cancel particular actions planned for the present day.

9.4.n.4.1 Current view

```
1>Actions
2 Action lists
```

Show actions, action lists, and exceptions scheduled for the current day.

Choose actions, action lists, or exceptions to view.

9.4.n.4.2 Date view

```
1 Date
         >02.01<
```

Show actions, action lists, and exceptions scheduled for the selected day.

Enter a date to view.

Next, choose actions, action lists, or exceptions to view.

9.5 Active schedule

```
00>None
01 Schedule 2
```

Use the Active schedule menu to choose a previously defined schedule for the system, or to remove a schedule.

9.6 View

```
1>Current view
------------
```

Use the View menu to see actions, action plans, and exceptions planned for the particular day according to the active schedule set in “9.5 Active schedule” on page 41.

This menu is similar to “9.4.n.4 View” described on page 41, except it applies only to the active schedule.

This menu also allows users to cancel particular actions planned for the present day.

User programmable functions

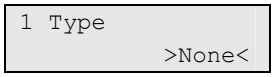
You can program your own user functions that can later be activated automatically or manually. For example, you can program a user function for setting an area or switching on an output, and then define a schedule for it.

Programming menu

The function programming menu is accessible from various menus where user programmable functions are used.

The list of allowed functions may vary for different menus.

To program a user function:



First, choose an appropriate function type using submenu 1.

Next, configure function parameters in submenu 2.

Available parameters depend on the selected function type. For particular types submenu 2 is disabled.

The following function types and parameters may be available.

Table 10: Available function types and parameters

Type	Description	Available parameters
Set	Set areas	01. Areas selection
Unset	Unset areas	01. Areas selection
Trigger	Change a trigger state	01. Trigger name 02. State change: Clear, Set, or Toggle
Doorbell	Change a doorbell state in the area	01. Areas selection 02. State change: Clear, Set, or Toggle
UG control	Change user group privileges	01. UG identifier 02 and further — user group privilege. Choose a privilege, and then allow it or deny.
RAS control	Change RAS options	01. RAS identifier 02. State change: lock or unlock

See also “9 Calendar” on page 36.

Common key sequences

See “Set and unset the system” on page 9.

The authorization method depends on system settings. Consult the system installer to define the authorization method.

Common key sequences for LCD keypad

Table 11: Common key sequences for LCD keypad

Action	Programmed method	Key sequence	[1]
Set	Set with key	On	❑
	Set with PIN	On, PIN, Enter	❑
		PIN, On	❑
	Set with card	Card	❑
		On, card	❑
		2 x card	❑
		3 x card	❑
		Hold card	❑
	Set with card and PIN	On, card, PIN, Enter	❑
		Card, PIN, On	❑
Unset	Unset with PIN	Off, PIN, Enter	❑
		PIN, Off	❑
	Unset with card	Card	❑
		Off, card	❑
		2 x card	❑
		3 x card	❑
		Hold card	❑
	Unset with card and PIN	Off, card, PIN, Enter	❑
		Card, PIN, Off	❑
Part set	Part set with key	Partset	❑
	Part set with PIN	Partset, PIN, Enter	❑
		PIN, Partset	❑
	Part set with card	Partset, card	❑
	Part set with card and PIN	Partset, card, PIN, Enter	❑
		Card, PIN, Partset	❑
Door access	Door access with PIN	PIN, Enter	❑
	Door access with card	Card	❑
	Door access with card and PIN	Card, PIN, Enter	❑

Action	Programmed method	Key sequence	[1]
Menu access	Menu access with PIN	Menu, PIN, Enter	❑
		PIN, Menu	❑
	Menu access with card	Menu, card	❑
	Menu access with card and PIN	Menu, card, PIN, Enter	❑
		Card, PIN, Menu	❑
Duress	Duress with PIN	Any set key (On / Off / Partset), duress code, Enter	❑
		Duress code, any set key	❑
	Duress with card and PIN	Any set key (On / Off / Partset), duress code, card, Enter	❑
		Card, duress code, any set key	❑

[1] Availability must be defined by the installer.

See also “Areas displayed during set and unset” on page 15.

Common key sequences for keypad without LCD

Table 12: Common key sequences for keypad without LCD

Action	Programmed method	Key sequence	[1]
Set	Set with PIN	On, PIN, On	❑
	Set with card	Card	❑
		On, card	❑
		2 x card	❑
		3 x card	❑
		Hold card	❑
	Set with card and PIN	On, card, PIN, On	❑
		Card, PIN, On	❑
Unset	Unset with PIN	Off, PIN, On	❑
	Unset with card	Card	❑
		Off, card	❑
		2 x card	❑
		3 x card	❑
		Hold card	❑
	Unset with card and PIN	Off, card, PIN, On	❑
		Card, PIN, Off	❑
Door access	Door access with PIN	Any digit, PIN, On	❑
	Door access with card	Card	❑
		Any digit, card	❑

Action	Programmed method	Key sequence	[1]
	Door access with card and PIN	Any digit, card, PIN, On	❑
		Card, PIN, On	❑
Duress	Duress with PIN	Any set key (On / Off), duress code, Enter	❑
		Duress code, any set key	❑
	Duress with card and PIN	Any set key (On / Off), duress code, card, Enter	❑
		Card, duress code, any set key	❑

[1] Availability must be defined by the installer.

When a PIN can be entered, the keypad beeps twice and flashes the red and green LEDs. When an operation fails the keypad beeps seven times. See “When you cannot set or unset” on page 10 for more information.

Programming records

Use the following pages to record the configuration and programming details for your system. The following areas are covered:

- Users
- User groups
- Condition filters (to be supplied by installer)
- Schedule
- Exceptions from schedule
- Frequently used SMS commands

We suggest that you complete the forms using a pencil so that you can erase obsolete entries and thereby keep your records up to date and compact.

It may be necessary to make copies of certain record sheets where the number of records exceeds the space allowed, for example, if your system uses more than four schedules.

We recommend that you store this manual and your record sheets together in a safe place, and ensure that they are always kept up to date.

User record

User name	User group	Full name

User name	User group	Full name

User group record

#	User group	Function summary

Condition filters

This information is provided by the installer.

Number	Filter name	Description

Number	Filter name	Description

Schedule

Days	Time	Action
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		
Mon Tue Wed Thu Fri Sat Sun		

Exceptions

Date	Time	Action

SMS commands

Command	Format or example

Command	Format or example

Appendix A. SMS control

This section specifies the SMS commands available in the systems equipped with ATS7310 GSM communication modules. You can send commands to the alarm system via SMS messages. These commands are listed in “SMS command list” on page 58.

See *Advisor Advanced SMS Control Reference Guide* for more information.

SMS control requirements

In order to use SMS control functions, you must follow these rules:

- Have a valid phone number defined in user options.

  This setting is available both locally and remotely. See the Register and Unregister command, as well as the Phone command description.
- Belong to the user group with the SMS control allowance.
- Have SMS control enabled. See the enable and Disable command description for more details.

Command syntax

The following syntax is used for all commands:

```
[<PIN>] <command> [<parameters>] [, <command>
[<parameters>] ]
```

The following principles apply:

- Commands are case-insensitive.
- Any number of consecutive blank characters (spaces, tabs, CRs, etc.) are interpreted as a single space.
- You can have up to 10 commands in one SMS message. Commands must be separated with a comma.
- In most cases <list> is a space-separated list, or “all”. If <list> is “all”, or is omitted, this is equivalent to a list of all objects for which the user has rights for the selected action.
- If the parameter is a phone number, it should be given in the fully expanded form, with country code preceded by “+”. For example: +48555223322.

User authentication

The user is authenticated by the phone number sending the SMS message.

Only registered phone numbers are allowed to send SMS commands.

The PIN field is required, if:

- The “User PIN req.” option is set to Yes

— or —

- More than one user sends SMS messages using the same phone number. The PIN is then required to identify the user.

If the PIN field is required and the command does not contain the PIN code, the following message is returned:

```
Command rejected, PIN required.
```

If the PIN field is required and the PIN is invalid, the following message is returned:

```
Command rejected, invalid PIN.
```

If the PIN field is not required, the PIN must *not* be present in SMS message.

SMS command list

Table 13: SMS commands

Command	Description	Example
status st	Get system status. The command returns the following: alarm in areas, areas set, areas being set, partset, unset, areas not ready, and fault list.	`st` Get system status.

area <area list>
ar <area list>
	Get area names.	`area 2`
		Get area 2 name.
		`ar 2 3 5`
		Get names of areas 2, 3, and 5.

set [<area list>]
s [<area list>]
	Set areas.
	If <area list> is “all”, or is omitted, this is equivalent to a list of all areas for which the user has rights for the selected action.
		`set`
		Set all allowed areas.
		`set 1`
		Set area 1.
		`s 2 3 5`
		Set areas 2, 3, and 5.
		`s all`
		Set all allowed areas.

unset [<area list>]
u [<area list>]
	Unset areas. Parameters are equal to the Set command.	`unset`
		Unset all allowed areas.
		`unset 1`
		Unset area 1.
		`u 2 3 5`
		Unset areas 2, 3, and 5.
		`u all`
		Unset all allowed areas.

Command	Description	Example

partset [<area list>]
p [<area list>]
partset2 [<area list>]
p2 [<area list>]
	Part set areas. Parameters are equal to the Set command.	`partset`
		Part set all allowed areas.
		`partset 1`
		Part set area 1.
		`p 2 3 5`
		Part set areas 2, 3, and 5.
		`p all`
		Part set all allowed areas.

forceset [<area list>]
fs [<area list>]
	Forced set areas. Parameters are equal to the Set command.	`forceset`
		Forced set all allowed areas.
		`forceset 1`
		Forced set area 1.
		`fs 2 3 5`
		Forced set areas 2, 3, and 5.
		`fs all`
		Forced set all allowed areas.

forcepartset [<area list>]
fp [<area list>]
	Forced part set areas. Parameters are equal to the Set command.	`forcepartset`
		Forced part set all allowed areas.
		`forcepartset 1`
		Forced part set area 1.
		`fp 2 3 5`
		Forced part set areas 2, 3, and 5.
		`fp all`
		Forced part set all allowed areas.

zone <zone list>
zn <zone list>
	Get zone details.
	The command returns zone name, areas that the zone belongs to, and zone type, for each zone in the list.
	Up to 10 zone entries can be returned.
		`zone 2`
		Get details for zone 2.
		`zn 2 3 5`
		Get details for zones 2, 3, and 5.

zone status [<area list>]
zs [<area list>]
	Get open and inhibit status of all zones in the areas listed.
	If <area list> is “all”, or is omitted, this is equivalent to a list of all areas for which the user has rights for the selected action.
		`zone status`
		Get status for all zones in all allowed areas.
		`zone status 1`
		Get status for zones of area 1.
		`zs 2 3 5`
		Get status for zones of areas 2, 3, and 5.
		`zs all`
		Get status from all zones in all allowed areas.

Command	Description	Example

zone faults [<area list>]
zf [<area list>]
	Get fault, tamper, and isolate status of all zones in the areas listed. Parameters are equal to the Zone Status command.	`zone faults`
		Get faults for all zones in all allowed areas.
		`zone faults 1`
		Get faults for zones of area 1.
		`zf 2 3 5`
		Get faults for zones of areas 2, 3, and 5.
		`zf all`
		Get faults from all zones in all allowed areas.

inhibit <zone list>
inh <zone list>
	Inhibit listed zones.	`inhibit 2`
		Inhibit zone 2.
		`inh 1 2 3 7`
		Inhibit zones 1, 2, 3, and 7.

uninhibit <zone list>
uninh <zone list>
	Uninhibit listed zones.	`uninhibit 2`
		Uninhibit zone 2.
		`uninh 1 2 3 7`
		Uninhibit zones 1, 2, 3, and 7.

isolate <zone list>
iso <zone list>
	Isolate listed zones.	`isolate 2`
		Isolate zone 2.
		`iso 1 2 3 7`
		Isolate zones 1, 2, 3, and 7.

unisolate <zone list>
uniso <zone list>
	Unisolate listed zones.	`unisolate 2`
		Unisolate zone 2.
		`uniso 1 2 3 7`
		Unisolate zones 1, 2, 3, and 7.

event [<type>] [<num>]
ev [<type>] [<num>]
	Get a selected event.
	Events are numbered starting from the most recent (1).
	Type can be one of the following:
	• “Mandatory” or “m”: mandatory events
	• “Nonmandatory” or “n”: non-mandatory events
	• “Installer” or “i”: installer events
	• “Access” or “a”: access events
	• “All”: all events
	If the <type> parameter is omitted, only the mandatory events are listed.
	If the number is omitted, the most recent event is returned.
		`event 23`
		Get mandatory event 23.
		`event access 3`
		Get access event 23.
		`ev all`
		Get the last event.
		`event all 13`
		Get event 13.
		`ev`
		Get the last mandatory event.

Command	Description	Example

events [<type>] [<num1>] [<num2>]
evs [<type>] [<num1>] [<num2>]
	Get events from the range, including <num1> and <num2>.
	Type usage is equal to the "event" command, with the following exceptions:
	• If one number is omitted, all events up to <num1> are returned (or <num1> of most recent events).
	• If both numbers are omitted, 10 most recent events are returned (1 to 10).
	Up to 25 events can be returned.
		`events 23`
		Get mandatory events from 1 to 23.
		`events access 3 13`
		Get access events from 3 to 13.
		`ev all`
		Get 10 last events.
		`event all 13`
		Get events 1 to 13.
		`ev 2 50`
		Get events 2 to 26 (only 25 events can be returned).

on <trigger list>	Activate listed triggers.	`on 1`
		Activate trigger 1.
		`on 2 5 6`
		Activate triggers 2, 5, and 6.

off <trigger list>	Deactivate listed triggers.	`off 1`
		Deactivate trigger 1.
		`off 2 5 6`
		Deactivate triggers 2, 5, and 6.

toggle <trigger list>	Toggle listed triggers states.	`toggle 1`
		Toggle trigger 1.
		`toggle 2 5 6`
		Toggle triggers 2, 5, and 6.

trigger <trigger list>
trig <trigger list>
	Get trigger names and states.	`trigger 1`
		Get trigger 1 name and state.
		`tr 2 3 5`
		Get names and states for triggers 2, 3, and 5.

output <num>
out <num>
	Get output state.	`output 3`
		Get output 3 status.
		`out 7`
		Get output 7 status.

outputs [<output list>]
outs [<output list>]
	Get listed outputs states.	`outputs 3`
		Get output 3 status.
		`outs 7 8 11`
		Get status of outputs 7, 8, and 11.

start reporting [<num>]
start [<num>]
	Start SMS reporting to the user <num>, or for the sender, if <num> is omitted [2][3].	`start reporting 6`
		Start reporting for user 6.
		`start`
		Start reporting for yourself.

stop reporting [<num>]
stop [<num>]
	Stop SMS reporting to the user <num>, or for the sender, if <num> is omitted, until the next system set [2][3].	`stop reporting 6`
		Stop reporting for user 6, until the next system set.
		`stop`
		Stop SMS reporting for yourself, until the next system set.

Command	Description	Example

stop reporting permanent [<num>]
stop perm [<num>]
	Stop SMS reporting to the user <num>, or for the sender, if <num> is omitted, until started again via the “start reporting” command [2][3].	`stop reporting permanent 6`
		Stop reporting for user 6, until it is allowed by the “start reporting” command.
		`stop perm`
		Stop reporting for yourself, until started again.

register <phone> <num>
r <phone> <num>
	Change phone number of the user <num> to the new <phone> [1].
	Note: You cannot change your own phone number using this command. Use “Phone” command instead.
		`register +48555223322 6`
		Change phone number of user 6 to the new one.
		`r +48223322555 9`
		Change phone number of user 9 to the new one.

unregister <num>
unr <num>
	Delete phone number of the user <num> [1].
	Note: You cannot delete your own phone number using this command.
		`unregister 6`
		Delete phone number of user 6.
		`unr 9`
		Delete phone number of user 9.

phone <phone>	Change own phone number to <phone>. The command must be sent from the old (currently registered) phone number. The registered phone is changed permanently once the next valid command is sent from the new phone number. If the next valid command is sent from the old phone number, the operation is cancelled.	`phone +48555223322` Change the registered phone number of the sender for the new one. The next command must be sent from the +48555223322.

pin <PIN> [<num>]	Change PIN for the user <num>, or for the sender, if <num> is omitted [2].	`pin 1234 6`
		Set user 6 PIN to 1234.
		`pin 4321`
		Set own PIN to 4321.

disable <num>
dis <num>
	Disable SMS control for the user <num> [1][4].	`disable 6`
		Disable control for user 6
		`dis 9`
		Disable control for user 9

enable <num>
en <num>
	Enable SMS control for the user <num> [1][4].	`enable 6`
		Enable control for user 6
		`en 9`
		Enable control for user 9

user <num>	Get user <num> details [1].
	The command returns user name, phone number, language, SMS control and reporting privileges.
		`user 6`
		List user 6 details
		`u 9`
		List user 6 details

Command	Description	Example

users [<num 1> <num2>]	List users from <num 1> to <num2> range together with their phone numbers, SMS control and reporting privileges [1].
	If the user range is omitted, the list contains only the users that belong to the user groups with “SMS reports allowed” or “SMS control allowed” privileges set.
		`users 6 9`
		List users from 6 to 9 and their phone numbers.
		`users`
		List all users that have “SMS reports” and “SMS control” allowed.

language <language> [<num>]	Change language of the user <num>, or for the sender, if <num> is omitted.
	<Language> is the localized language name, for example, English, Deutsch, Suomi.
		`language english 6`
		Set language for user 6 to English.
		`language polski`
		Set own language to Polish.

credits cr	Get GSM network credit information [1]. The answer format may vary for different GSM operators.	`cr` Get credit information.

connect <num>
conn <num>
	Start remote PC connection <num> [1]	`connect 2`
		Start PC connection 2.
		`conn 4`
		Start PC connection 4.

help	Get list of the allowed SMS commands.	`help` Get command list

[1] Only the Supervisor can execute this command.

[2] Non-supervisor users can perform this operation only for themselves. Only the Supervisor can execute this command for a different user than himself.

[3] The command affects the “SMS reporting” option in the user settings. The command can be performed only for those users that are allowed to receive SMS reports, for example, the user belongs to the User Group with the SMS reporting allowed.

[4] The command affects “SMS control” option in User settings. The command can be performed only for those users that belong to the User Group with SMS control allowed.

Glossary

Access control	The control of entry to, or exit from, a security area through doors.
Active	See “Normal / Active / Tamper / Inhibited / Isolated / Anti-mask”.
Alarm	The state of a security system when a device connected to a zone is activated and the condition of the area is such that activation should be signaled. For example, a door lock is broken, causing a siren to sound.
Alarm reporting	A procedure to transmit alarm events or other events to a central station by means of a dialer and a set of rules called a protocol.
Alarm control	The control over alarm functions.
Area	A section of premises that has specific security requirements. The Advisor Advanced system allows any premises to be divided into different areas having different security requirements. Each area has its own zones. Each area is identified by a number and a name. For example, Area 1 Office, Area 2 Workshop, Area 3 Boardroom, etc.
Armed	See “Set”.
Arming station (RAS)	A device that is the user control panel for security options for areas or for access points (doors). The arming station can be an Advisor console (LCD keypad, reader) or any other device that can be used to perform security function, such as set/unset, open doors, etc.
Autoset	An automatic setting of the premises started by a schedule or an exception. See Schedule, Exception.
Burglar alarm	An alarm triggered by a security device like a PIR or door contact, indicating someone has entered without authorized access. May also be referred to as an intrusion alarm.
Card	A medium holding credentials by which a user can be identified in a security system. A card is associated in the user configuration to a user by which the access rights are defined. Also referred to as a badge. Cards are used on readers or keypads with built-in readers.
Central station	A company that monitors whether an alarm has occurred in a security system. A central station is located away from the premises/area it monitors.
Condition filter	A set of rules that is created by logic inputs and logic equations. Used to control outputs and user groups.
Control panel	An electronic device that is used to gather all data from zones on the premises. Depending on programming and status of areas, it generates alarm signals. If required, alarms and other events can be reported to a central station.
DGP	Data gathering panel. A device that collects data from other security devices within an area, and transfers it to the Advisor Advanced control panel.
Dialler	An electronic device that allows the Advisor Advanced system to transmit alarms and other events to a central station. Can also be used to perform up/download.
Disarm	See “Unset”.
Door contact	A magnetic contact used to detect if a door or window is opened.
Door control	The control of doors. Part of access control features.

Dual	Dual detector. A security device used to detect intruders in a certain part of an area or premises. The technique used is based on two techniques like PIR and RADAR or PIR and Ultrasonic.
Duress	A situation where a user is being forced to breach the system security (for example, forced at gunpoint to open the door). The Advisor Advanced duress facility allows a signal to be activated (for example, notification to a central station) by the user. This is done by entering a duress digit in conjunction with a PIN.
Engineer	Personnel from an installer that is able to install and service the control panel.
Exception	Particular time periods when a schedule is extended or changed.
Fire alarm	An alarm triggered by fire or smoke detectors indicating a fire.
History	A list of past alarm and access control events stored in memory that can be viewed on an LCD arming station.
Hold-up	A (silent) alarm that is triggered by a hold-up button. Normally it does not trigger any siren, only sends a message to a central station. May also be called Panic Button.
Inhibit	See “Normal / Active / Tamper / Inhibited / Isolated / Anti-mask”.
Installer	A company that installs and services security equipment.
Keypad	A remote arming station with keys to input data (keypad). Used to program the control panel, perform user options, view alarms, etc.
Key switch	A device using a switch to set or unset areas. The switch needs a key to switch.
LCD	Liquid crystal display. The part of an arming station where messages are displayed.
LED	Light emitting diode. A light indicator on an arming station that conveys a condition. For example, area in alarm, communication fault, etc.
Normal / Active / Tamper / Inhibited / Isolated / Anti-mask	Describes the condition of a zone. • Normal: The zone is NOT activated. For example, Fire Exit Door closed. • Active: The zone is activated. For example, Fire Exit Door open. • Tamper: The zone is open or short-circuited. Someone may have tried to tamper the security device. • Inhibited: The zone has been inhibited from indicating normal or active status. It is excluded from functioning as part of the system for particular time. However, it is still monitored for tamper alarms. • Isolated: The zone has been inhibited from indicating normal or active status. It is excluded from functioning as part of the system permanently. • Ant-mask: The detector is masked.
Nuisance alarm	An alarm that is triggered by a security device, without any burglar. It could be caused by open windows, pets or incorrect projection of security equipment.
Online / offline	Operational/non-operational. A device may be offline due to a malfunction in the device itself or it may be disconnected from the control.
Output expander	A PCB module that connects to the Advisor Advanced control panel or a DGP to provide relay or open collector outputs.
Panic button	See hold-up.

Part set	The condition of part of an area where a change in the status of certain zones (from normal to active) causes an alarm. An area or premise is part set when it is partially unoccupied like the outside of a home is part set but the inside is still unset.
PIN	A 4 to 10 digit number given to, or selected by, a user. It is necessary to enter a PIN on an Advisor keypad as a prerequisite to perform most Advisor Advanced options. In the Advisor Advanced configuration the PIN is associated with a user number that identifies the PIN holder to the system.
PIR	Passive infrared detector. A security device used to detect intruders in a certain part of an area or premise. The technique used is based on infrared detection.
Poll	An inquiry message continually sent by the Advisor Advanced control panel to DGPs and arming stations. Polling allows the remote unit to transfer data to the control panel.
RAS	Remote arming station. See “Arming station”.
Reader	A device used for access control that can read cards to allow access. Depending on the needs and the type of cards, the reader can for example be a magnetic swipe reader or proximity reader. May be integrated into a keypad.
Reporting	See “Alarm reporting”.
Request to Exit zone	A zone that is programmed to open a door using a button or PIR. Used to allow users to exit without using the door reader. Request to exit is often abbreviated to RTE. Also called egress.
Schedule	A timed set of actions with a weekly structure.
Set	The condition of an area where a change in the status of any zone (from normal to active) causes an alarm. An area or premise is only set when it is unoccupied. Some zones (like vaults) can remain armed continually.
Tamper	A situation where a zone, an arming station, control panel, DGP or associated wiring are tampered with, or accidentally damaged. The Advisor Advanced tamper facility activates a signal when tamper occurs. Tamper alarms from zones are called zone tampers.
Unset	The condition of an area when it is occupied and normal activity does not set off an alarm.
Up/Download	A protocol providing means to view the status of an Advisor Advanced system or change parameters in the system either local or remote.
User	Anybody making use of the Advisor Advanced system. Users are identified to the Advisor Advanced system by a unique number that is associated with the user’s PIN.
User group	User groups define the options and permissions available to users.
Walk test	A test performed by a user or installer. To pass the test, the user or installer has to walk past detectors to activate these. The intention is to test the functionality of the security system.
Zone	An electrical signal from a security device (PIR detector, door contact) to the Advisor system. Each device is identified by a zone number and name. For example, 14 Reception Hold-up Button, 6 Fire Exit Door.

Index

User menu map

- 1 Inhibit zones
- 2 Isolate
  - 2.1 Isolate zones
  - 2.2 Isolate DGP / 2.3 Isolate RAS
- 3 View logs
  - 3.1 All
  - 3.2 Mandatory
  - 3.3 Non mandatory
  - 3.4 Installer
  - 3.5 Access
- 4 Panel status
  - 4.1 View open zones
  - 4.2 Alarms
  - 4.3 Faults
- 5 Change PIN
- 6 SMS & Voice
  - 6.1 User phone
  - 6.2 SMS reporting
  - 6.3 SMS control
- 7 Users
  - 7.0 Add user
  - 7.n Edit user
    - 7.n.1 User name
    - 7.n.2 Change PIN
    - 7.n.3 User card
    - 7.n.4 Language
    - 7.n.5 User groups
    - 7.n.6 SMS & Voice
      - 7.n.6.1 User phone
      - 7.n.6.2 SMS reporting
      - 7.n.6.3 SMS control
    - 7.n.7 Remove user
- 8 Service
  - 8.1 Time&date
    - 8.1.1 Time zone
    - 8.1.2 Date
    - 8.1.3 Time
    - 8.1.4 DST start mth
    - 8.1.5 DST start wk
    - 8.1.6 DST end mth
    - 8.1.7 DST end wk
    - 8.1.8 Set correction
      - 8.1.8.1 Mode
      - 8.1.8.2 Time/7days
  - 8.2 Walk test
  - 8.3 Manual test
  - 8.4 Sirens test
    - 8.4.1 Internal siren
    - 8.4.2 External siren
    - 8.4.3 Strobe
  - 8.5 Communication
    - 8.5.1 CS (central station)
      - 8.5.1.n Select central station
        - 8.5.1.n.1 Phone
    - 8.5.2 PC connection
    - 8.5.3 Credit
  - 8.6 Doorbell
  - 8.7 Engineer reset
  - 8.8 Service In

- 9 Calendar
  - 9.1 Actions
    - 9.1.n Select action
      - 9.1.n.1 Action name
      - 9.1.n.2 Start time
      - 9.1.n.3 Action filter
      - 9.1.n.4 Active
      - 9.1.n.5 Function
  - 9.2 Action lists
    - 9.2.n Select action list
      - 9.2.n.1 Action list name
      - 9.2.n.2 Active
      - 9.2.n.3 Action list
  - 9.3 Exceptions
    - 9.3.n Select exception
      - 9.3.n.1 Exception name
      - 9.3.n.2 Start date
      - 9.3.n.3 Stop date
      - 9.3.n.4 Substitute
      - 9.3.n.5 Active
      - 9.3.n.6 Actions
      - 9.3.n.7 Action lists
  - 9.4 Schedules
    - 9.4.n Select schedule
      - 9.4.n.1 Schedule name
      - 9.4.n.2 Week days
      - 9.4.n.3 Exceptions
      - 9.4.n.4 View
        - 9.4.n.4.1 Current view
        - 9.4.n.4.2 Date view
  - 9.5 Active schedule
  - 9.6 View