

NGP Essential

Installation Guide



Contents

Introduction	3	Configuration	16	Interconnection monitoring	30
Specifications	5	Pin Learn	17	Interconnection monitoring	31
Safety notes	7	Configuration menu programming	17	End of Line	31
Mounting and wiring	8	Button configuration	18	What happens when pins are configured and wired in this way	32
Removal of cover	9	Main menu display	19	Panel upload Download and Enhanced format signalling (SIA/CID)	33
Mounting	9	Inputs	21	Dial Capture	33
Connection terminals	10	Input Sense	22	Serial panel connections	33
Power connections	10	Inputs EOL (End of Line mode)	23	Connection advice	34
Alarm inputs	10	Outputs	24	Alarm list	35
Outputs	11	Network	25	Personal Data	37
Serial data connections	11	Serial connection panel type	26	Disposal	38
Dial capture	11	Offline reboot screen	28	Glossary	39
Programming	12	Restore defaults	28	Approvals	40
Unit initialisation	13	Web portal and AddSecure app	29	Appendix	43
Status display	13	Firmware updates	29		
Signal strength	14	Compliance with the user access level requirements of EN 50136	29		
Guide to signal strength	14				
Path status	14				
Pin inputs	15				
Output 2 (FUNC)	15				



Introduction

Introduction

Product description

The Addsecure NGP Essential unit is a wireless single path, roaming SIM, alarm signalling unit for transmitting alarm signals from a customer's alarm panel, via the Addsecure network to an Alarm Receiving Centre (ARC) using pass-through mode of operation. The NGP Essential unit has a UK roaming SIM with 4G/2G mobile technology.

The unit communicates via the Addsecure network and a valid TA (Terminal adapter) account must exist for the unit to communicate. The TA account will have been populated with the serial number of the unit. Once connected to the platform the unit uses a poll and response check to determine

path status. Path fail alarm is platform generated. The unit has 8 general purpose alarm inputs, and 2 outputs, making it suitable for connection to most common alarm panels.

The unit is supplied already fitted with a Addsecure enabled SIM card.

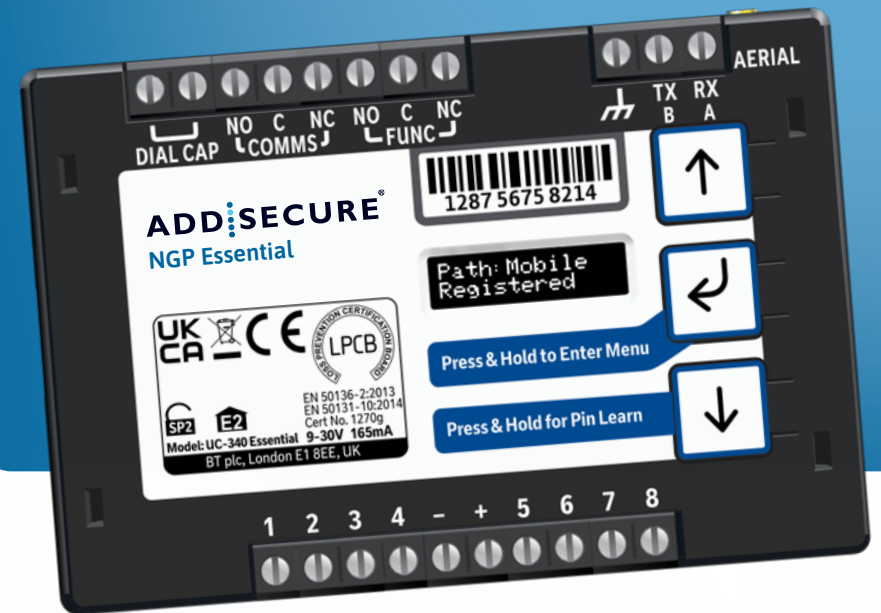


Figure 1 – NGP Essential unit (not to scale)

Specifications

NGP Essential	
Primary path fail reporting	60mins
Alarm transmission category EN standards / PD6669 (UK)	SP2
PD6669, EN50131 (2017) Grade	2
Grade option (Table 10 EN50131-1 2020)	2A, 2B
Environmental class	II
Information and substitution security	AES256

Current	Average Normal Operation	Average Max loading (inc relays and dial capture operated)
2G/4G unit @12V	70mA	165mA
Size:	95mm x 67mm x 17mm	
Weight:	73g	
Power:	9V – 30V	

INTRODUCTION

Alarm inputs:	8 General purpose inputs 1–8. (-0.5V – 30V)	
Alarm threshold:	High >2V, and Low <1.3V	
Outputs:	2 x Relay NO C NC (COMMS, FUNC). Max rating 1A @ 30V DC	
RS232 port:	Remote panel access (UDL) and signalling to some intruder panel types	
RS485 port:	Remote panel access (UDL) and signalling to some intruder panel types	
Configuration:	Using on-board configuration buttons, web portal or App	
Processor:	STM32	
Wireless module:	ELS61	ELS62
GSM/GPRS/EDGE:	Dual band 900/1800MHz, maximum transmit power +34.5dBm	850 (BdV) / 900 (BdVIII) / 1800(BdIII) / 1900 (BdII). Maximum power transmit +35.5dBm
LTE:	Penta-Band 700 (Bd28)/800 (Bd20)/900 (Bd8)/1800 (Bd3)/2100 MHz (Bd1), maximum transmit power +24dBm	2100(Bd1) / 1900(Bd2) / 1800(Bd3) / 2100(Bd4) / 850(Bd5) / 2600(Bd7) / 900(Bd8) / 800(Bd20) / 700(Bd28) / TDD2600(Bd38) / TDD2300(Bd40) / TDD2500(Bd41)2 / 2100(Bd66). Maximum power transmit +25.7dBm
Operating range:	-10 to +50 degrees Celsius, average 90% non condensing humidity	

Safety notes

Work area safety

- Keep work area clean, well lit and free of obstacles.
- Keep floor and walkways clear of cables and materials to avoid trip hazards.
- Keep children and bystanders away while performing installation and maintenance work.
- Remove any left over materials when finished and keep all items away from children and pets.

Personal safety

- Stay alert and attentive. A moment of inattention may result in personal injury.
- Do not perform installation or maintenance work when tired or under the influence of medication, drugs or alcohol.
- Upon commencing work on security system enclosures and components, ensure the item is securely fixed to

the wall and that no components or contents such as the battery can fall and cause personal injury.

Electrical safety

- Exercise care when working inside security system enclosures:
 - Metallic tools, fingers, body parts or jewellery coming into contact with mains wiring and terminals may cause electric shock.
 - Metallic tools or jewellery coming into contact with battery terminals may cause sparks, personal injury or create a fire risk.
- Exercise care when drilling into, or inserting fasteners into walls. Pipes and wiring may be present in the wall and contact with tools or fasteners may provide risk of electric shock, damage to premises services, or create a fire risk. Locate wiring, pipes and services first to avoid accidents.

WARNING!

Read all safety warnings and instructions. Failure to heed warnings and follow instructions may result in electric shock, fire risk and/or personal injury.



Mounting and wiring

Mounting and wiring

Removal of cover

The top cover can be removed by gently releasing each of the 4 clips on the base of the unit by pushing the clips outward with a screwdriver blade.

Regular access to the inside of the unit should not be required, although occasional access may be required to access the SIM card.

Mounting

The unit should be mounted inside a suitable robust enclosure, using the sticky mounting pads supplied. For security installations the enclosure must meet or exceed the protection requirements of the particular security grade for the whole installation as per EN 50131-1. For all installations access to the unit needs to meet EN50131-1 installer access level 3.

For optimum performance the supplied aerial should be mounted vertically outside of and away from the housing by removing the adhesive backing. Ideally the aerial should not be mounted on a metal surface. The aerial should be installed a distance of 20cm or greater away from any user or bystander.

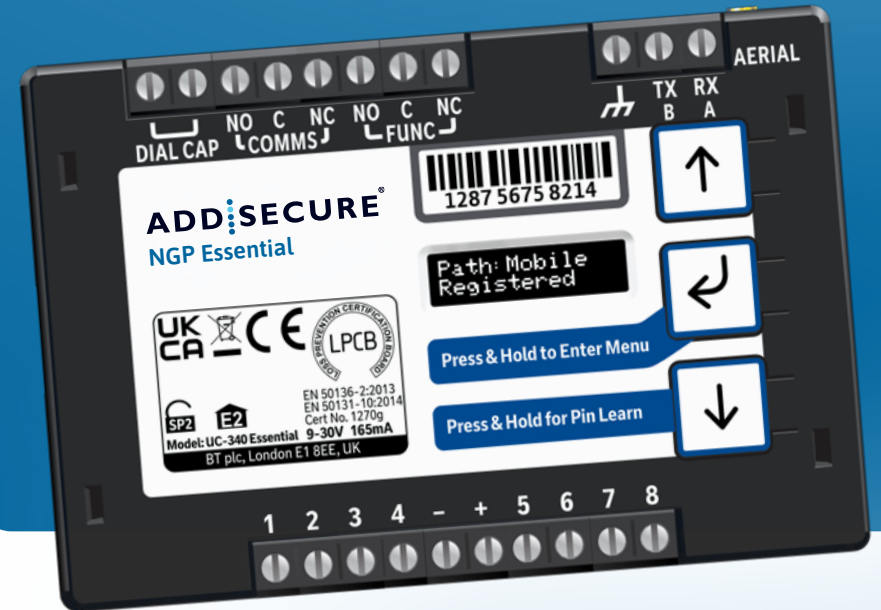


Figure 2 – Layout of terminals (not to scale)

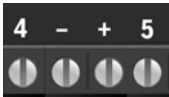
Connection terminals

The screw terminals for the alarm inputs are suitable for use with a standard 3mm blade terminal screwdriver.

Power connections

Power to the unit is via 2 screw terminals at the centre, with positive to the right nearest Pin 5. The supply voltage range is 9V to 30V. The unit is designed to be connected to the auxiliary power output on an associated alarm panel, or separate powered enclosure. For use with intruder alarm panels the power supply must meet the requirements of EN 50131-6.

Ensure the power source is sufficient to power all devices connected. *See the power requirements in the specification section.* The account at the Alarm Receiving Centre (ARC) should be put 'on test' before power up, as signals will be sent following initialisation.



Alarm inputs

The unit has 8 alarm inputs which are presented on screw terminals along the bottom of the unit. These are labelled as Pin 1-4 and 5-8.

By default the 8 alarm inputs require a positive condition to be presented to send an alarm. (Default = Positive applied). This can be changed using the Pin Learn button or through the configuration menu. *See later section on Configuration.*



Input (Pin)	Use
1	
2	Hold up alarm
3	Intruder alarm
4	Open / Close (Set / Unset)
5-8	General alarm

Figure 3 – Alarm input allocations. (Functions must be agreed with your ARC).

Outputs

Two relay outputs are provided on screw terminals at the top of the unit. Output 1 is COMMS, Output 2 is FUNC. See the further sections on outputs for a full explanation.

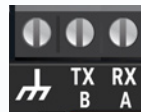


Serial data connections

The serial data connection labelled TX, RX, B and A is configurable for RS485 or RS232 connection depending on the panel.

This is done in the configuration menu. These ports allow serial alarm panel connection.

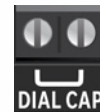
See the Panel Upload-Download section.



Dial capture

The Dial Capture (Dial Cap) terminals enable interfacing with an alarm panel's digital communicator. The alarm panel can then send SIA, CID or Fast Format messages through the unit to the Alarm Receiving Centre.

Dial Capture can also be used for upload download UDL allowing remote access with some types of alarm panel.



Aerial connection

Connect the supplied aerial to the MMCX connector on the top right of the unit.

The aerial should be placed in a vertical position that receives the best wireless coverage. Carry out a survey to establish the best location. If necessary, a mobile signal analyser, selection of high gain and extension aerials can be purchased via your ARC.



Programming

Simple set up, out of the box

Programming

Unit initialisation

The unit will immediately attempt to connect to the Addsecure platform over the mobile path.

The unit will typically complete path establishment in the following time from power up.



Figure 4 – Time to commission paths after unit power up

The unit sends a ‘System Reset’ event (Pin 984,1), followed by a ‘Unit Restarted’ restore (Pin 984,3) within two seconds. The unit also sends the state of all 8 pins and low battery alarm restore. Sending these alarm states at start up helps to ensure that the ARC alarm handling software reflects the true state of all pin alarms after start up.

Status display

The unit clearly displays its status on the OLED. In its normal working state, the unit will cycle its display.

Path: Mobile Registered

Mobile Path and if registered with the platform.

Signal Strength 4G[■ ■ ■] [-103]

Signal strength – network type (4G or 2G) received wireless signal strength in dBm and signal strength indicator bars. Two bars or more is the recommended signal level required.

Service Grade Redcare SP2

Service Grade – The EN Performance category SP2 will be shown.

Mobile1 Operator EE

Shows the mobile network that the device is connected to.

The performance category can only be determined by the unit while in contact with the platform. The unit will not show the performance category until the mobile path is registered with the platform when it will retrieve the performance grade.

Alarms GPI Alarm 3

Pin status – any outstanding alarm pins will be shown. If no pins are in the alarm state, then pin status will not be shown.

Alarms Battery Low Battery

The unit may also show Low Battery if the supply voltage is below the supply threshold.

Signal strength

Signal strength	Display	Signal strength	Display
On 2G below -90dBm	X will be displayed	On 4G below -120dBm	X will be displayed
On 2G between -90 and -85dBm	1 bar will be displayed	On 4G between -120 and -110dBm	1 bar will be displayed
On 2G between -85 and -80dBm	2 bars will be displayed	On 4G between -110 and -100dBm	2 bars will be displayed
On 2G between -80 and -75dBm	3 bars will be displayed	On 4G between -100 and -90dBm	3 bars will be displayed
On 2G above -75dBm	4 bars will be displayed	On 4G above -90dBm	4 bars will be displayed

X or 1 bar – try to improve the signal by moving the unit, aerial or using an extn or high gain aerial – via your ARC.

Guide to signal strength



Figure 5 – Signal strength chart



Figure 6 – Typical display cycling on a fully commissioned unit with a good signal strength and Pin 4 in the alarm or open state.

Path status

The status of the communication path is indicated by the OLED display. The mobile path status has the following possible status:

- **Up No Reg** – Path is up but not registered with the platform.
- **Registered** – Unit has contacted the platform and successfully registered.
- **Alarm/ACK** – Alarm is being transmitted and awaiting acknowledgement.
- **Down** – The path has lost connectivity to the platform and is trying to reconnect.

NOTE: When fully commissioned the mobile path should be registered.

Pin inputs

Pin 4 can have an RPS output associated with it. (See output 2 RPS).

Pins 1 – 8 can be set up for end of line and dual end of line interconnection monitoring.

Outputs

Output 1 (COMMS)

Output 1 acts as the communications fault output.

Output 2 (FUNC)

Output 2 has three configuration options:

1. User control output:

This can be remotely operated via the web portal or app.

2. RPS output for Pin 4:

The output will operate when input Pin 4 is triggered. It will return when an acknowledge signal is returned from the Addsecure platform. The output has a minimum operation time of 1s. When the acknowledgement is received in less than one second after Pin 4 is triggered then the output will remain operated for 1s.

3. Keyswitch:

Set or unset the alarm system in conjunction with the Addsecure app.

Keyswitch Mode (Visible when output 2 set to Keyswitch)

- **Momentary** – Momentary pulse to allow set and unset of alarm panel with customer app.
- **Latched** – Latched output option to allow set and unset of panel with customer app. Used in conjunction when setting output 2 as Keyswitch.

If using the Keyswitch you will need to ensure the intrusion alarm system is set up to comply with the requirements of BS 8243 when implementing remote setting/unsetting via the app.

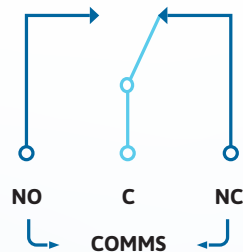
Default Outputs settings 1, 2 and 3:

- **Output 1** is set to single path fault.
- **Output 2** is set to User.

Output 1 operation as follows:

Condition	Output1	Relay Terminal
Power Off	Output1	C <-> NC
Path Up and Registered	Output1	C <-> NO
Path fail	Output1	C <-> NC

Relay status with path fail in operation





Configuration

Configuration

Pin Learn

For speed of installation a single button press Pin Learn is available. All pins to be used should be wired in and all the pins should be in the non alarm state. No tampers should be active (if wired in) and Pin 4 (open/close) should represent the system being set/closed.

When ready press and hold the down arrow for 3s. 'Notice – Done!' is displayed when finished. This has completed the Pin Learn. There is also an option to learn the pins within the configuration menu.

Configuration menu programming

The unit is supplied pre-configured with factory default values.

For most installations no changes to the configuration are required.



The unit can either be configured by using the on-board configuration menu driven by the buttons, or through the installer app or web portal. Some configurations are only available through the app or web portal. For use of the app or web portal remotely, written authorisation is required from a Level 2 user.

In the event log on the app or on the unit web page ** indicates a non-reportable event. If a single * is displayed by an event, this indicates no acknowledgement has been received.

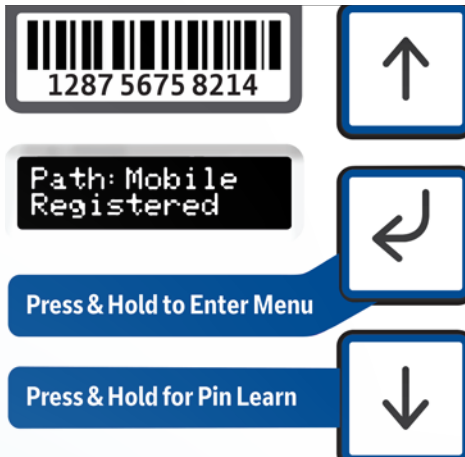
A minority of sites may require minimal configuration changes at installation, and most of these will be achievable through the button configuration, e.g.:

- Change the individual pin status.
- Enable dual end of line for interconnection monitoring.



Button configuration

The button configuration mode is entered by holding down the centre configuration button (Enter) for 3s.



When in the main menu, each press of will step to the next menu item down.

Use to step back up and eventually return to the top of the menu. The full main menu options are shown in Fig. 7.

The unit will then display 'Configuration'.

Configuration



Press the Enter button again and the display will show the first menu option.

Inputs



Pressing the Enter button on any menu item will enter the sub-menu and take you into edit mode. This will allow the function to be changed. Depending on the menu item will depend on the structure of the sub-menu.

Output Type 1* Single Path Fault

You know you are in edit mode and that changes can be made by a * next to the menu title.

Notice - Saved!

Typically, many menu items simply have two options, use the down and up arrow to switch between the two. Press and hold the Enter button to save changes. Display will show 'Notice – Saved!'

Some menu items have more options. E.g. Output 2 has three options to set the comms fault output type. On such menus, press the Enter button to enter the sub-menu, then use the down and up arrows to increment through the options with each press. Holding the Enter button for 5s will save changes. Display will show 'Notice – Saved!'

Some more complex menu items use the Enter button to also step through additional items in the sub-menu. E.g. Network Web Passcode to be changed.

Edit mode can be exited at any time, without saving changes, by pressing for 5s. This will return you to the sub-menu that you were making changes in.

The configuration menu can be exited at any time without saving any changes by pressing for 5s. This will take you back to the scrolling status display.



Main menu display

Main menu display

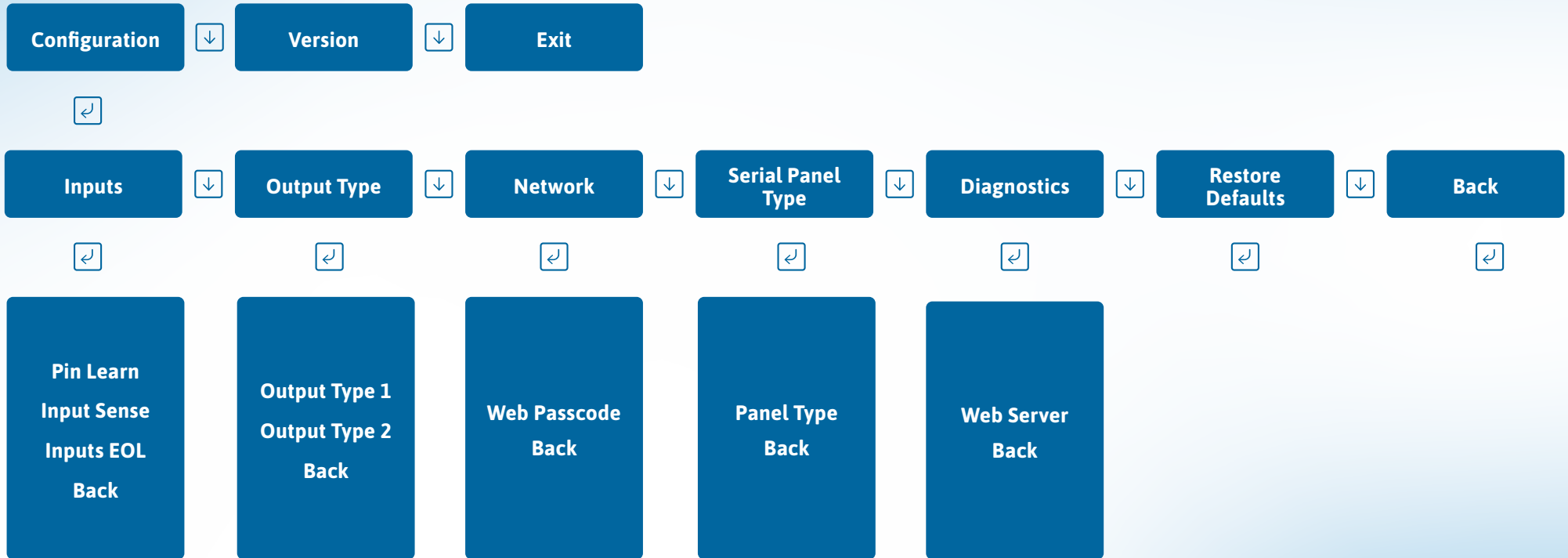


Figure 7 – Button configuration main menu options

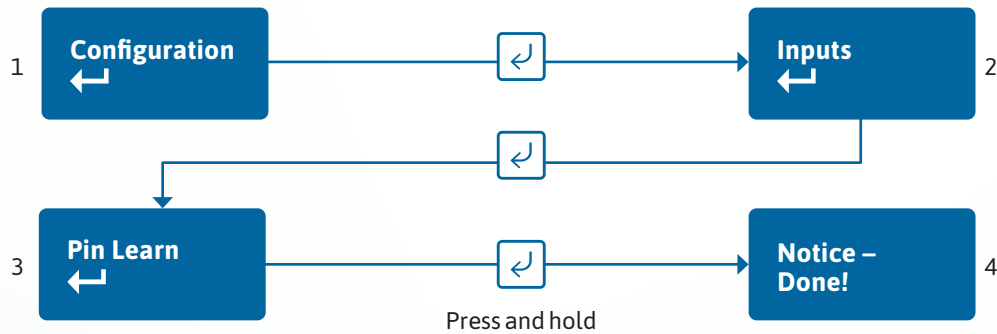
Inputs

Pin Learn

The polarity of pins can be learnt by pressing and holding the down arrow for 5s.

The display will show 'Notice – Done!' Pin Learn can also be carried out through the configuration menu.

Example – to learn the pin polarity in the configuration menu:



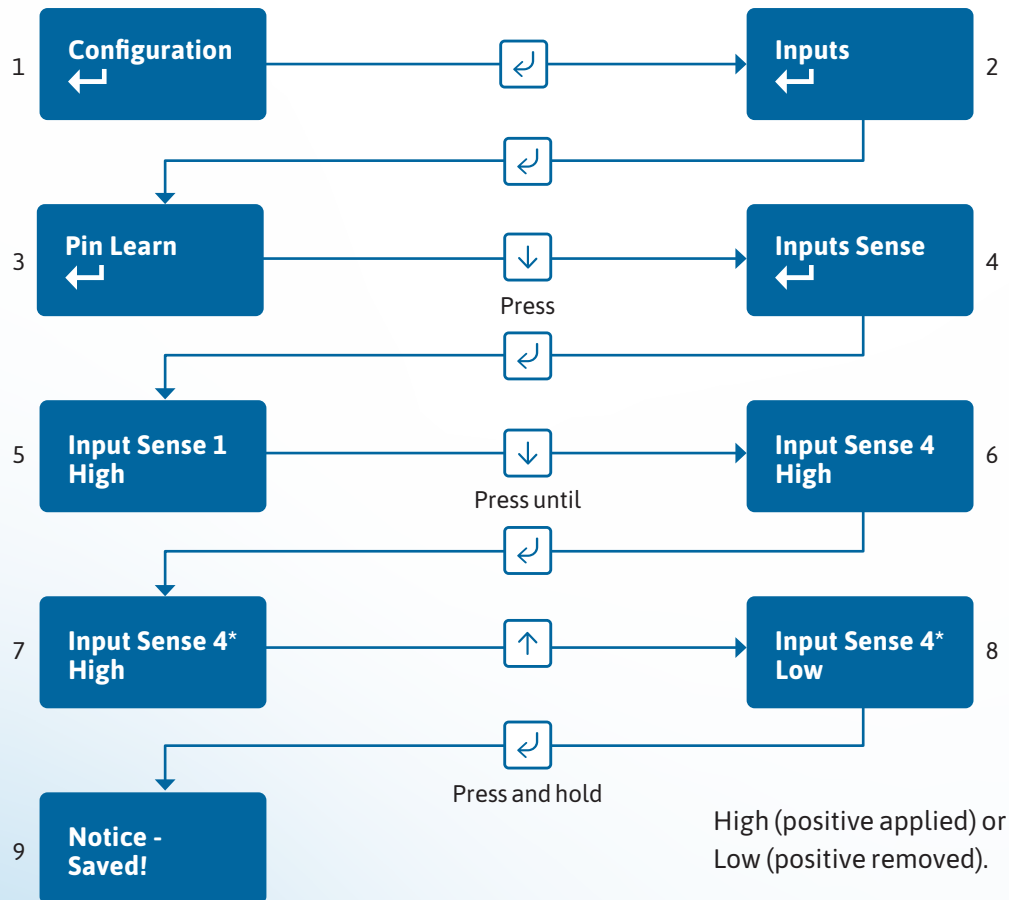
- Access the button configuration menu by holding the Enter button. 'Configuration' is displayed.
- Then press Enter again. The display will show 'Inputs'.
- Press Enter button again.
- The display now shows 'Pin Learn'.
- Press and hold the Enter button – the display shows 'Notice – Done!'.

The configuration menu can be exited at any time without saving any changes by pressing for 5s. This will take you back to the scrolling status display.



Input Sense

You can also manually configure the polarity of the pins. This is in addition to the Pin Learn function described earlier.



- Access the configuration menu by holding Enter button for three seconds, then press the Enter button again – the display will read. Press the Enter button again, the display will show Pin Learn. Press the down arrow. The display will show Input Sense. Press the Enter button again to enter Input Sense. Pin 1 and status will be shown.
- Use the down arrow to scroll through the pins. Once you reach the desired pin, press the Enter button. * will be displayed.
- Use down or up arrow to change to High or Low – High (positive applied) or Low (positive removed).
- Once selected, hold the Enter button down until 'Notice – Saved!' is displayed. Then it will return to the position in the menu for you to select another pin, or you can use the down arrow to scroll through all the pins to return to the Back option.

You can exit Edit mode at any time, without saving changes, by pressing for 5s. This will return you to the sub-menu that you were making changes in.

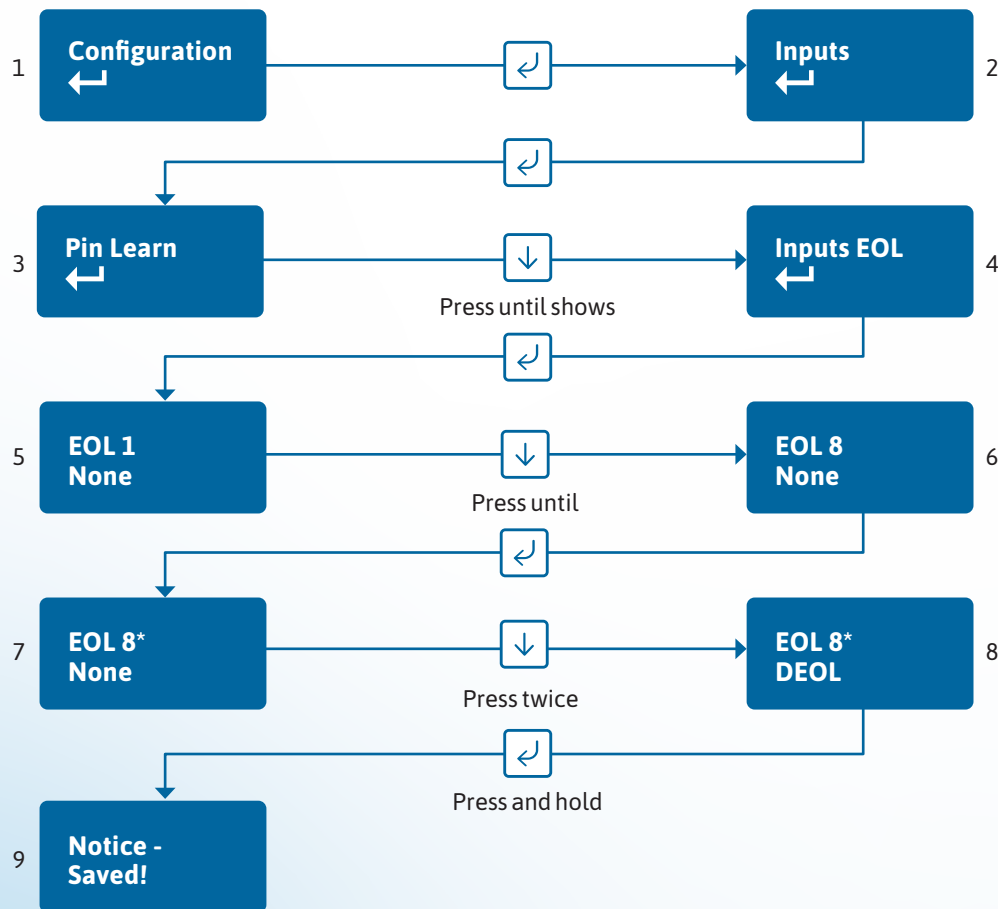
Exit the configuration menu at any time without saving any changes by pressing for 5s. This will take you back to the scrolling status display.

Inputs EOL (End of Line mode)

The alarm inputs (pins) can be set to the following modes:


- **None** – (Alarm and Restore)
- **EOL** (Single End of Line mode) – (Alarm, Restore and Cut)
- **DEOL** (Dual End of Line mode) – (Alarm, Restore, Cut and Short)


Example – configure Pin 8 for DEOL



This allows the unit to monitor the wiring to the alarm panel contacts.

- Access the configuration menu by holding the Enter button for 3s. Press the Enter button again, the display will show 'Pin Learn'. Press the down arrow twice. The display will show 'Inputs EOL'. Press the Enter button again to enter Input EOL. 'EOL 1 = None' will be shown.
- Use the down arrow to step through the pins. Once the desired pin is reached press the Enter button. * will be displayed. Use down or up arrow to change to None, EOL or DEOL.
- Once selected hold the Enter button down till 'Notice – Saved!' is displayed.
- Then it will return to the same position in the menu for you to select another pin or use the down arrow to step through all pins to get to the Back option.

Edit mode can be exited at any time, without saving changes, by pressing  for 5s. This will return you to the sub-menu that you were making changes in.

The configuration menu can be exited at any time without saving any changes by pressing  for 5s. This will take you back to the scrolling status display.

Outputs

1. Output type 1 (COMMS):

- **Single path fault** – Operates when the Mobile path is in fault.

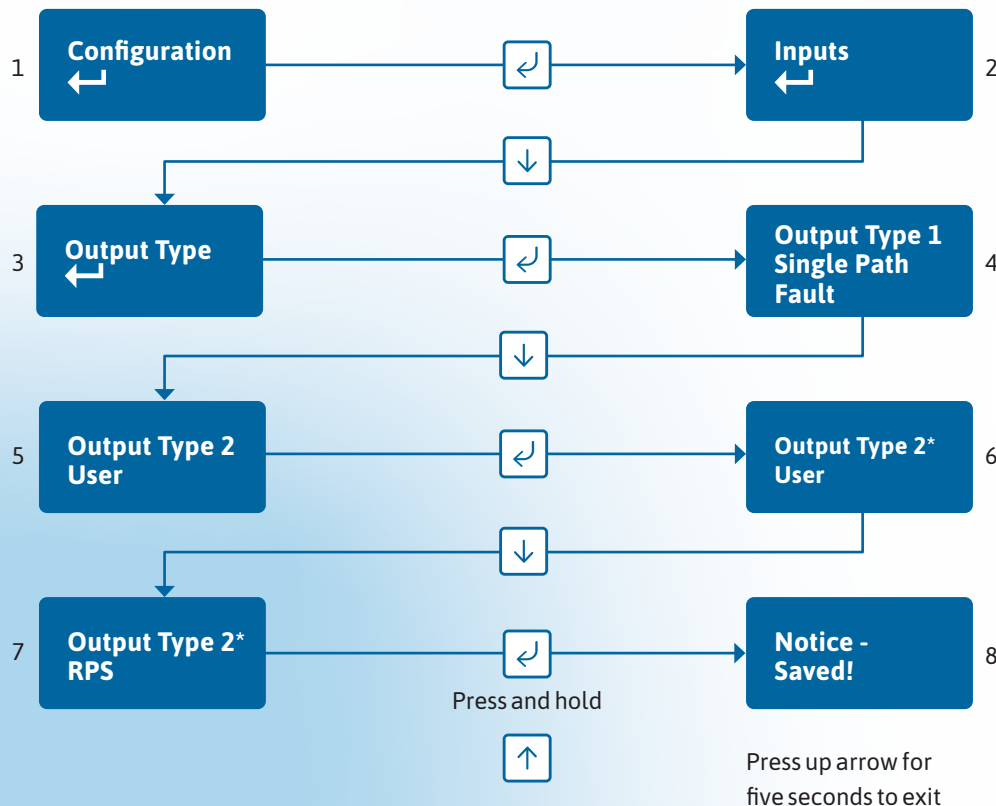
2. Output type 2 (FUNC):

- **User** – allow the relay to be operated remotely via the app or portal (default).
- **RPS** – return path signal operates in conjunction with Pin 4.
- **Keyswitch** – allows panel to be set/unset via the Addsecure customer app.

Keyswitch mode:

- **Momentary** – allow the FUNC relay, when set to Keyswitch, to be operated remotely via the app or portal by one pulse of the relay (default).
- **Latched** – allow the FUNC relay, when set to Keyswitch, to be operated remotely via the app or portal by latching the relay.

Example – configure Output 2 (FUNC) for RPS



- Access the configuration menu by holding the Enter button for three seconds. Press the Enter button again, the display will show Inputs. Press the down arrow until 'Output Type' is displayed. Press the Enter button again. The display will show the default setting for Output type 1. Use the down arrow to step through to Output type 2. Press the Enter button. * will be displayed. Use the down arrow to change to RPS.
- Once selected hold the Enter button down till 'Notice – Saved!' is displayed.
- It will return to the same position in the menu for you to select another output or use the down arrow to step through all options to get to the Back option.

Edit mode for that part of the menu can be exited at any time, without saving changes, by pressing for five seconds. This will return you to the sub-menu that you were making changes in.

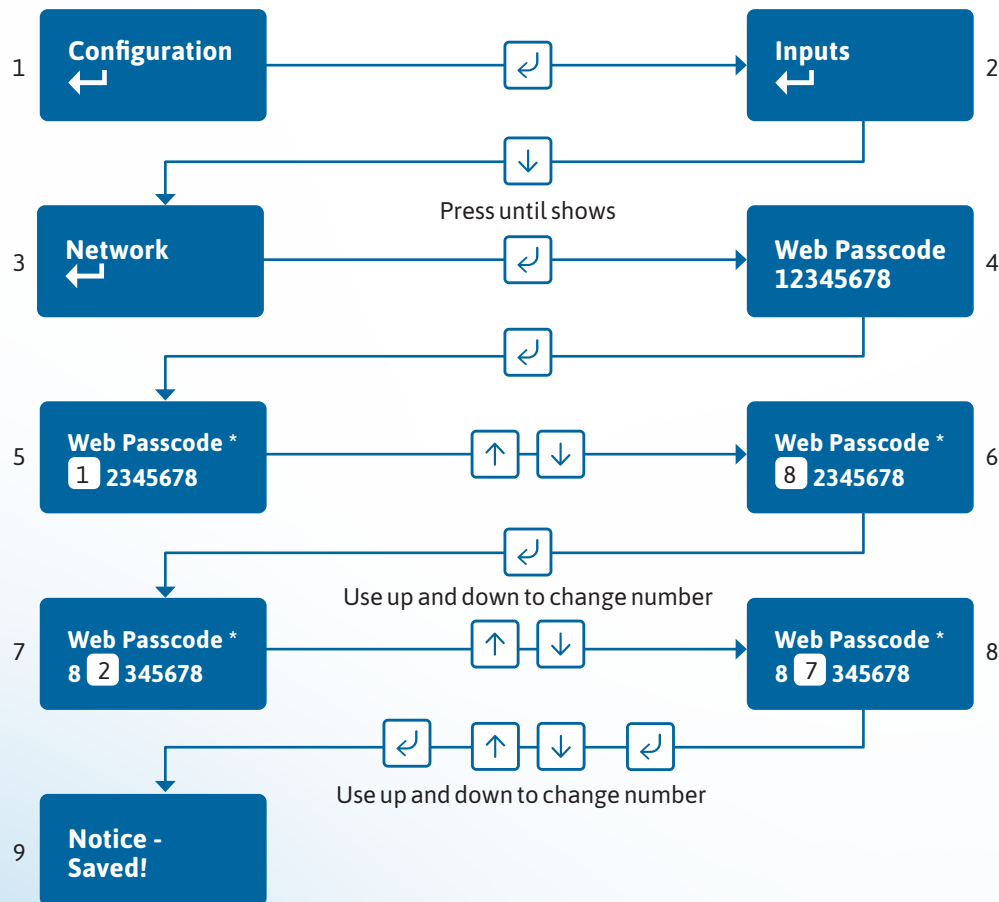
The configuration menu can be exited at any time without saving any changes by pressing for five seconds. This will take you back to the scrolling status display.

Network

The programming option under the network sub-menu is:

Web passcode

This code is used to set up both the installer and customer app. It can be changed from its default:



This passcode can be changed any time, if required, via this menu within settings.

For best practice, mobile app access requires the Installer to set up a Web passcode and pin in the device and then advise and show the end customer how to change the PIN.

Edit mode for that part of the menu can be exited at any time, without saving changes, by pressing for 5s. This will return you to the sub-menu that you were making changes in.

The configuration menu can be exited at any time without saving any changes by pressing for 5s. This will take you back to the scrolling status display.

Serial connection panel type

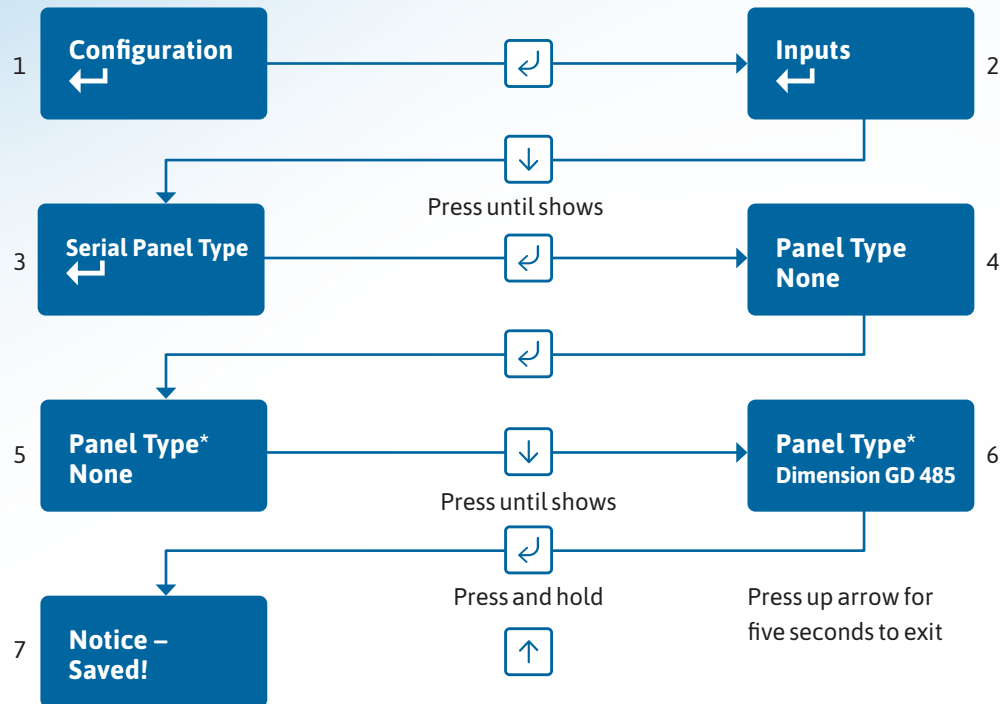
This menu selects the panel connection type for serial connected panels (RS232 or RS485).

Settings:

- None
- Dimension GD 232 (Galaxy Dimension 48/96/264/520 (RS232 9600 8n1))
- Dimension GD 485 (Galaxy Dimension 48/96/264/520 (RS485))
- Galaxy G3 232 (G3 48/144/520 (RS232 9600 8n1))
- Galaxy G3 485 (G3 48/144/520 (RS485))
- Galaxy G2 485 (G212/20/44 (RS485))
- Galaxy Classic 485 L (Classic 8/18/60/128 (RS485))
- Galaxy Classic 485 H (Classic 500/504/512 (RS485))
- Galaxy Flex 485
- Texecom 816 (Texecom 412/816/832 (RS232 19200 8n2 inv))
- Texecom 48 88 (Texecom 48/88/168 Com – IP (RS232 19200 8n2 inv))
- Texecom Premier (Texecom Premier Elite 48 Com-IP (RS232 19200 8n2 inv))
- Bespoke Panel
- Pyronix (RS232 9600 8n1) (Europe only not UK)
- Contact IP (RS232 9600/2400/1200 8n1)
- Panel RS232 UDL (8n1)
- Contact IPv2
- Eaton I-on



Example – changing the unit to connect to a Galaxy dimension panel via RS485.



- Access the configuration menu by holding Enter button for 3 seconds. Press the Enter button again, the display will show Inputs. Press the down arrow until serial panel type is shown. Press the Enter button again to enter serial panel type. 'Default status = None' will be shown.
- Use the down arrow to step through the available panel. Once the desired panel is reached press and hold the Enter button down till 'Notice – Saved!' is displayed.
- Then it will return to the same position in the menu for you to select a different panel or use the down arrow to step through all pins to get to the Back option.

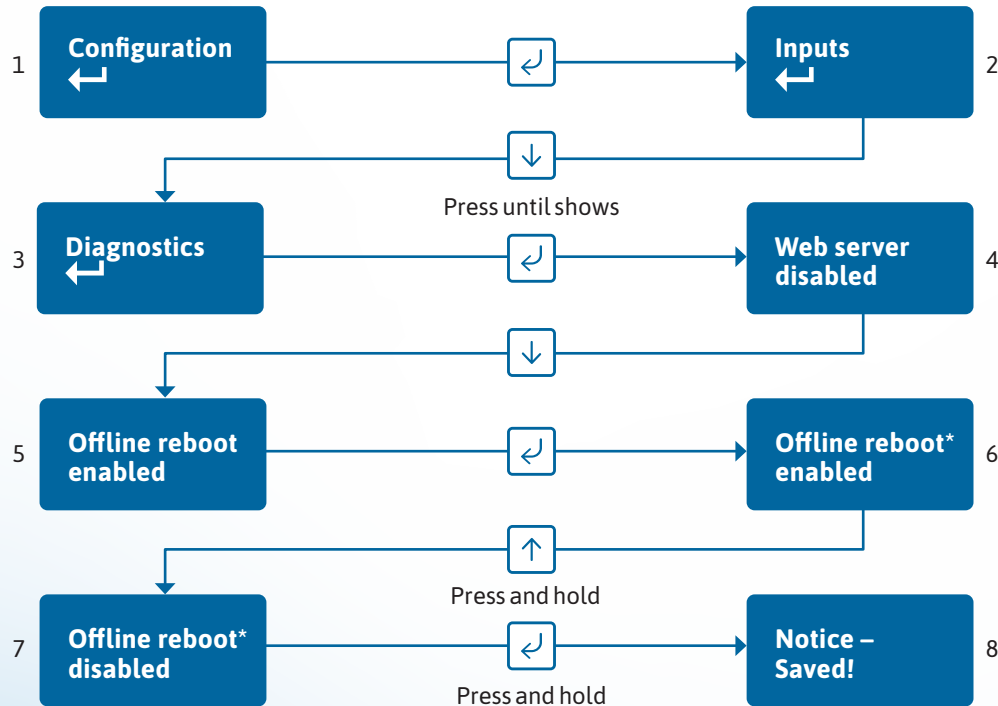
Edit mode for that part of the menu can be exited at any time, without saving changes, by pressing for 5s. This will return you to the sub-menu that you were making changes in.

The configuration menu can be exited at any time without saving any changes by pressing for 5s. This will take you back to the scrolling status display.

Offline reboot screen

Device will automatically reboot if offline for approx. 2 hours (time will vary between 2 and 3 hours)

This feature can be disabled as follows



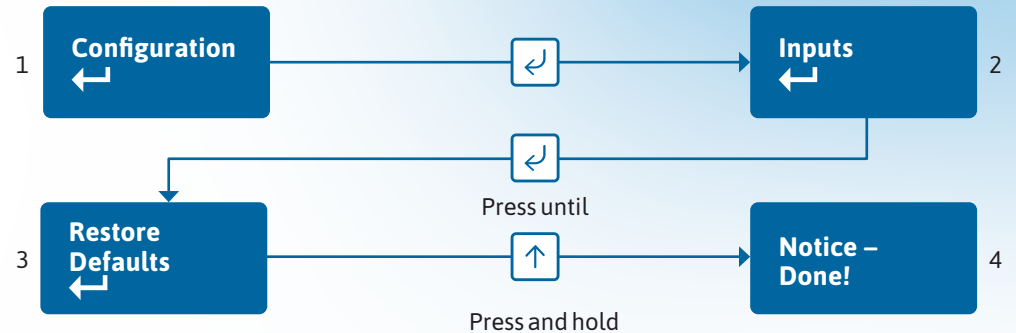
You can exit Edit mode at any time, without saving changes, by pressing for 5s. This will return you to the sub-menu that you were making changes in.

Exit configuration menu at any time without saving any changes by pressing for 5s. This will take you back to the scrolling status display.

Restore defaults

The Restore defaults option on the menu can be used to set the unit back to factory default. All settings will be reset to their standard values.

Example – setting the unit back to factory default



The configuration menu can be exited at any time without saving any changes by pressing for 5s. This will take you back to the scrolling status display.

Web portal and AddSecure app

The device menus are accessible via the Addsecure web portal and app.

The Webportal displays the license agreement and privacy agreements on first login and the user must accept the T&Cs before continuing. The date and time when the user accepts the license agreement is captured. The Installer should obtain the End Customers consent should they wish to use any personal information.

Addsecure App Password

To change an existing known password on the Addsecure App:

- Go to Settings and turn off the app lock (password) by toggling the button.
- You will need to enter your current password,
- When you re enable app Lock (password) it will ask you to create a new password.
- If you forget your App password you will need to un install and re install the app.

Firmware updates

During the installation process or annual maintenance visit, it's important to check to see if there are any firmware updates available for the device. You should apply any firmware updates at that point - either from the Addsecure web portal, or by the Addsecure Helpdesk under the instruction of an on-site engineer. There'll be firmware updates for security updates, bug fixes and additional functions. Once you've installed a device, you can check for firmware updates and apply them at any time, using the Addsecure web portal. It's your responsibility to update the firmware, as a reboot of the device will take place.

Notification of software updates is via the web portal. If the update is critical, then the installer will receive an email indicating the risks mitigated by the new version. The release notes and relevant documentation will also provide details on the period of service disruption should the user initiate the upgrade.

Relevant upgrade documentation is saved as part of the Webportal for the installers. You will need to login to find the latest information.

It is the responsibility of the installer to communicate with the end-customer before changes are made to the communicators.

Compliance with the user access level requirements of EN 50136

When using the web portal and app remotely after installation is completed then the following will apply.

Access to the configuration options by an installer must be authorised by a level 2 user e.g. site owner. For the Next Generation alarm transmission equipment compliance is achieved at installation by requiring a one-time authorisation agreed as part of a service level agreement.

It is recommended the signed authorisation is retained with the 'as fitted' documentation.

An example authorisation form is provided in the Appendix.

To comply with EN 50136-2 Clause 5.2 Access levels, the PIN code access must be set to 6-digits. You can change the access PINs in the USER settings. This applies for all types of access to the device.

For best practice, mobile app access requires the Installer to set up a Web passcode and pin in the device and then advise and show the end customer how to change the PIN.

For passcode/pin recovery the End Customer needs to contact their Installer. For PIN resets you can use the reset pin function in the Ultrasync portal.



Interconnection monitoring

Interconnection monitoring

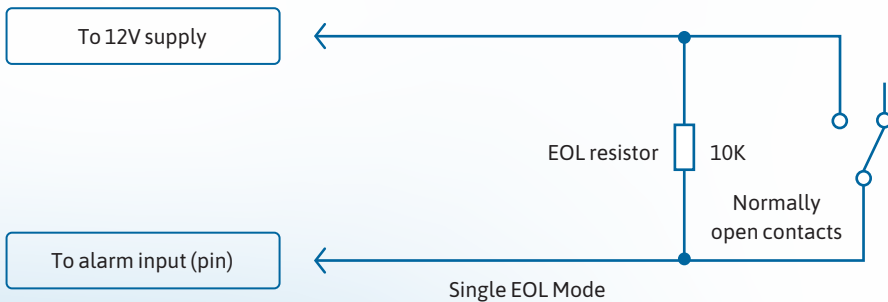
If the signalling unit is remote from the alarm panel, it is possible to wire the pin inputs to be able to detect open or short circuits on the interconnection wiring between the panel and the unit.

To enable the interconnection monitoring you will need to program the unit via the configuration menu, app or web portal.

End of Line

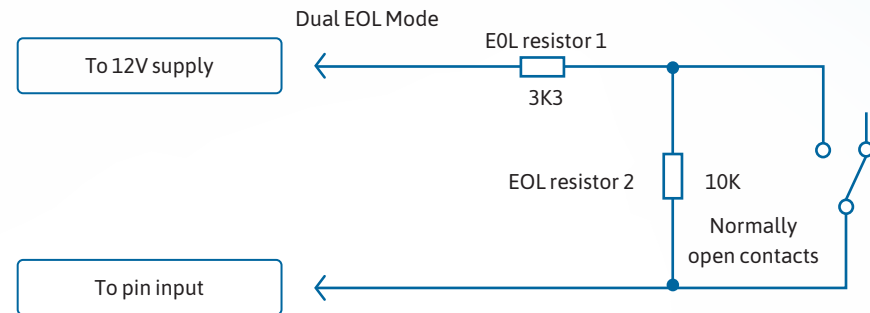
Single EOL mode

Each of the required pins will need to be wired as shown below.



Wiring for interconnection monitoring

Each of the pins required will need to be wired as shown below.



You will need 1 x 3K3 and 1 x 10K resistor for each Pin with interconnection monitoring.

3.3KΩ 1%



orange, orange, black, red, brown

10KΩ 1%



brown, black, black, red, brown

What happens when pins are configured and wired in this way

The dual resistor EOL mode is able to detect four states:

- Alarm event
- Restore
- Wire cut
- Wire shorted

The OLED display will show pin cut 1 through 16 to indicate the wire cut condition for any of Pins 1–16, which are presently in the wire cut state.

Alarms GPI Cut
6

Above, example Cut on Pin 6.

The OLED display will show Short 1 through 16 to indicate the wire shorted condition for any of Pins 1–16, which are presently in the wire shorted state.

Alarms GPI Short
8

Above, example Short on Pin 8.

Alarms will also be sent through to the Alarm Receiving Centre for each of these conditions.



Panel upload Download and Enhanced format signalling (SIA/CID)

Remote access to the alarm panel can be achieved using the Addsecure UDL facility. Additional panel set up information is also available for enhanced format signalling. Contact your Addsecure representative for further details.

Dial Capture

The Dial Capture pins present a 'phone line' to the panel's onboard digital communicator. Connect the alarm panel's digital communicator line connections to the terminals marked DIAL CAP on the unit.



The terminals are not polarity conscious.

Configure the alarm panel digital communicator to dial 29 and use the last 4 digits of the TAID as the account number.

The Dial Capture board will auto detect the panel protocol as events are sent from the alarm panel. SIA, CID or FF.

Please check current panel compatibility listing.

If there are any issues, you can easily spot them and put them right by connecting a test phone, or listening device to the Dial Capture inputs. The Dial Capture pins with a test phone connected and line seized (as if making a phone call) will provide a continuous tone (dialling tone). The Dial Capture pins will also have a voltage on there of 45V.

Serial panel connections

Select the required panel via the serial panel type menu option via the buttons, app or web portal.

Please contact your Addsecure representative for the latest information on panel compatibility for Upload Download and enhanced format signalling via serial connections.

Then wire in the panel using the GND, TX/B and RX/A terminals.



Example below shows connection via RS 485 to a Galaxy Dimension panel:

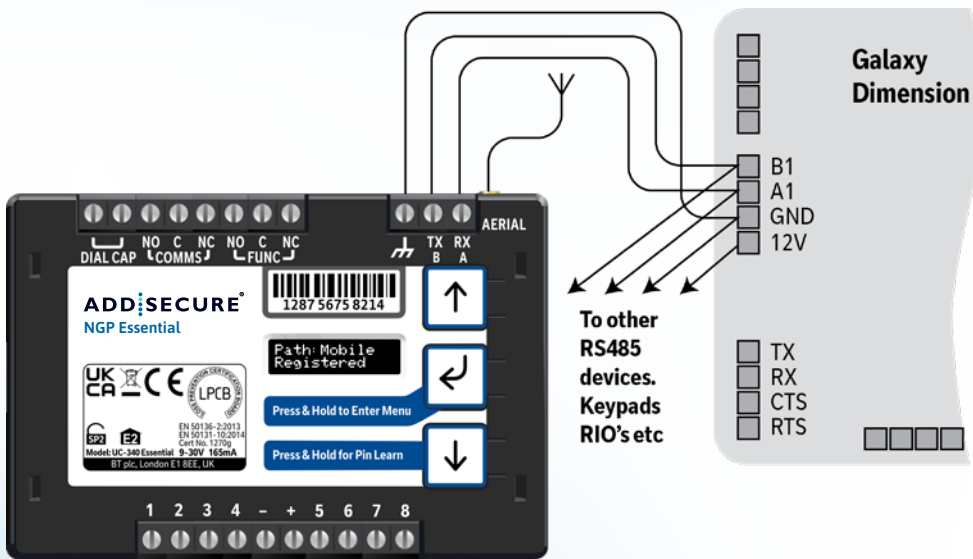


Figure 8 (not to scale)

Connection advice

The unit should be connected to the Honeywell Galaxy panel as shown in figure 10, RS485A to A1 and RS485B to B1. Do not use the secondary data line (if your panel has one – A2/ B2) as it will not work. Ensure that the GND of the unit is connected to the GND terminal on the panel.

It is recommended that good quality screened cable (Belden type, CAT5e or equivalent) is used in all wiring of this type to avoid interference on the panel's data bus. A 680Ω resistor should be used at the end of the 'daisy chain' line of devices in the normal way, taking care not to exceed the maximum number of devices allowed on that data line. If the unit is fitted less than 5m from the alarm panel then an additional termination resistor is generally not required.

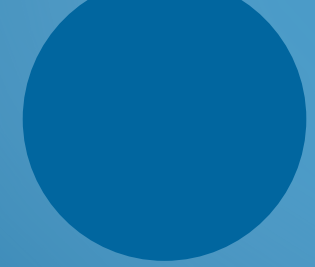
The unit does not have a terminating resistor.

Alarm list

Description	Pin	CID (zone)
Inputs 1-8	1-8	323 (901-908)
Low Battery	985	302 (999)
Unit reboot	984	305 (995)
Panel dial fail	983	314 (999)
Software changed	979	304 (999)
Panel message error	958	311 (997)
Panel Connection	n/a	356 (997)
BSIA 175 Test	n/a	354 (998/999)
Inputs 1-8 cut alarm	n/a	325 (901-908)
Inputs 1-8 Short Alarm	n/a	324 (901-908)
Total Comms Fault	n/a	350 (999)

Figure 9 – Alarms signals as delivered to your ARC

IMPORTANT NOTE: If intending to use Dial Capture or serial for sending alarms, please confirm beforehand with your ARC that their automation software is capable of differentiating correctly between pin alarms (NGP Essential or Addsecure Platform generated alarms) and alarm panel generated ZONE alarms.



Personal Data

Personal information consent

Installers should obtain the End Customers consent should they wish to include any personal data in the app or portal.

End of Service

The End Customer needs to follow the standard process to cease the service with their installers. The following steps should be followed by the installer when disabling a service. The Installer should cease the service with the Alarm Receiving Centre. Addsecure will then cease the entry on the portal within 3 months (this allows for re instatement of any cease in errors) **The communicator needs to be recovered from site by the installer or defaulted to restore its configuration to factory defaults.** The installation quick start guide provides steps to set the unit back to factory defaults. The unit should then be powered down so that it will not attempt connection to the network.

All personal data associated with the unit will be deleted from the device. However, historical event information will remain in the system archives for 7 years as part of compliance requirements.

Withdraw of End Customer Consent

The only way for an End Customer to withdraw consent of personal data processing by Addsecure is to deactivate the service. Please refer to the End of Service section above for more details. The End Customer will need to remove the APP from their personal smart device using standard methods. Installers will need to delete the Site from their APP using standard site deletion method.

AddSecure privacy policy can be found here <https://www.addsecure.com/alarm-signalling/uk/> which includes what to do if you are unhappy about how we have handled personal information.



Disposal

The symbol shown here and on the product means that it's classed as Electrical or Electronic Equipment, and should not be disposed of with other household or commercial waste at the end of its working life.

The Waste Electrical and Electronic Equipment (WEEE) Directive (2012/19/EU) has been put in place to recycle products using the best available recovery and recycling techniques, to minimise the impact on the environment, treat any hazardous substances and avoid increasing landfill.



Product disposal instructions for users

Please dispose of the product as per your local authority's recycling processes. For more information please contact your local authority or retailer where the product was purchased. You can return the product to the freepost address below:

BT Supply Chain
Darlington Road
Northallerton
North Yorkshire
DL6 2PJ

Disclaimer

The manufacturer or his agents disclaim responsibility for any damage, financial loss or injury caused to any equipment, property or persons resulting from any use of this equipment. The manufacturer is not liable for any purely economic loss arising from any use of this equipment. All responsibility and liability in the use of Addsecure products are assumed by the user.

This unit is designed to be used in customer premises. Use of this equipment in other locations may void warranty.

This unit is not intended for use in marine environments or water borne vessels.

Addsecure may make changes to features and specifications at any time without prior notification in the interest of ongoing product development and improvement.

Glossary

ARC

Alarm Receiving Centre

BSIA

British Security Industry Association

GMT

Greenwich Mean Time

IP

Internet Protocol

MMCX

Micro Miniature Coaxial Connector

OLED

Organic Light Emitting Diode

PIN

Parallel Input

RPS

Return Path Signalling (An output that confirms delivery of Pin 4 to the ARC)

RX

Receive

SID

Serial Identity number – 12 digit unique identity number of a unit

SIM

Subscriber identity module (sim card)

TTL

Transistor Transistor Logic

TX

Transmit

USB

Universal Serial Bus



Approvals

**BT Redcare,
British Telecommunications plc 2024.
Registered office: 1 Braham Street,
London E1 8EE.
Registered in England
No. 1800000.**

November 2024

Compliance to EN 50136-2: 2013 and EN 50131-10: 2014

NGP Essential is suitable for use in systems installed to conform to PD6662:2017 at Grade 2 (SP2) and environmental class 2.

Technical Data: see www.addsecure.com/alarm-signalling/uk/

Technical support:

AddSecure Ltd
Phone: +44 20 461 431 70
Email: support.smartalarms.uk@addsecure.com

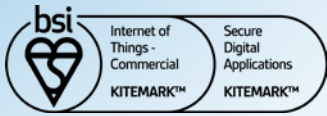
Additional performance parameters:



Support

For assistance with your AddSecure installation, please contact the AddSecure Helpdesk on: 0800 800 628, option 3.
If there is a problem with the service and/or communicator the End Customer should contact the alarm installer. The alarm installer can contact AddSecure Helpdesk M-F 9 till 5.

Description	Transmission Time	Information Security	Substitution Security	Reporting Time
SP6	SP6	SP6	SP2	SP2



KM 742188

In respect of: Internet of Things (IoT)
Security of a device against common vulnerabilities for use in a commercial environment (includes Residential environment)



KM 742187

In respect of: OWASP ASVS and MASVS
Secure Digital Applications
Mobile Applications (OWASP MASVS Ver 1.3 Level 1):
AddSecure Mobile Application Android version 2.18.0 Build 0363
AddSecure Mobile Application iOS version 2.18.0 Build 0463
Web Application (OWASP ASVS 4.0.2 Level 1)
The AddSecure Ultrasync Portal Application



LPCB certification

- Extensive testing by BRE has independently validated the performance of Advanced/Advanced Extra and demonstrated compliance with the applicable EN 50131 and EN 50136 standards.
- Regular on-going surveillance of the manufacturing facilities by BRE, ensures the high quality of the Next Generation range is maintained through the life of the products.
- LPCB certification provides prescribers and owners of intrusion alarm systems with assurance that the signalling equipment will respond rapidly and continue function reliably, a prerequisite for any monitored alarm system.

BSI 'Kitemark' accreditation for IoT devices, app and portal

- The Kitemark is designed to help consumers confidently and easily identify IoT devices, apps and portals that they can trust to be safe, secure, and functional.
- Once the BSI Kitemark is achieved the product will undergo regular monitoring and assessment including functional and interoperability testing, further penetration testing and an audit to review any necessary remedial action. Importantly, if security levels and product quality are not maintained the BSI Kitemark will be revoked until any flaws are rectified.
- The IoT Kitemark assessment process involves a series of tests that help ensure the device is fully compliant to the requirements.

Before being awarded the Kitemark the manufacturer is assessed against ISO 9001, and the product is required to pass both an assessment of functionality and interoperability, as well as penetration testing scanning for vulnerabilities and security flaws.

- An app that has been awarded a BSI Kitemark™ for Secure Digital Applications has demonstrated that it has appropriate robust security controls in place for the information it is handling. To achieve the BSI Kitemark, an app must undergo rigorous and independent testing.

Police CPI 'Secured By Design' (SBD) accreditation

- Police Crime Prevention Initiatives (Police CPI) is a police-owned organisation which delivers a wide range of crime prevention and demand reduction initiatives across the UK.
- The extensive Police CPI portfolio covers a variety of crime prevention initiatives, of which Secured by Design is the most well-known, with all initiatives designed to keep the public safe from crime.
- Secured by Design (SBD) operates an accreditation scheme on behalf of the UK Police Service for products or services that have met recognised security standards. These products or services, which must be capable of deterring or preventing crime, are known as being of a 'Police Preferred Specification'.

Appendix

Example authorisation form

For the purposes of on-going maintenance and configuration

Company name

Authorises

Installer company name

Remote access to Addsecure Next Generation Supervised Premises Transceiver

Serial No. *number*

Installed at: *premises address*

Date

Signature

ADD:SECURE

